



Trend Micro Portable Security™ 3

サイト管理者向け SIEM (セキュリティ情報イベント管理) ツール

ユーザガイド

2022年4月1日

ドキュメントバージョン 1.18

目次

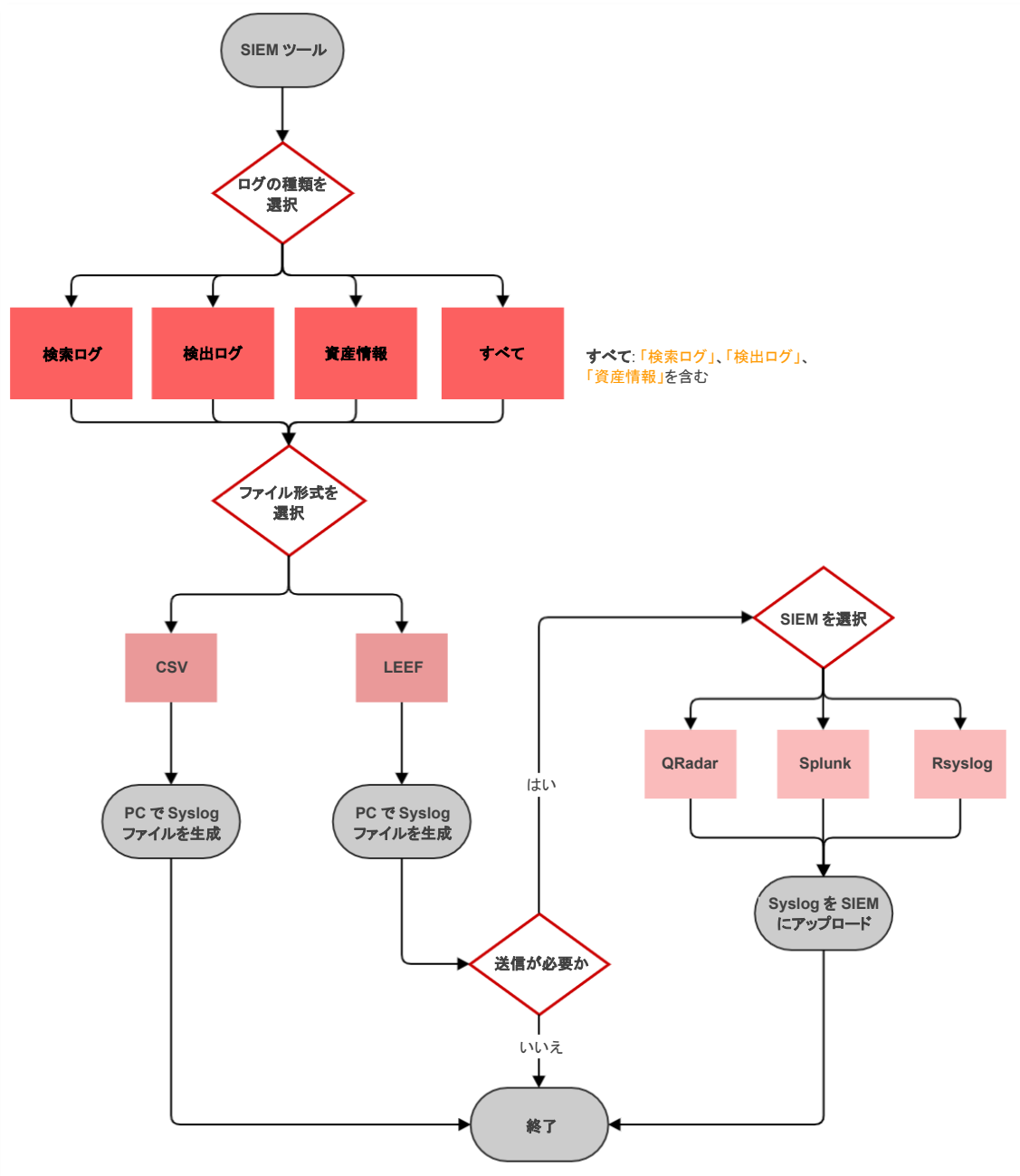
Trend Micro Portable Security™ 3	1
1. 概要	3
提供されるもの	3
SIEM ツールのフローチャート	3
2. SIEM ツールについて	4
3. 前提条件 - SIEM サーバでの設定	5
QRadar での設定	5
Splunk での設定	8
RSyslog での設定	13
4. SIEM ツールでの準備手順	13
対象環境	13
SIEM ツールの設定	13
config.ini の設定	14
5. SIEM ツールの使用方法	15
6. デバッグログの収集方法	22
7. TMPS3 ログの LEEF 形式の定義	23
LEEF 2.0 の基本形式	23
カスタムイベントキーブロック	23

1. 概要

提供されるもの

- SIEM ツールパッケージ (SIEM-tool.zip)

SIEM ツールのフローチャート



2. SIEM ツールについて

1. SIEM ツールはコマンドラインインタフェースとして設計されており、オペレータは、管理プログラムがインストールされたコンピュータから SIEM サーバにログのクエリを実行できます。
2. ログの定義: ログには「検索ログ」、「検出ログ」、および「資産情報」があります。

