Deep Discovery™ Analyzer 7.6

Syslog コンテンツマッピングガイド

Deep Discovery Analyzer 7.6 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

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro

P/N: APEM769915/240703

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 Analyzer 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 Analyzer 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 4 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 Analyzer 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	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 管理者ガイドには、Deep Discovery Analyzer を設定して管理する方法の詳細な手順、および Deep Discovery Analyzer 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	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 インストールガイドには、Deep Discovery Analyzer 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	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 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 Analyzer 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 Analyzer 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	Deep Discovery Analyzer 管理コンソールからアクセスできる Web ベースのドキュメントです。 オンラインヘルプには、Deep Discovery Analyzer のコンポーネントと機能、Deep Discovery Analyzer 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/dcx/s/?language=ja

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

https://www.trendmicro.com/ja_jp/business/products/downloads.html?clk=left_nav&clkval=all_download&regs=jp

対象読者

この Deep Discovery Analyzer 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

Deep Discovery Analyzer 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 Analyzer 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 Analyzer 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、5 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 Analyzer 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、25 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 Analyzer 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、45 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 Analyzer 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)

イベント

Deep Discovery Analyzer では、次のイベントがサポートされます。

表 1-1. サポートされるイベント

イベント名	イベントの説明
仮想アナライザ分析ログ: 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
仮想アナライザ分析ログ: URL 分析イベント	仮想アナライザの URL 分析イベント
統合製品検出ログ: 検出結果イベント	Deep Discovery Inspector や InterScan Web Security Virtual Appliance などの統合製品の検出
仮想アナライザ分析ログ: 著しい特性イベント	仮想アナライザの結果の著しい特性
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	仮想アナライザの結果の不審オブジェクト
システムイベントログ	システムによって生成されるイベントログ
アラートイベントログ	アラートによって生成されるイベントログ
ICAP 事前検索によるログ	ICAP 事前検索からの検出

バージョン履歴

表 1-2. Deep Discovery Analyzer のバージョン履歴

バージョン	改訂
5.5	初期バージョン
5.5 SP1	統合製品検出ログ: 検出結果イベントを追加
6.0	• システムイベントログを追加 • アラートイベントログを追加 • 統合製品検出ログ: 検出結果イベントの ICAP プロトコルの `deviceDirection` の値を更新
7.1	ICAP 事前検索による検出ログを追加
7.5	統合製品検出ログ: 検出結果イベントのサンプルのサブミッションに関連した新しいキーを追加

第 2 章

Syslog コンテンツマッピング - CEF

次の各表は、Deep Discovery Analyzer 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 製品検出ログ: 検出イベント / 統合された製品からのサブミットによる検出イベント

表 2-1. CEF 製品検出ログ: 検出イベント / 統合された製品からのサブミットによる検出イベント

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200119
Header (eventName)	説明	Sample file sandbox analysis is finished
Header (severity)	重大度	3: 情報
cn1	GRID/CSSS の結果	• -1: GRID が不明 • 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

CEF キー	説明	値
cn2	ROZ レーティング (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
cn2Label	ROZ レーティング (仮想アナライザの分析結果用内部コード)	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
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

CEF 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
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
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 形式の仮想アナライザ分析ログ: URL 分析イベント

表 2-2. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200126
Header (eventName)	説明	URL sandbox analysis is finished

CEF キー	説明	値
Header (severity)	重大度	3: 情報
cn2	ROZ レーティング (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
cn2Label	ROZ レーティング (仮想アナライザの分析結果用内部コード)	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
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
fileHash	SHA1	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+08:00

ログの例:

CEF 形式の統合製品検出ログ: 検出結果イベント

表 2-3. CEF 形式の統合製品検出ログ: 検出結果イベント

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200128
Header (eventName)	説明	SUBMISSION_ANALYZED
Header (severity)	Deep Discovery Analyzer のリスクレベルマッピング:	• 1: 未評価 • 2: リスクなし • 4: 低 • 6: 中 • 8: 高
app	アプリケーションプロトコル	例: FTP/HTTPS/MSN/...
c6a2	送信元 IPv6 アドレス	例: 2001:db8::1

CEF キー	説明	値
c6a2Label	送信元 IPv6 アドレス	srcIPv6
c6a3	送信先 IPv6 アドレス	例: 2001:db8:a0b:12f0::1
c6a3Label	送信先 IPv6 アドレス	dstIPv6
cn1	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
cn1Label	サンプルの種類	sampleType
cs1	不正プログラム名	例: HEUR_NAMETRICK.A
cs1Label	不正プログラム名	malName
cs2	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	メール ID	messageId
cs3	アプリケーションプロトコルグループ	例: SMTP/HTTP/…
cs3Label	アプリケーションプロトコルグループ	appGroup
cs4	サブミッター	
cs4Label	サブミッター	サブミッター
cs5	サンプルを手動でサブミットしたサブミッターのホスト名またはユーザ名	例: shost1
cs5Label	サブミッターのホスト名	submitterName
cs6	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cs6Label	sha256	

