Deep Discovery™ Director

Syslog コンテンツマッピングガイド

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

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

商標について

P/N: APEM59260/210318_JP (2021/08)

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 Director 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 Director における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

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

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

目次

はじめに

本書について

Trend Micro Deep Discovery Director Syslog コンテンツマッピングガイドをお読みいただきありがとうございます。次の項目を参照してください。

ドキュメント

Deep Discovery Director 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 Director を設定して管理する方法の詳細な手順、および Deep Discovery Director の概念や機能に関する説明が記載されています。
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 Director 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。
Automation API Guide	Deep Discovery Director オートメーション API の使用方法を説明する PDF ドキュメントです。
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 Director 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 Director のコンポーネントと機能、Deep Discovery Director を設定するために必要な手順が説明されています。
サポートポータル	サポートポータルは、問題の解決およびトラブルシューティングの情報を参照できるオンラインデータベースです。製品の既知の問題に関する最新の情報を得ることができます。サポートポータルにアクセスするには、以下の Web サイトをご覧ください。 https://success.trendmicro.com/jp/technical-support

対象読者

この Deep Discovery Director 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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

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

トレンドマイクロについて

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

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

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

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

第 1 章

はじめに

Syslog コンテンツマッピングガイドには、ログの管理基準や、Trend Micro Deep Discovery Director 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 Director 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、15 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。	CEF は 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 Director 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、47 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 Director では LEEF ディクショナリのサブセットを使用します。

第 2 章

Syslog コンテンツマッピング - CEF

次の各表は、Deep Discovery Director 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。

- Deep Discovery Director の不審オブジェクトのリスト:
  - 17 ページの「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」
- Deep Discovery Inspector の検出ログ:
  - 19 ページの「CEF 形式の脅威ログ」
  - 24 ページの「CEF 形式の要注意アプリケーションログ」
  - 27 ページの「CEF 形式の Web レピュテーションログ」
- Deep Discovery Email Inspector のログ:
  - 31 ページの「CEF 形式の検出ログ: メール検出ログ」
  - 34 ページの「CEF 形式の検出ログ: 添付ファイル検出ログ」
  - 36 ページの「CEF 形式の検出ログ: URL 検出ログ」
  - 37 ページの「CEF 形式のメッセージ追跡ログ」
- 仮想アナライザの分析ログ:
  - 40 ページの「CEF 形式の仮想アナライザ分析ログ: ファイル分析イベント」

CEF 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 2-1. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	200120
Header (eventName)	説明	Deny List updated
Header (severity)	重大度	3 (固定値)
act	イベントの処理	• Add • 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
cs2Label	リスクレベル	RiskLevel
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

CEF キー	説明	値
dhost	送信先ホスト名	例: dhost1
dpt	送信先ポート	1〜65535 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 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104300
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	例: http://1.2.3.4/query?term=value
rt	分析時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200120|Deny List updated|3|rt=1593761104000 d
vc=192.168.156.239 dvchost=ddd3-239 dvcmac=00:0c:30:05:a0:8b d
eviceExternalId=FA68DBC5-D354-444C-A834-60352F1A4027 cs1Label=
type cs1=Deny List Domain end=1593761104300 act=Add dhost=mt6x
.ejvu50k.6x.org cs2Label=RiskLevel cs2=Medium
```

CEF 形式の脅威ログ

表 2-2. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
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 • 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

CEF キー	説明	値
c6a4Label	ピア IPv6 アドレス	PeerIPv6
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	CCCA_Detection
cn3	脅威の種類	0〜4 の値 • 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 • VIRTUAL_ANALYZER • USER_DEFINED
cs5Label	CCCA ログの検出元	CCCA_DetectionSource
cs6	攻撃段階	例: • 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、1、または 2 • 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

CEF キー	説明	値
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	1〜65535 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	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
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

CEF キー	説明	値
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
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 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000
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	1〜65535 の値
suid	ユーザ名	例: User1
suser	メール送信者	例: suser1

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|0|Eicar_test_file - HTTP (Response)|8|dvc=172
.22.9.32 dvcmac=00:50:56:AD:03:BD dvchost=localhost deviceExte
rnalId=E9A3FA433916-4738984C-A4BF-84A0-D603 rt=1593761104000 a
pp=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=eicarco
m2.zip fileType=262340608 fsize=308 requestClientApplication=W
get/1.12 (linux-gnu) act=not blocked cn3Label=Threat Type cn3=
0 destinationTranslatedAddress=172.22.9.5 fileHash=BEC1B52D350
D721C7E22A6D4BB0A92909893A3AE cs4Label=FileNameInArchive cs4=e
icar.com sourceTranslatedAddress=172.22.9.54 cnt=1 cat=Malware
cs6Label=pAttackPhase cs6=Point of Entry flexNumber1Label=vLAN
Id flexNumber1=4095 request=http://172.22.9.54/eicarcom2.zip d
evicePayloadId=0:143:P
```