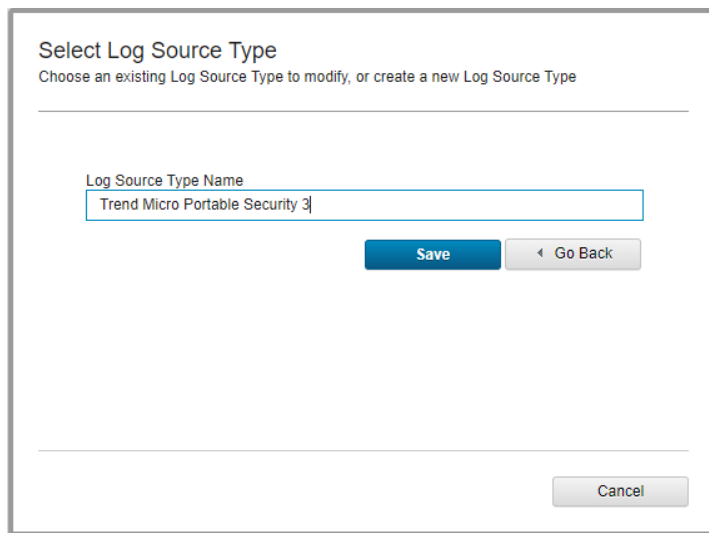
そのいずれか 1 つまたはすべてを選択して、エクスポート/送信を行うことができます。

- **検索ログ:** 検索したエンドポイントのリストとともに、脅威が検出された/検出されなかった、または検索がキャンセルされたなど、すべての結果が含まれます。
- **検出ログ:** 検索したエンドポイントのリストとともに、「脅威が検出された」結果のみが含まれます。ログファイルには、各検出が 1 列ごとに記録されます。脅威の検出されなかった結果は保存されません。
- **資産情報:** 検索したエンドポイントのリストとともに、次の 3 つのファイルを含む資産情報が含まれます。
 - **資産情報:** システムとハードウェアの情報
 - **アプリケーション情報:** インストールされているアプリケーションのリスト
 - **アップデート情報:** アップデートの情報 (Microsoft アプリケーションのみ)

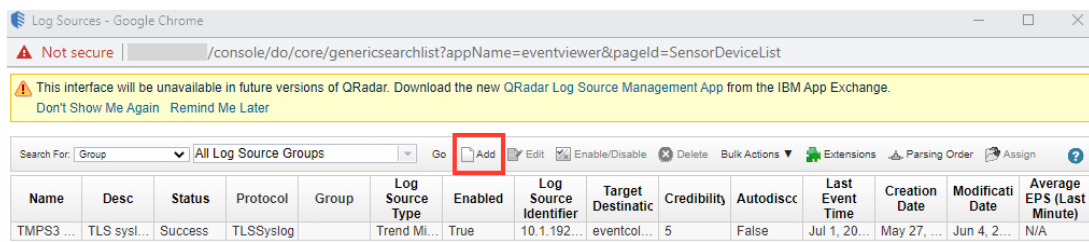
3. 前提条件 - SIEM サーバでの設定

QRadar での設定

1. ログソースタイプを作成します。
 - a. [Admin]→[DSM Editor] の順にクリックし、[Select Log Source Type] 画面で [Create New] をクリックします。
 - b. このログソースタイプの名前を指定します。



2. ログソースを作成します。
 - a. [Admin]→[Log Sources] の順にクリックし、[Log Sources] 画面で [Add] をクリックします。



Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destinat...	Credibility	Autodiscc	Last Event Time	Creation Date	Modificati...	Average EPS (Last Minute)
TMPS3 ...	TLS syst...	Success	TLSSyslog		Trend Mi...	True	10.1.192...	eventcol...	5	False	Jul 1, 20...	May 27, ...	Jun 4, 2...	N/A

- b. 他の関連情報とともに、管理プログラムがインストールされたコンピュータの IP アドレスを [Log Source Identifier] に入力します。

Log Sources - Google Chrome

Not secure | /console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&pagelId=SensorDeviceList&hasSearched=false&id=...

Edit a log source

Warning: This log source uses an undocumented protocol. IBM Support cannot troubleshoot problems with receiving event data. Events received by an undocumented protocol may be in a format unrecognized by the DSM. Use the DSM Editor to resolve any parsing issues.

Log Source Name:

Log Source Description:

Log Source Type: Trend Micro Portable Security 3

Protocol Configuration:

Log Source Identifier:

TLS Listen Port:

Authentication Mode:

Certificate Type:

Maximum Connections:

TLS Protocols:

Enabled:

Credibility:

Target Event Collector:

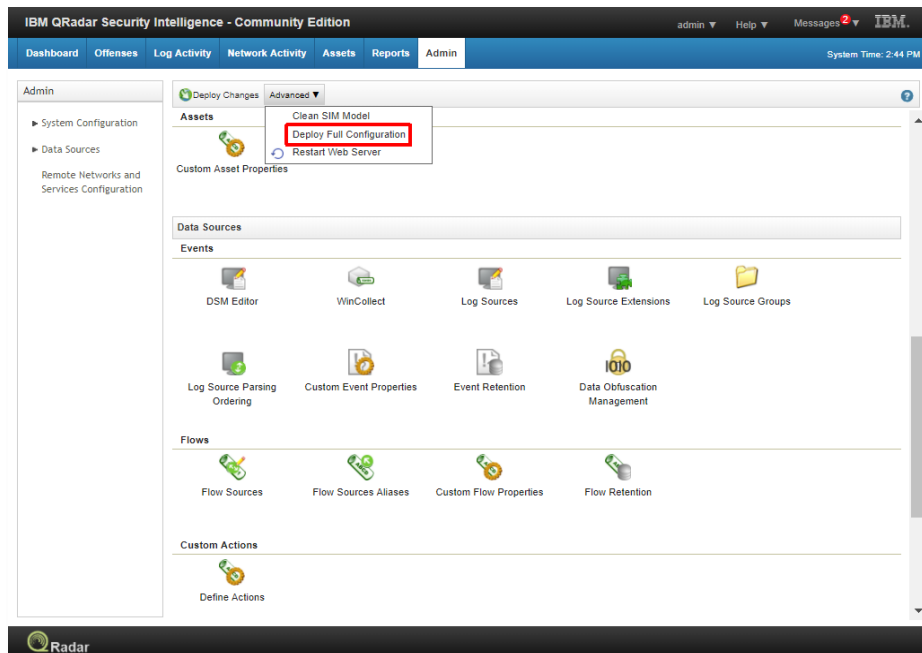
Coalescing Events:

Store Event Payload:

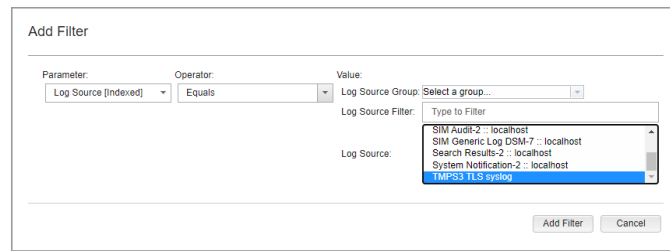
Log Source Extension:

Please select any groups you would like this log source to be a member of:

- c. 保存後、[Admin] タブに移動し、[Advanced]→[Deploy Full Configuration] の順にクリックして、作成したログソースを配信します。



3. QRadar の証明書ファイルを SIEM ツールにコピーします。
 - a. TLS 暗号化されたログを送信するには、クライアントに SIEM サーバの証明書ファイルが必要です。
 - b. QRadar の証明書ファイルは、/opt/qradar/conf/trusted_certificates にあります。
 - c. /opt/qradar/conf/trusted_certificates/syslog-tls.cert を SIEM ツールのフォルダにコピーして、config.ini に記載されている SIEM ツールのファイル名が正しいことを確認します。
4. 「[4. SIEM ツールでの準備手順](#)」を参照して、ログを QRadar に送信します。
5. QRadar に戻り、DSM エディタでログを開きます。
 - a. [Log Activity] をクリックします。
 - b. [Add Filter] をクリックして、[Parameter] に [Log Source [Indexed]] を、[Operator] に [Equals] を選択し、[Log Source] を選択して、SIEM ツールから送信されたログを表示します。

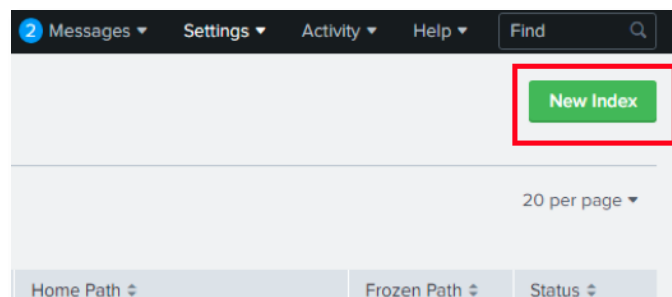
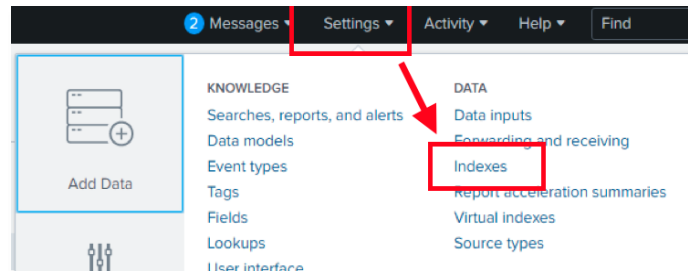


Splunk での設定

1. 検索ログ、検出ログ、および資産情報に関する 3 種類のログそれぞれに**新規インデックス**を追加します。

注意: インデックスはログと同じ名前にする必要があります。

例: scannedlog、detectedlog、assetinfo、applicationinfo、および updateinfo



New Index

General Settings

Index Name:

Index Data Type: Events Metrics

Home Path: optional

Cold Path: optional

Thawed Path: optional

Data Integrity Check: Enable Disable

Max Size of Entire Index: 500 GB

Max Size of Hot/Warm/Cold Bucket: auto GB

Frozen Path: optional

App: Search & Reporting

Storage Optimization

Tsidx Retention Policy: Enable Reduction Disable Reduction

2. 次に示す手順に従って、HTTP イベントコレクタを設定します。

The screenshot shows the Splunk Settings interface. The 'Settings' menu is open, and 'Data inputs' is highlighted with a red box. A red arrow points from 'Data inputs' to the 'HTTP Event Collector' option in the 'Local inputs' section, which is also highlighted with a red box. The 'HTTP Event Collector' description reads: 'Receive data over HTTP or HTTPS.'