CEF キー	説明	値
cs7	サンプルのサブミッション時間	例: Mar 03 2016 16:28:20 GMT+08:00
cs7Label	送信時間	submittedTime
cs8	サンプルの分析の完了時間	例: Mar 03 2016 16:28:20 GMT+08:00
cs8Label	完了時間	completedTime
deviceDirection	関連付けられた方向	ICAP プロトコルの場合: • 0: ICAP REQMOD • 1: ICAP RESPMOD その他のプロトコルの場合: • 0: 受信 • 1: 送信 • 2: 不明
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceProcessName	アプライアンスのプロセス名	例: explorer.exe
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC アドレス	例: 00:0C:29:6E:CB:F9
dpt	送信先ポート	0〜65535 の値
dst	送信先 IPv4 アドレス	例: 10.1.144.199
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
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	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
requestClientApplication	ユーザエージェント	例: IE
rt	サブミッターでのイベント生成時間	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 アドレス	例: 00:0C:29:6E:CB:F9
spt	送信元ポート	0〜65535 の値
src	送信元 IPv4 アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|7.5.0.1115|2001
28|SUBMISSION_ANALYZED|8|rt=Mar 21 2023 15:32:50 GMT+08:00
 dvc=192.168.1.1 dvchost=DDAN dvcmac=B8:CA:3A:68:2F: CC de
viceExternalId=B4F796E5-C139-4241-80FD-248D10F7CCB2 src=19
6.109.36.118 spt=39899 dst=108.109.7.8 dpt=11503 cn1Label=
sampleType cn1=1 fileHash=F00C4312D16CBC0B2926A45544B01BE2
```

```
FF24E184 request=http://www.bq998.com/DownFiles/FoxJD.Rar
cs1Label=malName cs1=VAN_WEB_THREAT.UMXX cs4Label=submitte
r cs4=Deep Discovery Inspector cs5Label=submitterName cs5=
localhost.localdomain cs6Label=sha256 cs6=E0EFF50D6D817BE9
9AAD183A131A29DFC34CAECCA43F93D55A9347A1C2B27F72 cs7Label=
submittedTime cs7=Mar 21 2023 15:29:51 GMT+08:00 cs8Label=
completedTime cs8=Mar 21 2023 15:29:58 GMT+08:00
```

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 2-4. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200127
Header (eventName)	説明	Notable Characteristics of the analyzed sample
Header (severity)	重大度	6: 警告
cs1	違反ポリシー名	例: Internet Explorer Setting Modification
cs1Label	違反ポリシー名	PolicyCategory
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
cs3	サンドボックスイメージの種類	例: win7

CEF キー	説明	値
cs3Label	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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: Source: ATSE\nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.1246\nMalware Pattern Version: 11.501.90
rt	分析時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

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 2-5. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200120
Header (eventName)	説明	Deny List updated
Header (severity)	重大度	3: 情報
act	イベントの処理	Add
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 IPv4 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
end	拒否リストの有効期限	例: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
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+08:00

ログの例:

CEF 形式のシステムイベントログ

表 2-6. CEF 形式のシステムイベントログ

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventid)	イベント ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	説明	例: Updates: Component update settings modified by 'admin' from 192.168.10.2.
Header (severity)	重大度	3: 情報

CEF キー	説明	値
dvc	アプライアンスの IP アドレス	例: IPv4: 192.168.10.1
devmac	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
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 03 2016 16:28:20 GMT+08:00
cs1Label	イベントの種類のラベル	eventType
cs1	イベントの種類	例: Account Logon/Logoff
duser	ユーザ名	例: admin
src	送信元 IPv4 アドレス	例: IPv4: 192.168.10.1
c6a2Label	送信元 IPv6 アドレスのラベル	srcIPv6
c6a2	送信元 IPv6 アドレス	例: 2620:0101:4002:0401::131
shost	送信元ホスト名	例: shost1
outcome	結果のステータス	• Success • Failure

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|3009
99|Log Settings: Settings modified by 'admin' from 10.204.
1.2|3|rt=Nov 07 2017 10:05:58 GMT+00:00 dvc=10.204.1.1 dvc
host=DDAN dvcmac=00:0C:29:2F:3B:6B deviceExternalId=423E63A
A-D466-406E-A15F-6AC6F3CEE50A cs1Label=eventType cs1=System
```

```
Setting duser=admin src=10.204.1.2 outcome=Success
```

CEF 形式のアラートイベントログ

表 2-7. CEF 形式のアラートイベントログ

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventid)	イベント ID	300105
Header (eventName)	説明	ALERT_EVENT
Header (severity)	重大度	• 2: 情報 • 6: 重要 • 8: 重大
dvc	アプライアンスの IP アドレス	例: • IPv4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
devmac	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	イベントのログ記録日時	例: Mar 03 2016 16:28:20 GMT+08:00
cs1Label	ルール名のラベル	ruleName

CEF キー	説明	値
cs1	ルール名	例: High Memory Usage
cs2Label	影響を受けるアプライアンスのラベル	affectedAppliance
cs2	影響を受けるアプライアンス	例: DDAN.com (10.204.1.2 | FE80::29FF:29FF: 29FF: 29FF)
cs3Label	件名のラベル	subject
cs3	件名	例: DDAN Important Alert - High Memory Usage
cs4Label	メッセージのラベル	ruleContent
cs4	メッセージ	メッセージの内容