CEF 形式の要注意アプリケーションログ

表 2-3. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	100120
Header (eventName)	説明	Deep Discovery Inspector により、このプロトコルが監視対象ネットワークで検出されました。
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

CEF キー	説明	値
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
cnt	総数	PeerIPv6
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、1、または 2 • 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

CEF キー	説明	値
dpt	送信先ポート	1〜65535 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
flexNumber1	vLANId	例: 4095
flexNumber1Label	vLANId	vLANId
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000
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	1〜65535 の値
src	送信元 IP アドレス	例: 10.1.144.199

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100120|Deep Discovery Inspector detected the
protocol in your monitored network.|2|dvc=172.22.9.32 dvcmac=0
0:50:56:AD:03:BD dvchost=localhost deviceExternalId=E9A3FA4339
16-4738984C-A4BF-84A0-D603 rt=1593761104000 app=eDonkey device
Direction=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=3993
3 smac=00:30:da:2d:47:32 cn3Label=Threat Type cn3=6 sourceTran
slatedAddress=10.1.117.231 destinationTransla tedAddress=10.1.
```

```
100.223 cnt=1 flexNumber1Label=vLANId flexNum ber1=4095 device
PayloadId=6:11:P
```

CEF 形式の Web レピュテーションログ

表 2-4. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント 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

CEF キー	説明	値
c6a4	ピア IPv6 アドレス	例: 2001:0:0:1::21
c6a4Label	ピア IPv6 アドレス	PeerIPv6
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、1、または 2 • 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	1〜65535 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

CEF キー	説明	値
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000
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	1〜65535 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:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100101|Ransomware URL in Web Reputation Servi
ces database - HTTP (Request)|8|dvc=172.22.9.32 dvcmac=00:50:5
6:AD:03:BD dvchost=localhost deviceExternalId=E9A3FA433916-473
8984C-A4BF-84A0-D603 rt=1593761104000 cs3Label=HostName_Ext cs
3=ca95-1.winshipway.com cn2Label=WRSScore cn2=49 cn3Label=Thre
at 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 sourceTranslatedAddre
ss=172.22.9.5 cn1Label=CCCA_Detection cn1=1 request=http://ca9
5-1.winshipway.com/ requestClientApplication=Wget /1.12 (linux
-gnu) app=HTTP deviceDirection=1 dhost=150.70.1 62.115 dst=150
.70.162.115 dpt=80 cs2Label=URLCategory cs2=Ransomware destina
tionTranslatedAddress=150.70.162.115 cs4Label=pAttackPhase cs4
=Command and Control Communication flexNumber1Label=vLANId fle
xNumber1=4095 request=http://ca95-1.winshipway.com/ devicePayl
oadId=5:17:
```

CEF 形式の検出ログ: メール検出ログ

表 2-5. CEF 形式の検出ログ: メール検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダ	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	100130
Header (eventName)	説明	EMAIL_DETECTION
Header (severity)	メールの重大度	• 2: 使用不可 • 4: 低 • 6: 中 • 8: 高
act	イベントの処理	例: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized

CEF キー	説明	値
cn1	脅威の種類	• 1: 標的型不正プログラム • 2: 不正プログラム • 3: 不正 URL • 4: 不審ファイル • 5: 不審 URL • 6: スパムメール/グレーメール • 7: フィッシング • 8: コンテンツ違反 • 9: 情報漏えい対策イベント
cn1Label	脅威の種類	threatType
cn2	メールのサイズ	例: 30841
cn2Label	メールのサイズ	msgSize
cs1	メールで検出された脅威の名前	例: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	メールで検出された脅威の名前	threats
cs2	内部メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	内部メールの ID	msgUuid
cs3	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	メール ID	messageId
cs4	送信者のメールアドレス	例: user1@example.com
cs4Label	送信者のメールアドレスのラベル	senderMail

CEF キー	説明	値
cs5	受信者のメールアドレス	例: user2@example.com
cs5Label	受信者のメールアドレスのラベル	rcptMail
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	メール受信者	例: user1@example2.com;test@163.com
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
msg	メールの件名	例: hello
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000
src	送信元 IP アドレス	例: 10.1.144.199
suser	メール送信者	例: user2@example.com

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100130|EMAIL_DETECTION|6|rt=1593761104000 src
=150.70.186.134 cs3Label=messageId cs3=<20150323115314.BCA2C91
68EA@internalbeta.bcc.ddei> deviceExternalId=c425624a-e9db-4f3
f-8088-2726f15e6587 act=passed dvchost=internalbeta.bcc.ddei d
vc=10.64.1.131 duser=user1@domain1.com;user2@domain1.com;user3
@domain1.com msg=Virus_Report-20150323_02:00 cn2Label=msgSize
cn2=83878 cn1Label=threatType cn1=3 suser=user@domain2.com dvc
mac=C4:34:6B:B8:09:BC cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-
```

```
BCEE-6BB5EC111FE7 cs1Label=threats cs1=PUA_Test_File|TROJ_GEN.
R04AC0PAH15|PAK_Generic.005|ADW_DOWNLOADER.WRS|LOW-REPUTATION-
URL_BLOCKED-LIST.SCORE.WRS|LOW-REPUTATION-URL_BLOCKED-LIST.SCO
RE.WRS|TROJ_GEN.R02SC0OLH14|TROJ_GENERIC.WRS|TROJ_DOWNLOADER.W
RS
```

CEF 形式の検出ログ: 添付ファイル検出ログ

表 2-6. CEF 形式の検出ログ: 添付ファイル検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダ	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	100131
Header (eventName)	説明	ATTACHMENT_DETECTION
Header (severity)	重大度	• 2: 使用不可 • 4: 低 • 6: 中 • 8: 高
cs1	脅威の名前	例: VAN_BOT.UMXX
cs1Label	脅威の名前	threats
cs2	内部メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	内部メールの ID	msgUuid
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	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例:131372
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100131|ATTACHMENT_DETECTION|6|rt=159376110400
0 fileHash=E49395FEACC12A5613E7BA6C69AC5E42EDFDA42D fsize=1768
1 fileType=MIME Base64 dvchost=internalbeta.bcc.ddei dvc=10.64
.1.131 deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 c
s2Label=msgUuid cs2=E89A23BE-11F5-2505-BCEE-21027D078154 fname
=3C761B45-626D-4E75-B4782FD0E5E8369C.eml dvcmac=C4:34:6B:B8:09
:BC cs1Label=threats cs1=TROJ_UP.258A1A7D
```

CEF 形式の検出ログ: URL 検出ログ

表 2-7. CEF 形式の検出ログ: URL 検出ログ

CEF キー	説明	値
Header (logVer)	CEF 形式のバージョン	CEF: 0
Header (vendor)	アプライアンスのベンダ	Trend Micro
Header (pname)	アプライアンス製品	Deep Discovery Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	100132
Header (eventName)	説明	URL_DETECTION
Header (severity)	メールの重大度	• 4: 低 • 6: 中 • 8: 高
cat	カテゴリ	例: 90:02
cs1	脅威の名前	例: LOW-REPUTATION-URL_MALWARE.WRS
cs1Label	脅威の名前	threats
cs2	内部メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	内部メールの ID	msgUuid
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost

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
request	URL	例: http://www.example.com/?utm_campaign=4-21-2014 | http://example.com/eloquaimage
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100132|URL_DETECTION|6|rt=1593761104000 cs2La
bel=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB5EC111FE7 dvcmac=C4
:34:6B:B8:09:BC dvchost=internalbeta.bcc.ddei request=http://w
ww.alltobid.com/guopai/upload/dan201401.zip d vc=10.64.1.131 d
eviceExternalId=c425624a-e9db-4f3f-8088-2726f 15e6587
```

CEF 形式のメッセージ追跡ログ

表 2-8. CEF 形式のメッセージ追跡ログ

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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	100136
Header (eventName)	説明	MESSAGE_TRACKING

CEF キー	説明	値
Header (severity)	メールの重大度	• 2: 使用不可 • 2: 未評価 • 2: 正常 • 4: 低 • 6: 中 • 8: 高
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
dvchost	アプライアンスのホスト名	例: localhost
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	ログ生成時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000
cs1Label	メール ID のラベル	messageId
cs1	メール ID	例: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	内部メールの ID	msgUuid
cs2	内部メールの ID	例: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	メール送信者	例: user2@example.com
duser	メール受信者	例: user1@example2.com;test@163.com

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

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100136|MESSAGE_TRACKING|2|rt=1593761104000 cs
3Label=latestStatus cs3=Delivery unsuccessful dvchost=localhos
t.localdomain deviceExternalId=9ceb7be2-3ec5-4b80-8697-6b4913e
b044b dvc=10.204.63.177 duser=test@test.com dvcmac=00:50:56:A7
```

```
:5F:AD reason=host 10.204.253.179[10.204.253.179] said: 552 te
st@test.com mailbox full (in reply to end of DATA command) cs1
Label=messageId cs1=20180427025553.4D771D6135F@localhost.local
domain cs4Label=senderMail cs4=marks@relay.ddei.com suser=fake
@test.test msg=plain_text_upper_case.HTML/HTM cs2Label=msgUuid
cs2=EB715918-6ACB-A405-BF46-56F53CE3FD86 cs6Label=procHistory
cs6=Apr 27 2018 02:55:53 GMT+00:00 Received,Apr 27 2018 02:55:
53 GMT+00:00 Sent for analysis,Apr 27 2018 02:56:48 GMT+00:00
Action set to 'pass',Apr 27 2018 02:56:48 GMT+00:00 Delivery u
nsuccessful,Reason:host 10.204.253.179[10.204.253.179] said: 5
52 test@test.com mailbox full (in reply to end of DATA command
)
```

CEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

表 2-9. CEF 形式の仮想アナライザ分析ログ: ファイル分析イベント

CEF キー	説明	値
Header (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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント 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	• 0: GRID が無害と知らない • 1: GRID が無害と知っている
cn1Label	GRID/CSSS の結果	GRIDIsKnownGood

CEF キー	説明	値
cn2	ROZ レーティング	例: 3: リスク高
cn2Label	ROZ レーティング	ROZRating
cn3	PCAP 使用可能	• 0: PCAP が使用不可能 • 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
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar

CEF キー	説明	値
fsize	ファイルサイズ	例:131372
rt	分析時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200119|Sample file sandbox analysis is finish
ed|3|rt=1593761104000 dvc=10.64.1.131 dvchost=internalbeta.bcc
.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a-e9db-
4f3f-8088-2726f15e6587 fname=Wonga Express Loan Promtion 3.5%
Offer.doc fileHash=A46E1F56969DECC5FEAF120A2279946A2F42D619 fi
leType=MS Office fsize=53760 cs1Label=SandboxImageType cs1=win
81en cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=1
cs2Label=MalwareName cs2=VAN_MALWARE.UMXX cn3Label=PcapReady c
n3=1
```

CEF 形式の仮想アナライザ分析ログ: URL 分析イベント

表 2-10. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	200126

CEF キー	説明	値
Header (eventName)	説明	URL sandbox analysis is finished
Header (severity)	重大度	3
cn2	ROZ レーティング	例: 3: リスク高
cn2Label	ROZ レーティング	ROZRating
cn3	PCAP 使用可能	• 0: PCAP が使用不可能 • 1: PCAP が使用可能
cn3Label	PCAP 使用可能	PcapReady
cs1	サンドボックスイメージの種類	例: win7
cs1Label	サンドボックスイメージの種類	SandboxImageType
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	例: http://www.example.com/?utm_campaign=4-21-2014 | http://example.com/eloquaimage
rt	分析時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200126|URL sandbox analysis is finished|3|rt=
1593761104000 dvc=10.64.1.131 dvchost=internalbeta.bcc.ddei dv
cmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a-e9db-4f3f-808
8-2726f15e6587 request=http://paypal-world.ga/home/? fileHash=
5EA358C987D1FDE34957B9A36AF38321C5F37D8B cs1Label=SandboxImage
Type cs1=win81en cn2Label=ROZRating cn2=3 cn3Label=PcapReady c
n3=1
```