2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Global Settings **New Token**

20 per page ▾

Source Type ▾	Index ▾	Status ▾
	scannedlog	Enabled

2 Messages ▾

Add Data ● ○ ○ ○
Select Source Input Settings Review Done

< Back **Next >**

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector >
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Configure a new token for receiving data over HTTP. [Learn More](#)

Name

Source name override?

Description?

Output Group (optional)

Add Data | Select Source | Input Settings | Review | Done | < Back | **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context | Search & Reporting (search) ▾

Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Select Allowed Indexes | Available item(s) | add all > | Selected item(s) < remove all

Available item(s):
detectedlog
history
main
scannedlog
summary

Selected item(s):
applicationinfo
assetinfo
detectedlog
scannedlog
updateinfo

Default Index | updateinfo ▾ | Create a new index

クリック (Click) - points to the 'scannedlog' item in the 'Available item(s)' list.

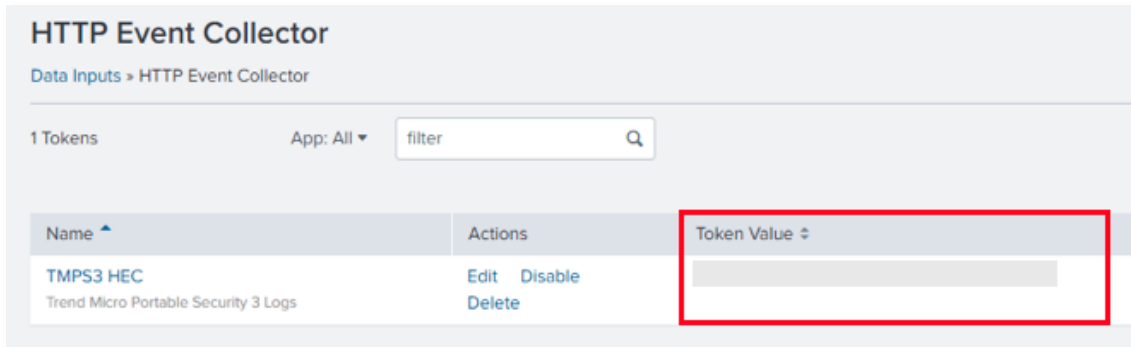
Add Data | Select Source | Input Settings | Review | Done | < Back | **Submit >**

Review

Input Type Token
Name TMPS3 HEC
Source name override N/A
Description N/A
Enable indexer acknowledg No
Output Group N/A
Allowed indexes applicationinfo
assetinfo
detectedlog
updateinfo
scannedlog

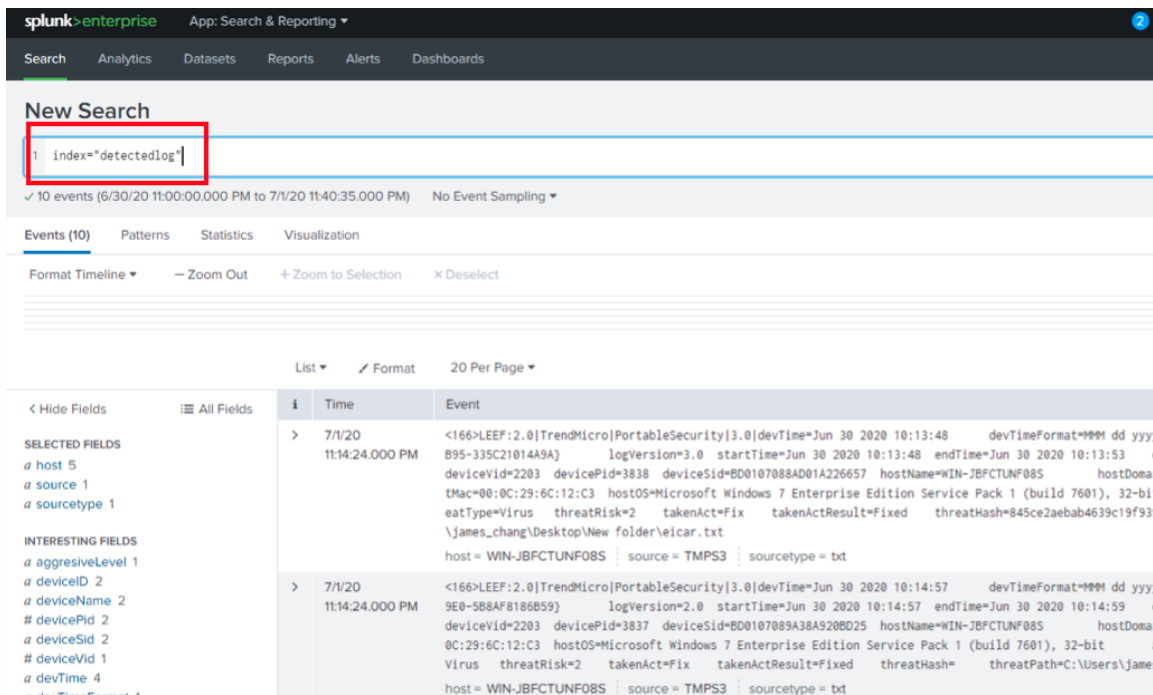
Default index updateinfo
Source Type Automatic
App Context search