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300105
|ALERT_EVENT|6|rt=Nov 07 2017 08:39:54 GMT+00:00 dvc=10.204.
1.1 dvchost=DDAN dvcmac=00:0C:29:2F:3B:6B deviceExternalId=4
23E63AA-D466-406E-A15F-6AC6F3CEE50A cs1Label=ruleName cs1=Hi
gh CPU Usage cs2Label=affectedAppliance cs2=DDAN ( 10.204.19
1.1 | FE80::20C:29FF:FE2F:3011 ) cs3Label=subject cs3=DDAN I
mportant Alert - High CPU Usage cs4Label=ruleContent cs4=The
 average CPU usage in the last 5 minutes exceeded the thresh
old of 90%.\n\nAverage CPU usage: 96%\nAffected appliance: D
DAN (10.204.191.1 | FE80::20C:29FF:FE2F:3011)\n\nReduce the
number of Virtual Analyzer instances, or add a secondary app
liance to improve performance.\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=
\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\nAlert time: 20
17-11-07 08:39:54\nManagement console: https://10.204.191.1/
 | https://[FE80::20C:29FF:FE2F:3011]/
```

CEF 形式の ICAP 事前検索による検出ログ

表 2-8. CEF 形式の ICAP 事前検索による検出ログ

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	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Analyzer
Header (pver)	アプライアンスのバージョン	例: 7.1.0.1088
Header (eventid)	署名 ID	200129
Header (eventName)	イベント名	ICAP_PRESCAN_EVENT
Header (severity)	リスクレベル	8
rt	ログ生成時刻	例: May 31 2021 15:56:04 GMT+08:00
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
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
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
src	送信元 IPv4 アドレス	例: 10.1.144.199
dst	送信先 IPv4 アドレス	例: 10.1.144.198
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar

CEF キー	説明	値
cn1Label	サンプルの種類	sampleType
cn1	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
request	URL	例: http://example.com:80/
cs1Label	不正プログラム名	malName
cs1	不正プログラム名	例: HEUR_NAMETRICK.A
cs2Label	submitterName	
cs2	ICAP クライアント	例: 10.205.190.3
cs3Label	icapMode	
cs3	ICAP モード	例: • REQMOD:ICAP 要求の変更方法 • RESPMOD:ICAP 応答の変更方法
cs4Label	送信元ユーザ	
cs4	ICAP クライアントにより送信された X-Authenticated-User ICAP ヘッダ	例: test.com
cs5Label	検出元	

CEF キー	説明	値
cs5	オブジェクトを処理した検出モジュールの名前	例: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)
cs6Label	sha256	
cs6	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:31:35 GMT+00:00 d
vc=10.2.3.100 dvchost=DDAN dvcmac=00:50:56:98:33:69 device
ExternalId=627EE441-DD62-4483-B9E4-60B3C8A92529 src=10.2.1
1.122 cn1Label=sampleType cn1=1 fileHash=317D137FE590EE561
648ECA137CB2B6898526115 request=http://wrs21.test.com:80/
cs1Label=malName cs1=TSPY_KEYLOG.GC cs2Label=submitterName
 cs2=10.2.1.6 cs3Label=icapMode cs3=REQMOD cs4Label=source
User cs5Label=identifiedBy cs5=Web Reputation Services cs6
Label=sha256 cs6=F5C748A953D23B8CE4F5C792FDC1E7987471DD48F
E24ABA07C3CFD10B4AEF72F
```