CEF 形式の仮想アナライザ分析ログ: 著しい特性イベント

表 2-11. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventid)	イベント ID	200127
Header (eventName)	説明	Notable Characteristics of the analyzed sample
Header (severity)	重大度	6
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

CEF キー	説明	値
cs2Label	違反イベントの分析	PolicyName
deviceExternalId	アプライアンスの GUID	例: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	アプライアンスの IP アドレス	例: 10.1.144.199
dvchost	アプライアンスのホスト名	例: localhost
dvcmac	アプライアンスの MAC アドレス	例: 00:0C:29:6E:CB:F9
fileHash	SHA-1	例: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	実際のファイルタイプ	例: RIFF ビットマップファイル
fname	ファイル名	例: excel.rar
fsize	ファイルサイズ	例:131372
msg	詳細	例: Process ID:3020\n Image Path:%ProgramFiles%\\Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 / prefetch:2
rt	分析時刻 形式: UNIX タイムスタンプ (1970 年 1 月 1 日 (UTC) からのミリ秒数)	例: 1593761104000

ログの例:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200127|Notable Characteristics of the analyze
d sample|6|rt=1593761104000 dvc=10.64.1.131 dvchost=internalbe
ta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a
-e9db-4f3f-8088-2726f15e6587 fname=http://bsjv.tk/bbb/bbb/bbb
fileHash=2D302EEEF703CBB8713B806B3C5B4B3A2A28E92A fileType=URL
```

```
fsize=0 cs1Label=PolicyCategory cs1=Process, service, or memor
y object change msg=Process ID: 3020\n Image Path: %ProgramFil
es%\\Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921
/prefetch:2 cs2Label=PolicyName cs2=Creates process
```

第 3 章

Syslog コンテンツマッピング - LEEF

次の各表は、Deep Discovery Director 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。

- Deep Discovery Director の不審オブジェクトのリスト:
  - 48 ページの「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」
- Deep Discovery Inspector の検出ログ:
  - 50 ページの「LEEF 形式の脅威ログ」
  - 57 ページの「LEEF 形式の要注意アプリケーションログ」
  - 60 ページの「LEEF 形式の Web レピュテーションログ」
  - 64 ページの「LEEF 形式の相関関係のあるインシデントログ」

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 3-1. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
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
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	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	1〜65535 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: 10.1.96.147

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	検出元	• Sandbox • UDSO
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。

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|DENYLIST_CHANGE|devTime=Apr 01 2019 18:26:
11 GMT+08:00<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=
3<009>dvc=10.1.96.147<009>dvchost=DDD-IB-int<009>deviceMacAddr
ess=00:50:56:A3:CE:81<009>deviceGUID=C4BD2B76-6C3D-416E-AB0C-6
FA204D00FBC<009>end=Jan 19 2038 11:14:07 GMT+08:00<009>act=Add
<009>type=Deny List File SHA1<009>fileHash=BF378BF908A802DEADF
A9CB9FA0C02955C904F08<009>deviceExternalRiskType=High<009>pCom
p=Sandbox
```