- [Token Value] を config.ini ファイルの「[Splunk] Token」パラメータにコピーします。



- 「[4. SIEM ツールでの準備手順](#)」を参照して、ログを Splunk に送信します。

Splunk に戻り、作成されたインデックスを検索して、SIEM ツールから送信されたログを表示します。



RSyslog での設定

関連する修正を RSyslog 設定に記述できます。

1. Syslog メッセージの設定時に <Priority> 情報をすべての送信メッセージに含めたい場合:
\$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat ではなく、
\$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format を使用してください。
2. データの文字化けを防止するには:
\$EscapeControlCharactersOnReceive off を設定してください。

これらの設定を/etc/rsyslog.conf で修正した後、rsyslogd を再起動してください。

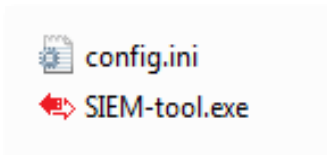
4. SIEM ツールでの準備手順

対象環境

管理プログラムがインストールされたコンピュータ

SIEM ツールの設定

1. サブフォルダとファイルを含め、**SIEM-Tool** フォルダを適切な場所に保存します (例: C:¥work¥SIEM-tool¥)。



2. **SIEM-Tool** フォルダで、**config.ini** ファイルを必要に応じて確認および修正します。
 - a. **SIEM-Tool** フォルダの **config.ini** ファイルをテキストエディタで開きます。
 - b. SIEM サーバの設定に合わせて **config.ini** を修正します。

config.ini の設定

[Section] パラメータ	説明
[General Setting]	この.ini ファイルには、初期設定がいくつか用意されています。コマンドラインインタフェースから同じオプションを指定してツールを実行すると、それらの設定が上書きされます。
Startdate	クエリを開始する日付を指定します。クエリの対象は「Startdate」から現在までです。 注意: <ol style="list-style-type: none"> この値を空にすると、管理プログラム内の最も古い記録からクエリが開始されます。 SIEM ツールから SIEM へのログの転送が完了すると、この値は自動的に更新されます。 各ログの時間は各コンピュータのローカル時間によって異なります。タイムスタンプに基づくログの転送でエラーが発生しないようにするには、各コンピュータを標準時と同期するようにします。
Facility	SIEM サーバがログのカテゴリを識別するためのファシリティコードを示す整数値です。 初期設定は LOG_LOCAL4 (20) です。
InstalledFolder	管理プログラムのインストール先が初期設定と異なる場合は、「;」記号を削除して、独自のインストール先に更新します。
Event=1xxx	「検索」ログのイベントに対する初期設定の重大度レベルです。 この各イベントの初期設定値は、ログファイル内のステータスや結果で使用され、受信イベントの重大度を識別します。
Event=2xxx	「検出」ログのイベントに対する初期設定の重大度レベルです。 この各イベントの初期設定値は、ログファイル内のステータスや結果で使用され、受信イベントの重大度を識別します。
Event=3xxx	「資産情報」ログのイベントに対する初期設定の重大度レベルです。
LeefTimeFormat	LEEF 形式の時間の形式の設定です。
[Splunk]	Splunk 向けの設定
ServerAddress	Splunk の IP アドレスまたはホスト名
ServerPort	Splunk の待機ポート
Token	Splunk との通信に使用するトークン

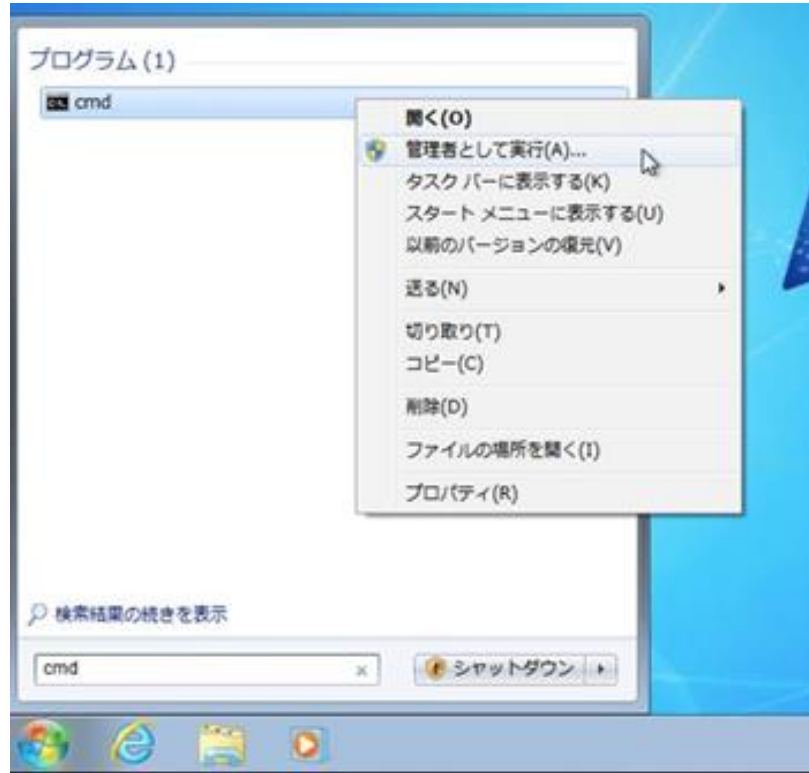
[Section] パラメータ	説明
[QRadar]	QRadar 向けの設定
ServerAddress	QRadar の IP アドレスまたはホスト名
ServerPort	QRadar の待機ポート
CertFile	QRadar との通信に使用する証明書ファイルのパス
[RSyslog]	
ServerAddress	RSyslog の IP アドレスまたはホスト名
ServerPort	RSyslog の待機ポート
Protocol	RSyslog のネットワークプロトコル (現在は UDP のみサポート)