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:31:31 GMT+00:00 d
vc=10.2.1.52 dvchost=DDAN dvcmac=00:50:56:98:33:69 deviceE
xternalId=627EE441-DD62-4483-B9E4-60B3C8A92529 dst=10.2.1.
122 src=10.2.1.123 cn1Label=sampleType cn1=0 fname=3-layer
.zip fileType=ZIP archive fileHash=D7273555CB0AC08303415CB
EB3F3D72DD0893BC4 request=http://test.com/3-layer.zip cs1L
abel=malName cs1=Eicar_test_file,TROJ_OLEXP.TPD cs2Label=s
ubmitterName cs2=10.2.1.6 cs3Label=icapMode cs3=RESPMODE c
s4Label=sourceUser cs5Label=identifiedBy cs5=Advanced Thre
at Scan Engine cs6Label=sha256 cs6=08F18BC62297A67DD91E192
A27C1EEDE3C1BBEE19A90FC0B1FADD07CE93B9823
```

第 3 章

Syslog コンテンツマッピング - LEEF

次の各表は、Deep Discovery Analyzer 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 製品検出ログ: 検出イベント/統合された製品からのサブミットによる検出イベント

表 3-1. LEEF 製品検出ログ: 検出イベント/統合された製品からのサブミットによる検出イベント

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
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
deviceProcessHash	上位の SHA-1	例: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar

LEEF キー	説明	値
fsize	ファイルサイズ	例: 131372
gridIsKnownGood	GRID/CSSS の結果	• -1: GRID が不明 • 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 (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
sev	重大度	3: 情報

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。

ログの例:

LEEF 形式の形式の仮想アナライザ分析ログ: URL 分析イベント

表 3-2. LEEF 形式の形式の仮想アナライザ分析ログ: URL 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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
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
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
devTime	ログ生成時刻	例: Jan 28 2015 02:00:36 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	SHA1	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

LEEF キー	説明	値
pComp	検出エンジン/コンポーネント	Sandbox
rozRating	ROZ レーティング (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
sev	重大度	3: 情報
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「<009>」で区切ります。

ログの例:

LEEF 形式の統合製品検出ログ: 検出結果イベント

表 3-3. LEEF 形式の統合製品検出ログ: 検出結果イベント

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 Analyzer

LEEF キー	説明	値
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventName)	説明	SUBMISSION_ANALYZED
app	アプリケーションプロトコル	例: FTP/HTTPS/MSN/...
appGroup	アプリケーションプロトコルグループ	例: SMTP/HTTP/…
deviceDirection	関連付けられた方向	ICAP プロトコルの場合: • 0: ICAP REQMOD • 1: ICAP RESPMOD その他のプロトコルの場合: • 0: 受信 • 1: 送信 • 2: 不明
deviceProcessName	アプライアンスのプロセス名	例: explorer.exe
devTime	サブミッターでのイベント生成時間	例: Jan 28 2015 02:00:36 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
dst	送信先 IPv4 アドレス 送信先 IPv6 アドレス	例: 10.1.144.199 例: 2001:db8:a0b:12f0::1
dstMAC	送信先 MAC アドレス	例: 00:0C:29:6E:CB:F9
dstPort	送信先ポート	0〜65535 の値
duser	メール受信者	例: user1@example2.com;test@163.com

LEEF 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
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
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
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
malName	不正プログラム名	例: HEUR_NAMETRICK.A
messageId	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
requestClientApplication	ユーザエージェント	例: IE
sampleType	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
sev	Deep Discovery Analyzer のリスクレベルマッピング:	• 1: 未評価 • 2: リスクなし • 4: 低 • 6: 中 • 8: 高

LEEF キー	説明	値
sha256	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
shost	送信元ホスト名	例: shost1
src	送信元 IPv4 アドレス 送信元 IPv6 アドレス	例: 10.1.144.199 例: 2001:db8::1
srcMAC	送信元 MAC アドレス	例: 00:0D:60:AF:1B:61
srcPort	送信元ポート	0〜65535 の値
サブミッター	サブミッター	
submitterName	サンプルを手動でサブミットしたサブミッターのホスト名またはユーザ名	例: shost1
suser	メール送信者	例: user2@example.com
url	URL	例: http://1.2.3.4/query?term=value
submittedTime	サンプルのサブミッション時間	例: Mar 03 2016 16:28:20 GMT+08:00
submittedTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
completedTime	サンプルの分析の完了時間	例: Mar 03 2016 16:28:20 GMT+08:00
completedTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z

ログの例:

```
LEEF: 1.0|Trend Micro|Deep Discovery Analyzer|7.5.0.1115|S
UBMISSION_ANALYZED|devTime=Mar 21 2023 17:05:04 GMT+08:00#
011devTimeFormat=MMM dd yyyy HH:mm:ss z#011sev=8#011dvc=19
2.168.1.1#011dvchost=DDAN#011deviceMacAddress=EC:F4:BB:DE:
E1:F8#011deviceGUID=B4F796E5-C139-4241-80FD-248D10F7CCB2#0
```

```
11src=192.168.88.108#011srcPort=13861#011dst=42.62.93.35#0
11dstPort=6891#011sampleType=0#011fname=evasion-000002#011
fsize=2868884#011fileType=ELF Executable#011fileHash=BD846
3790E46BB9B7571378FA2ADBA69F0342576#011malName=Troj.ELF.TR
X.XXELFC1DFF026,VAN_TROJAN.UMXX#011submitter=Deep Discover
y Inspector#011submitterName=localhost.localdomain#011sha2
56=1BC25EF196A08EA25DBBF2832E010C3AE4A3E227B1F7A3F5D014C80
DDC3AEE32#011submittedTime=Mar 21 2023 17:02:06 GMT+08:00#
011submittedTimeFormat=MMM dd yyyy HH:mm:ss z#011completed
Time=Mar 21 2023 17:04:54 GMT+08:00#011completedTimeFormat
=MMM dd yyyy HH:mm:ss z
```

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 3-4. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
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:29:56:B3:57
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+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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
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:884 \nFile: %TEMP%\~DF7A0C28F4D7D9E792.TMP\nType: VSDT_ERROR
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	6: 警告

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。

ログの例:

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 3-5. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventName)	イベント名	DENYLIST_CHANGE
act	イベントの処理	Add
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+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
dpt	送信先ポート	0〜65535 の値
dst	送信先 IPv4 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

LEEF キー	説明	値
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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	検出エンジン/コンポーネント	Sandbox
sev	重大度	3: 情報
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「<009>」で区切ります。

ログの例:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|DENY
LIST_CHANGE|devTime=Feb 28 2015 02:50:03 GMT+00:00<009>devTim
eFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<00
9>dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC
:F4:BB:C6:F1:D0<009> deviceGUID=758B04C9-F577-4B8A-B527-ABCB8
4FDAC83<009>end=Mar 30 2015 02:45:48 GMT+00:00<009>act=Add<00
9>fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD<009>devic
eExternalRiskType=High<009>type=Deny List File SHA1
```