LEEF 形式の脅威ログ

表 3-2. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventName)	イベント名	• MALWARE_DETECTION • MALWARE_OUTBREAK_DETECTION • SECURITY_RISK_DETECTION
origin	ログの取得元となった Deep Discovery アプライアンス	Inspector
act	イベントの処理	• blocked • 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	ボットのコマンド	例: COMMIT
botUrl	ボットの URL	例: example.com
cccaDestination	CCCA アドレス	例: 10.1.144.199
cccaDestinationFormat	CCCA の種類	• IP_DOMAIN • IP_DOMAIN_PORT • URL • EMAIL

LEEF キー	説明	値
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
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

LEEF キー	説明	値
deviceRiskConfidenceLevel	判定の確実性	• 1: 高 • 2: 中 • 3: 低 • 0: 未定義
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	1〜65535 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

LEEF キー	説明	値
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: 10.1.96.147
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	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
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	注目する 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

LEEF キー	説明	値
msg	説明	例: HEUR_NAMETRICK.A - SMTP (Email)
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	検出エンジン/コンポーネント	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

LEEF キー	説明	値
ruleId	ルール ID	例: 52
sAttackPhase	二次攻撃段階	例: Point of Entry
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	1〜65535 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

LEEF キー	説明	値
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
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	VLANID	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。

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|SECURITY_RISK_DETECTION|origin=Inspector<0
09>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>ptype=IDS<009>dvc=
10.1.105.120<009>deviceMacAddress=00:50:56:B6:FE:C0<009>dvchos
t=twddiv-120<009>deviceGUID=92A12204F15F-48B59215-C17B-C516-B2
CB<009>devTime=Apr 01 2019 10:24:45 GMT+00:00<009>sev=8<009>pr
otoGroup=TCP<009>proto=TCP<009>vLANId=4095<009>deviceDirection
=1<009>dhost=2.2.2.2<009>dst=2.2.2.2<009>dstPort=443<009>dstMA
C=58:35:d9:de:4a:42<009>shost=10.1.117.172<009>src=10.1.117.17
2<009>srcPort=35702<009>srcMAC=00:08:e3:ff:fd:90<009>malName=U
SR_SUSPICIOUS_IP.UMXX<009>malType=MALWARE<009>fileType=-65536<
009>fsize=0<009>ruleId=729<009>msg=Callback to IP address in C
ontrol Manager and Deep Discovery Director User-Defined Suspic
ious Objects list<009>deviceRiskConfidenceLevel=1<009>pComp=CA
```

```
V<009>riskType=1<009>srcGroup=My Company/TW 12F<009>srcZone=1<
009>dstZone=0<009>detectionType=1<009>act=not blocked<009>thre
atType=1<009>interestedIp=10.1.117.172<009>peerIp=2.2.2.2<009>
cnt=5<009>aggregatedCnt=1<009>cccaDestinationFormat=IP_DOMAIN<
009>cccaDetectionSource=USER_DEFINED<009>cccaRiskLevel=3<009>c
ccaDestination=2.2.2.2<009>cccaDetection=1<009>evtCat=Callback
<009>evtSubCat=Bot<009>aptRelated=0<009>pAttackPhase=Command a
nd Control Communication
```

LEEF 形式の要注意アプリケーションログ

表 3-3. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventName)	イベント名	DISRUPTIVE_APPLICATION_DETECTION
origin	ログの取得元となった Deep Discovery アプライアンス	Inspector
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

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	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	1〜65535 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: 10.1.96.147
dvchost	アプライアンスのホスト名	例: localhost
interestedIp	注目する IP	例: 10.1.144.199
msg	説明	例: HEUR_NAMETRICK.A - SMTP (Email)
pComp	検出エンジン/コンポーネント	例: VSAPI
peerIP	ピア IP アドレス	例: 10.1.144.199

LEEF キー	説明	値
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
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	1〜65535 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	VLANID	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。

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|DISRUPTIVE_APPLICATION_DETECTION|origin=In
spector<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>dvc=10.20
1.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=d
di38-143<009>deviceGUID=6B593E17AFB7-40FBBB28-A4CE-0462-A536<0
09>ptype=IDS<009>devTime=Mar 09 2015 14:20:38 GMT+08:00<009>se
v=2<009>protoGroup=STREAMING<009>proto=WMSP<009>vLANId=4095<00
9>deviceDirection=1<009>dhost=12.190.48.13<009>dst=12.190.48.1
3<009>dstPort=80<009>dstMAC=00:17:9a:65:f3:05<009>shost=192.16
8.33.2<009>src=192.168.33.2<009>srcPort=35125<009>srcMAC=00:16
:6f:a1:3d:7a<009>msg=Deep Discovery Inspector detected the pro
tocol in your monitored network.<009>pComp=CAV<009>threatType=
6<009>srcGroup=Default<009>srcZone=1<009>dstZone=0<009>interes
tedIp=192.168.33.2<009>peerIp=12.190.48.13<009>cnt=1<009>aggre
gatedCnt=1
```