5. SIEM ツールの使用方法

1. コマンドプロンプトを起動します。

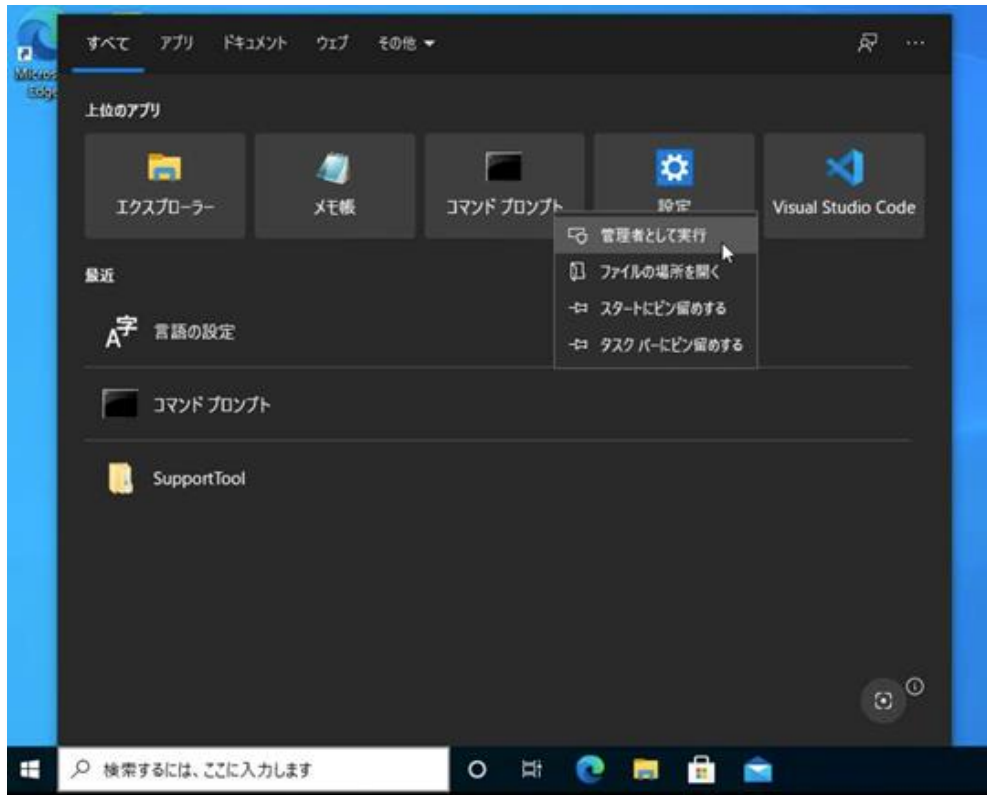
a. Windows 7 の場合

- i. キーボードで <Windows> キーを押します。
- ii. 「cmd」と入力します。
- iii. [cmd] を右クリックし、[管理者として実行] をクリックしてコマンドプロンプトを起動します。



b. Windows 10 の場合

- i. 画面下部のメニューで Windows ロゴを右クリックします。
- ii. 表示されるメニュー項目で、[コマンド プロンプト] を右クリックします。
- iii. [その他]→[管理者として実行] の順に選択して、コマンドプロンプトを起動します。



2. 現在のフォルダを、SIEM-Tool.exe が保存されているフォルダに変更します。次のとおりに入力して、<Enter> キーを押します。

```
C:¥> cd C:¥work¥SIEM-Tool
```

3. コマンドプロンプトのカーソルが、「SIEM ツール」のディレクトリに変わります。
-h オプションを指定して次の実行可能ファイル名を入力し、<Enter> キーを押して実行します。

```
C:¥work¥SIEM-Tool> SIEM-Tool.exe -h
```