LEEF 形式のシステムイベントログ

表 3-6. LEEF 形式のシステムイベントログ

LEEF キー	説明	値
Header (logVer)	LEEF 形式のバージョン	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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventName)	イベント名	• PRODUCT_UPDATE • SYSTEM_EVENT
sev	重大度	3: 情報
dvc	アプライアンスの IP アドレス	例: 192.168.10.1
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	イベントのログ記録日時	例: Mar 03 2016 16:28:20 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
eventType	イベントの種類	• System Setting • Account Logon/Logoff • System Update
duser	ユーザ名	例: admin
msg	詳細	例: Updates: Component update settings modified by 'admin' from 10.64.54.159.

LEEF キー	説明	値
src	送信元 IPv4/IPv6 アドレス	例: 192.168.100.100
shost	送信元ホスト名	例: shost1
outcome	結果のステータス	• Success • Failure

ログの例:

```
LEEF: 1.0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|SYS
TEM_EVENT|devTime=Nov 07 2017 10:08:30 GMT+00:00<009>devTime
Format=MMM dd yyyy HH:mm:ss z<009>sev=3<009>dvc=10.204.1.1<0
09>dvchost=DDAN<009>deviceMacAddress=00:0C:29:2F:3B:6B<009>d
eviceGUID=423E63AA-D466-406E-A15F-6AC6F3CEE50A<009>eventType
=System Setting<009>duser=admin<009>src=10.204.1.2<009>msg=L
og Settings: Settings modified by 'admin' from 10.204.1.2<00
9>outcome=Success
```

LEEF 形式のアラートイベントログ

表 3-7. LEEF 形式のアラートイベントログ

LEEF キー	説明	値
Header (logVer)	LEEF 形式のバージョン	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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventName)	イベント名	ALERT_EVENT

LEEF キー	説明	値
sev	重大度	• 2: 情報 • 6: 重要 • 8: 重大
dvc	アプライアンスの IP アドレス	例: • IPv4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	イベントのログ記録日時	例: Mar 03 2016 16:28:20 GMT+08:00
devTimeFormat	時刻の形式	MMM dd yyyy HH:mm:ss z
ruleName	ルール名	例: High Memory Usage
affectedAppliance	影響を受けるアプライアンス	例: DDAN.com (10.204.1.1 | FE80:: 29FF:29FF: 29FF: 29FF)
subject	件名	例: DDAN Important Alert - High Memory Usage
ruleContent	メッセージ	メッセージの内容

ログの例:

```
LEEF: 1.0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|ALE
RT_EVENT|devTime=Nov 07 2017 08:39:54 GMT+00:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>dvc=10.204.1.1<00
9>dvchost=DDAN<009>deviceMacAddress=00:0C:29:2F:3B:6B<009>de
viceGUID=423E63AA-D466-406E-A15F-6AC6F3CEE50A<009>ruleName=H
igh CPU Usage<009>affectedAppliance=DDAN ( 10.204.1.1 | FE80
```

```
::20C:29FF:FE2F:1B6B )<009>subject=DDAN Important Alert - Hi
gh CPU Usage<009>ruleContent=The average CPU usage in the la
st 5 minutes exceeded the threshold of 90%.\n\nAverage CPU u
sage: 96%\nAffected appliance: DDAN (10.204.1.1 | FE80::20C:
29FF:FE2F:1B6B)\n\nReduce the number of Virtual Analyzer ins
tances, or add a secondary appliance to improve performance.
\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=
\=\=\=\=\=\=\=\nAlert time: 2017-11-07 08:39:54\nManagement
console: https://10.204.1.1/ | https://[FE80::20C:29FF:FE2F:
1B6B]/
```

LEEF 形式の ICAP 事前検索による検出ログ

表 3-8. LEEF 形式の ICAP 事前検索による検出ログ

CEF 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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 7.1.0.1088
Header (eventName)	イベント名	ICAP_PRESCAN_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: Jan 28 2015 02:00:36 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

CEF キー	説明	値
dvchost	アプライアンスのホスト名	例: localhost
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar
sha256	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
sampleType	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
url	URL	例: http://1.2.3.4/query?term=value
src	送信元 IPv4 アドレス	例: 10.1.144.199
dst	送信先 IPv4 アドレス	例: 10.1.144.198
sourceUser	ICAP クライアントにより送信された X-Authenticated-User ICAP ヘッダ	例: test
sev	リスクレベル	8: 高
malName	不正プログラム名	例: HEUR_NAMETRICK.A
icapMode	ICAP モード	例: • REQMOD:ICAP 要求の変更方法 • RESPMOD:ICAP 応答の変更方法

CEF キー	説明	値
identifiedBy	オブジェクトを処理した検出モジュールの名前	例: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)