LEEF 形式の Web レピュテーションログ

表 3-4. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventName)	イベント名	WEB_THREAT_DETECTION
origin	ログの取得元となった Deep Discovery アプライアンス	Inspector
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
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	1〜65535 の値

LEEF キー	説明	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: 10.1.96.147
dvchost	アプライアンスのホスト名	例: localhost
hostName	ホスト名	例: CLIENT1
interestedIp	注目する 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	検出エンジン/コンポーネント	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

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	1〜65535 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
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	VLANID	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。

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|WEB_THREAT_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=6B593E17A
FB7-40FBBB28-A4CE-0462-A536<009>ptype=IDS<009>devTime=Mar 09 2
015 14:06:36 GMT+08:00<009>sev=6<009>protoGroup=HTTP<009>proto
=HTTP<009>vLANId=4095<009>deviceDirection=1<009>dhost=www.free
webs.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>sr
cPort=12121<009>srcMAC=fe:ed:be:ef:5a:c6<009>hostName=www.free
webs.com<009>msg=Dangerous URL in Web Reputation Services data
base - 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
>threatType=5<009>interestedIp=172.16.1.197<009>peerIp=216.52.
115.2
```

LEEF 形式の相関関係のあるインシデントログ

表 3-5. 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 Director
Header (pver)	アプライアンスのバージョン	例: 5.3.0.1212
Header (eventName)	イベント名	SUSPICIOUS_BEHAVIOUR_DETECTION
origin	ログの取得元となった Deep Discovery アプライアンス	Inspector
data0	相関データ 0	追加の属性値
data1	相関データ 1	追加の属性値

LEEF キー	説明	値
data2	相関データ 2	追加の属性値
data3	相関データ 3	追加の属性値
data4	相関データ 4	追加の属性値
data5	相関データ 5	追加の属性値
data6	相関データ 6	追加の属性値
data7	相関データ 7	追加の属性値
data8	相関データ 8	追加の属性値
data9	相関データ 9	追加の属性値
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
dvc	アプライアンスの IP アドレス	例: 10.1.96.147
dvchost	アプライアンスのホスト名	例: localhost
interestedHost	注目すべきホスト名	例: example.net
interestedIp	注目する IP	例: 10.1.144.199
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

LEEF キー	説明	値
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	検出エンジン/コンポーネント	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。

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|SUSPICIOUS_BEHAVIOUR_DETECTION|origin=Insp
ector<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>deviceMacAd
dress=00:0C:29:A6:53:0C<009>dvchost=ddi38-143<009>pComp=Correl
ation<009>dvc=10.201.156.143<009>ptype=IDS<009>deviceGUID=D2C1
D6D20FF8-4FC98F92-25EB-D7DA-AF0E<009>devTime=Mar 11 2015 22:05
```

```
:50 GMT-04:00<009>sev=2<009>interestedIp=172.16.0.100<009>inte
restedHost=172.16.0.100<009>interestedMacAddress=00:0c:29:70:4
5:...36<009>ruleId=47<009>ruleName=This host has responded to
DNS queries.<009>threatType=Unregistered Service<009>threatNam
e=Unregistered DNS Server<009>proto=DNS Response<009>userGroup
=Default<009>deviceDirection=1
```