4. 「ヘルプ」情報が表示されます。

```

=====
Trend Micro Portable Security 3
(c) 2020 Trend Micro Incorporated. All Rights Reserved.
=====
Usage:
  SIEM-tool.exe export --log=<log> --format=<format> [--date <from> <to>] (--
ip=<ip> | [--netmask=<netmask>]) [--hostname=<hostname>] [-d | --debug]
  SIEM-tool.exe send --siem=<siem> --log=<log> [--startdate=<startdate>] [-d |
--debug]
  SIEM-tool.exe -h | --help
  SIEM-tool.exe -v | --version

Arguments:
  export      Export logs from Management Program to a local directory
  send        Generate logs to a local directory and also send them to SIEM

Options:
  -h, --help          Show help screen

  -v, --version        Show SIEM-tool version

  -d, --debug          Run in debug mode

  --log=<log>          Select type of log to be exported
                      (scannedlog | detectedlog | assetinfo | all)
                      e.g. --log=scannedlog

  --assetinfo=<assetinfo> Select type of Asset Info to be exported
                      (default all)
                      (assetinfo | applicationinfo | updateinfo | all)
                      e.g. --assetinfo=assetinfo,applicationinfo
                      e.g. --assetinfo=assetinfo
                      e.g. --assetinfo=all

  --format=<format>    Select export log format (csv | leef)
                      e.g. --format=csv

  --siem=<siem>        Input which SIEM platform you're uploading
                      to (qradar | splunk | rsyslog)
                      e.g. --siem=qradar

  --date              Filter entries by a range of dates (ddMMyyyy)
                      e.g. --date 01012000 31122017

  --ip=<ip>            Filter entries by host ip
                      e.g. --ip=192.168.0.1

  --netmask=<netmask> Filter entries by netmask
                      e.g. --netmask=192.168.0.0/24

  --hostname=<hostname> Filter entries by host name
                      e.g. --hostname=france

```

```
--startdate=<startdate> Specify the starting date to query  
from "startdate"  
e.g. --startdate="2018-03-05 12:16:08"
```

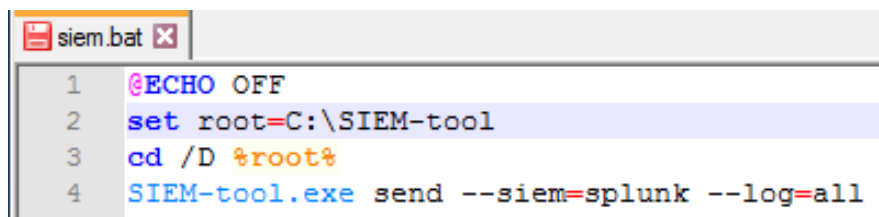
5. 一般的なユースケースは次のとおりです。

- a. すべてのログをエクスポートし、初期設定の LEEF 形式で QRadar サーバに送信する:

```
C:¥work¥SIEM-Tool> SIEM-Tool.exe send --log=all --siem=qradar
```

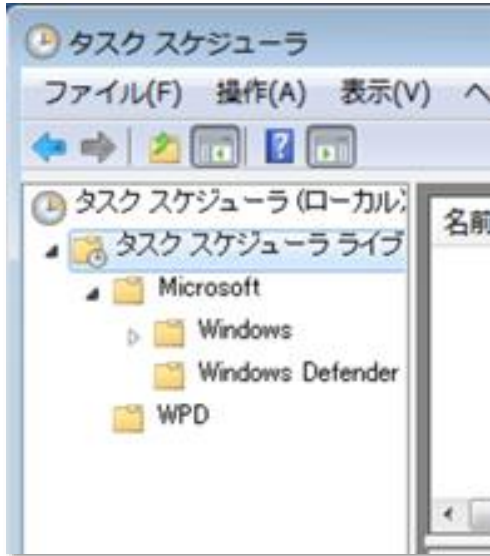
注意:

1. [QRadar] セクションのすべての設定が正しく行われていることを確認してください。
 2. サポートされるのは、LEEF 形式での SIEM サーバ (QRadar/Splunk) へのログの送信のみです。
- b. タスク スケジューラを使用し、すべてのログを自動的にエクスポートして、初期設定の LEEF 形式で Splunk に送信する:
 - i. 自動化ジョブに使用するバッチスクリプトを用意します。
以下を参考にしてください。

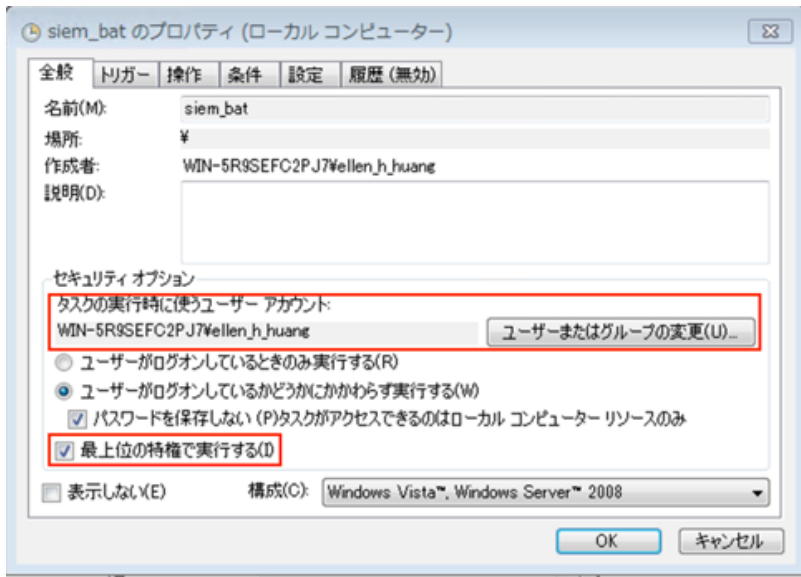


```
siem.bat x  
1 @ECHO OFF  
2 set root=C:\SIEM-tool  
3 cd /D %root%  
4 SIEM-tool.exe send --siem=splunk --log=all
```

ii. Windows メニューから **[タスク スケジューラ]** を起動します。



iii. タスク スケジューラの **[全般]** タブでユーザの権限を設定します。



iv. [トリガー] タブでスケジュールに従うトリガーを設定します。

新しいトリガー

タスクの開始(G): スケジュールに従う

設定

1回(N) 毎日(D) 毎週(W) 毎月(M)