ログの例:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|7.1.0.1009|IC
AP_PRESCAN_EVENT|devTime=May 31 2021 15:56:04 GMT+08:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=8<009>dvc=1
0.204.191.223<009>dvchost=DDAN<009>deviceMacAddress=00:50:
56:98:39:75<009>deviceGUID=22DB5662-BDEC-4071-9D82-E5008EF
8B328<009>dst=10.204.190.8<009>src=10.204.190.7<009>sample
Type=1<009>fileHash=317D137FE590EE561648ECA137CB2B68985261
15<009>url=http://test.com:80/<009>malName=VAN_WEB_THREAT.
UMXX<009>submitterName=10.204.190.6<009>icapMode=RESPMODE<
009>sourceUser=auth_test2<009>identifiedBy=Web Reputation
Services<009>sha256=F5C748A953D23B8CE4F5C792FDC1E7987471DD
48FE24ABA07C3CFD10B4AEF72F
```

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|7.1.0.1009|IC
AP_PRESCAN_EVENT|devTime=Jun 02 2021 13:26:17 GMT+08:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=8<009>dvc=1
```

```
0.204.191.223<009>dvchost=DDAN<009>deviceMacAddress=00:50:
56:98:39:75<009>deviceGUID=22DB5662-BDEC-4071-9D82-E5008EF
8B328<009>dst=10.204.191.122<009>src=10.204.190.6<009>samp
leType=0<009>fname=\\x332d6c617965722e7a6970<009>fileType=
ZIP archive<009>fileHash=D7273555CB0AC08303415CBEB3F3D72DD
0893BC4<009>malName=TROJ_OLEXP.TPD,Eicar_test_file<009>sub
mitterName=10.204.190.6<009>icapMode=RESPMODE<009> sourceU
ser=auth_test<009>identifiedBy=Advanced Threat Scan Engine
<009>sha256=08F18BC62297A67DD91E192A27C1EEDE3C1BBEE19A90FC
0B1FADD07CE93B9823
```

第 4 章

Syslog コンテンツマッピング - TMEF

次の各表は、Deep Discovery Analyzer 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 製品検出ログ: 検出イベント / 統合された製品からのサブミットによる検出イベント

表 4-1. TMEF 製品検出ログ: 検出イベント / 統合された製品からのサブミットによる検出イベント

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200119
Header (eventName)	説明	FILE_ANALYZED
Header (severity)	重大度	3: 情報
cn1	GRID/CSSS の結果	• -1: GRID が不明 • 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

TMEF キー	説明	値
cn2	ROZ レーティング (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
cn2Label	ROZ レーティング (仮想アナライザの分析結果用内部コード)	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:29:6E:CB:F9
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

TMEF キー	説明	値
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
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+08:00

ログの例:

TMEF 形式の仮想アナライザ分析ログ: URL 分析イベント

表 4-2. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200126
Header (eventName)	説明	URL_ANALYZED
Header (severity)	重大度	3: 情報

TMEF キー	説明	値
cn2	ROZ レーティング (仮想アナライザの分析結果用内部コード)	• -1: ROZ でサポートされていないファイルタイプ • 0: 検出リスクなし • 1: リスク低 • 2: リスク中 • 3: リスク高 注意 負の値は常にエラーを示します。
cn2Label	ROZ レーティング (仮想アナライザの分析結果用内部コード)	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:29:6E: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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

TMEF キー	説明	値
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+08:00

ログの例:

TMEF 形式の統合製品検出ログ: 検出結果イベント

表 4-3. TMEF 形式の統合製品検出ログ: 検出結果イベント

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200128
Header (eventName)	説明	SUBMISSION_ANALYZED
Header (severity)	Deep Discovery Analyzer のリスクレベルマッピング:	• 1: 未評価 • 2: リスクなし • 4: 低 • 6: 中 • 8: 高
app	アプリケーションプロトコル	例: FTP/HTTPS/MSN/...
appGroup	アプリケーションプロトコルグループ	例: SMTP/HTTP/…

TMEF キー	説明	値
c6a2	送信元 IPv6 アドレス	例: 2001:db8::1
c6a2Label	送信元 IPv6 アドレス	srcIPv6
c6a3	送信先 IPv6 アドレス	例: 2001:db8:a0b:12f0::1
c6a3Label	送信先 IPv6 アドレス	dstIPv6
cn1	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
cn1Label	サンプルの種類	sampleType
cs1	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs1Label	メール ID	messageId
cs2	サブミッター	
cs2Label	サブミッター	サブミッター
cs3	サンプルを手動でサブミットしたサブミッターのホスト名またはユーザ名	例: shost1
cs3Label	サブミッターのホスト名	submitterName
cs6	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cs6Label	SHA256	
cs7	サンプルのサブミッション時間	例: Mar 03 2016 16:28:20 GMT+08:00
cs7Label	送信時間	submittedTime
cs8	サンプルの分析の完了時間	例: Mar 03 2016 16:28:20 GMT+08:00

TMEF キー	説明	値
cs8Label	完了時間	completedTime
deviceDirection	関連付けられた方向	ICAP プロトコルの場合: • 0: ICAP REQMOD • 1: ICAP RESPMOD その他のプロトコルの場合: • 0: 受信 • 1: 送信 • 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
deviceProcessName	アプライアンスのプロセス名	例: explorer.exe
dhost	送信先ホスト名	例: dhost1
dmac	送信先 MAC アドレス	例: 00:0C:29:6E:CB:F9
dpt	送信先ポート	0〜65535 の値
dst	送信先 IPv4 アドレス	例: 10.1.144.199
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
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

TMEF キー	説明	値
fileType	実際のファイルタイプ	例: RIFF bitmap file
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
malName	不正プログラム名	例: HEUR_NAMETRICK.A
request	URL	例: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
requestClientApplication	ユーザエージェント	例: IE
rt	サブミッターでのイベント生成時間	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 アドレス	例: 00:0C:29:6E:CB:F9
spt	送信元ポート	0〜65535 の値
src	送信元 IPv4 アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|7.5.0.1115|2001
28|SUBMISSION_ANALYZED|8|rt=Mar 21 2023 17:32:22 GMT+08:00
 dvc=192.168.1.1 dvchost=DDAN deviceMacAddress=EC:F4:BB:DE
:E1:F8 deviceGUID=B4F796E5-C139-4241-80FD-248D10F7CCB2 src
=69.65.60.111 spt=18442 dst=116.32.60.114 dpt=50200 cn1Lab
el=sampleType cn1=1 fileHash=A5D14065EC35E86101F2EF1F8550C
02A8CF7C49F request=http://easienglish.com/IWhCoZ malName=
VAN_WEB_THREAT.UMXX cs2Label=submitter cs2=Deep Discovery
Inspector cs3Label=submitterName cs3=localhost.localdomain
```

```
cs6Label=sha256 cs6=E845A4884E75D4465BCDC19D864AA63B26BBEE8
3147CD515F39511CBC03B2BB3 cs7Label=submittedTime cs7=Mar 21
 2023 17:29:24 GMT+08:00 cs8Label=completedTime cs8=Mar 21
2023 17:29:38 GMT+08:00
```

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 4-4. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191
Header (eventid)	署名 ID	200127
Header (eventName)	説明	NOTABLE_CHARACTERISTICS
Header (severity)	重大度	6: 警告
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

TMEF キー	説明	値
fileHash	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例: 131372
msg	詳細	例: ATSE\nDetection Name: TROJ_FAM_00004f2.TOMA\nEngine Version: 9.826.1078\nMalware Pattern Version: 11.749.92
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+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:

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 4-5. 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 (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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 5.5.0.1191

TMEF キー	説明	値
Header (eventid)	署名 ID	200120
Header (eventName)	説明	DENYLIST_CHANGE
Header (severity)	重大度	3: 情報
act	イベントの処理	Add
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
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
deviceExternalRiskType	リスクレベル	• Low • Medium • High • Confirmed Malware
dhost	送信先ホスト名	例: dhost1
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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

TMEF キー	説明	値
pComp	検出エンジン/コンポーネント	Sandbox
rt	ログ生成時刻	例: Mar 09 2015 17:05:21 GMT+08:00

ログの例:

TMEF 形式のシステムイベントログ

表 4-6. TMEF 形式のシステムイベントログ

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventid)	イベント ID	• 300102 • 300999
Header (eventName)	説明	• PRODUCT_UPDATE • SYSTEM_EVENT
Header (severity)	重大度	3: 情報
dvc	アプライアンスの IP アドレス	例: 192.168.10.1
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

TMEF キー	説明	値
rt	イベントのログ記録日時	例: Mar 03 2016 16:28:20 GMT+08:00
cs1Label	イベントの種類のラベル	eventType
cs1	イベントの種類	• System Setting • Account Logon/Logoff • Logoff System Update
duser	ユーザ名	例: admin
msg	詳細	例: Updates: Component update settings modified by 'admin' from 192.168.10.2.
src	送信元 IPv4 アドレス	例: 192.168.100.100
c6a2Label	IPv6 アドレスのラベル	srcIPv6
c6a2	IPv6 アドレス	例: 2001:db8::1
shost	送信元ホスト名	例: shost1
outcome	結果のステータス	• Success • Failure

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300999
|SYSTEM_EVENT|3|rt=Nov 07 2017 10:05:58 GMT+00:00 dvc=10.204
.1.1 dvchost=DDAN deviceMacAddress=00:0C:29:2F:3B:6B deviceG
UID=423E63AA-D466-406E-A15F-6AC6F3CEE50A cs1Label=eventType
cs1=System Setting duser=admin src=10.204.1.2 msg=Log Settin
gs: Settings modified by 'admin' from 10.204.1.2 outcome=Suc
cess
```

TMEF 形式のアラートイベントログ

表 4-7. TMEF 形式のアラートイベントログ

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 6.0.0.1001
Header (eventid)	イベント ID	300105
Header (eventName)	説明	ALERT_EVENT
Header (severity)	重大度	• 2: 情報 • 6: 重要 • 8: 重大
dvc	アプライアンスの IP アドレス	例: • IPv4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
deviceMacAddress	アプライアンスの MAC アドレス	例: 00:0D:60:AF:1B:61
dvchost	アプライアンスのホスト名	例: DDAN
deviceGUID	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	イベントのログ記録日時	例: Mar 03 2016 16:28:20 GMT+08:00
ruleName	ルール名	例: High Memory Usage
cs1Label	影響を受けるアプライアンスのラベル	affectedAppliance

TMEF キー	説明	値
cs1	影響を受けるアプライアンス	例: DDAN.com (10.204.1.2 | FE80:: 29FF:29FF: 29FF: 29FF)
cs2Label	件名のラベル	subject
cs2	件名	例: DDAN Important Alert - High Memory Usage
cs3Label	メッセージのラベル	ruleContent
cs3	メッセージ	メッセージの内容

ログの例:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300105
|ALERT_EVENT|6|rt=Nov 07 2017 08:39:54 GMT+00:00 dvc=10.204.
1.1 dvchost=DDAN deviceMacAddress=00:0C:29:2F:3B:6B deviceGU
ID=423E63AA-D466-406E-A15F-6AC6F3CEE50A ruleName=High CPU Us
age cs1Label=affectedAppliance cs1=DDAN ( 10.204.1.1 | FE80:
:20C:29FF:FE2F:1B6B ) cs2Label=subject cs2=DDAN Important Al
ert - High CPU Usage cs3Label=ruleContent cs3=The average CP
U usage in the last 5 minutes exceeded the threshold of 90%.
\n\nAverage CPU usage: 96%\nAffected appliance: DDAN (10.204
.1.1 | FE80::20C:29FF:FE2F:1B6B)\n\nReduce the number of Vir
tual Analyzer instances, or add a secondary appliance to imp
rove performance.\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\
=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\nAlert time: 2017-11-07 08:3
9:54\nManagement console: https://10.204.1.1/ | https://[FE8
0::20C:29FF:FE2F:1B6B]/
```

TMEF 形式の ICAP 事前検索による検出ログ

表 4-8. TMEF 形式の ICAP 事前検索による検出ログ

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 Analyzer
Header (pver)	アプライアンスのバージョン	例: 7.1.0.1088
Header (eventName)	イベント名	ICAP_PRESCAN_EVENT
Header (severity)	リスクレベル	8
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
rt	ログ生成時刻	例: May 31 2021 15:56:04 GMT+08:00
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:56:B3:57
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	SHA1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF bitmap file
fname	ファイル名	例: excel.rar

TMEF キー	説明	値
sha256	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cn1Label	サンプルの種類	sampleType
cn1	サンプルの種類	• 0: ファイルのサンプル • 1: URL のサンプル
request	URL	例: http://example.com:80/
malName	不正プログラム名	例: HEUR_NAMETRICK.A
src	送信元 IPv4 アドレス	例: 10.1.144.199
dst	送信先 IPv4 アドレス	例: 10.1.144.198
cs1Label	submitterName	malName
cs1	ICAP クライアント	例: 10.205.190.3
cs2Label	icapMode	
cs2	ICAP モード	
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
cs2Label	submitterName	例: • REQMOD:ICAP 要求の変更方法 • RESPMOD:ICAP 応答の変更方法
cs3Label	送信元ユーザ	

TMEF キー	説明	値
cs3	ICAP クライアントにより送信された X-Authenticated-User ICAP ヘッダ	例: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)
cs4Label	検出元	
cs4	オブジェクトを処理した検出モジュールの名前	例: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)
cs5Label	sha256	

TMEF キー	説明	値
cs5	SHA256	例: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

ログの例:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:36:08 GMT+00:00 d
vc=10.204.191.52 dvchost=DDAN deviceMacAddress=00:50:56:98
:33:69 deviceGUID=627EE441-DD62-4483-B9E4-60B3C8A92529 src
=10.2.11.122 cn1Label=sampleType cn1=1 fileHash=317D137FE5
90EE561648ECA137CB2B6898526115 request=http://wrs21.test.c
om:80/ malName=TSPY_KEYLOG.GC cs1Label=submitterName cs1=1
0.204.190.6 cs2Label=icapMode cs2=REQMOD cs3Label=sourceUs
er cs4Label=identifiedBy cs4=Web Reputation Services cs5La
bel=sha256 cs5=F5C748A953D23B8CE4F5C792FDC1E7987471DD48FE2
4ABA07C3CFD10B4AEF72F
```

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:36:11 GMT+00:00 d
vc=10.204.191.52 dvchost=DDAN deviceMacAddress=00:50:56:98
:33:69 deviceGUID=627EE441-DD62-4483-B9E4-60B3C8A92529 dst
=10.2.1.123 src=10.2.1.122 cn1Label=sampleType cn1=0 fname
=3-layer.zip fileType=ZIP archive fileHash=D7273555CB0AC08
303415CBEB3F3D72DD0893BC4 request=http://test.com/3-layer.
zip malName=Eicar_test_file,TROJ_OLEXP.TPD cs1Label=submit
terName cs1=10.204.190.6 cs2Label=icapMode cs2=RESPMODE cs
3Label=sourceUser cs4Label=identifiedBy cs4=Advanced Threa
t Scan Engine cs5Label=sha256 cs5=08F18BC62297A67DD91E192A
27C1EEDE3C1BBEE19A90FC0B1FADD07CE93B9823
```

索引