開始(S): 4/20/2021 12:28:50 PM タイムゾーンにまたがって同期(Z)

間隔(C): 1 日

詳細設定

遅延時間を指定する(ランダム)(K): 1時間

繰り返し間隔(P): 1時間 継続時間(F): 1日間

繰り返し継続時間の最後に実行中のすべてのタスクを停止する(I)

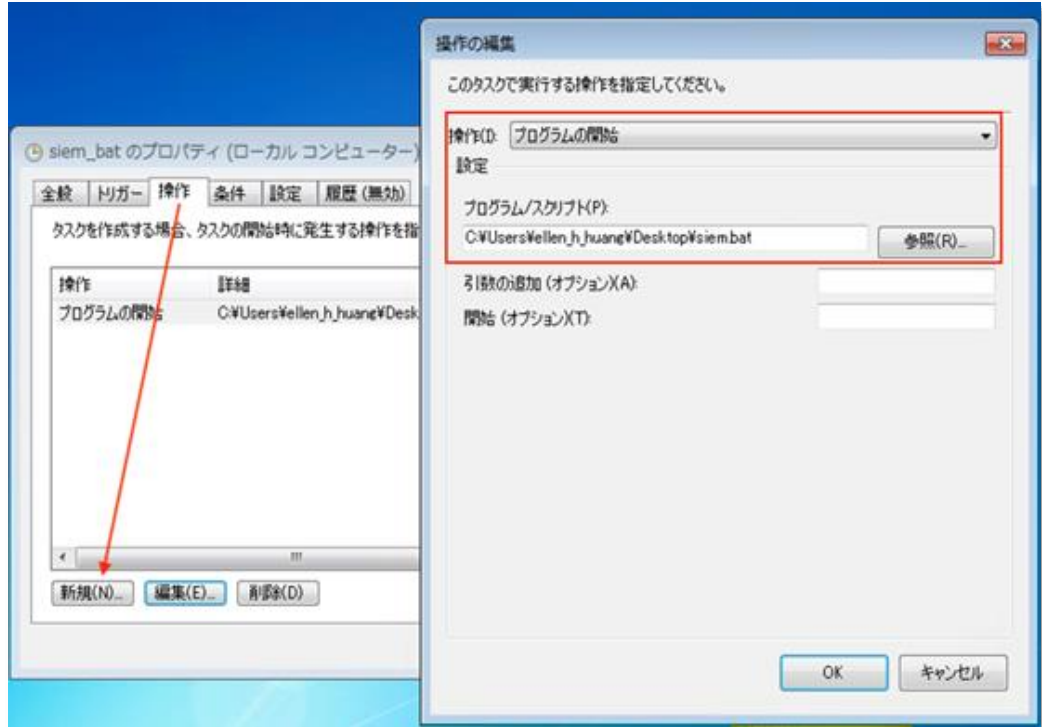
停止するまでの時間(L): 3日間

有効期限(X): 4/20/2022 12:28:50 PM タイムゾーンにまたがって同期(E)

有効(B)

OK キャンセル

- v. SIEM-tool.exe のタスクを含むバッチスクリプトで **[操作]** を設定し、**[OK]** をクリックします。最初のバッチが実行されれば、あとは設定された間隔で Splunk サーバがログを受信します (例: 5 分ごと)。



- c. 2000/01/01 から 2017/12/31 までの scannedlog を CSV 形式でローカルディレクトリにエクスポートする:

```
C:\work\SIEM-Tool> SIEM-Tool.exe export --log=scannedlog --format=csv
--date 01012000 31122017
```

6. デバッグログの収集方法

1. -d オプションに続けてエラーの原因となったコマンドを入力することで、デバッグモードを有効にします。
2. デバッグメッセージは debug_log_SIEM-tool.txt に収集されます。

7. TMPS3 ログの LEEF 形式の定義

LEEF 2.0 の基本形式

LEEF:2.0|ベンダ|製品|バージョン|イベント ID|カスタムイベントキーブロック

カスタムイベントキーブロック

- scannedlog

列	説明	例
devTime	日時	devTime=Jul 10 2020 17:01:08
devTimeFormat	日時の形式	devTimeFormat=MMM dd yyyy HH:mm:ss
sev	重大度	sev=2
eventId	イベント ID	eventId=1000
logID	ログ ID (一意のキー)	logID={A125CB7E-6A6B-4E8C-8D73-17CD67773CBE}
logVersion	ログのバージョン (3.0)	logVersion=3.0
startTime	イベントの開始時間 (MMM dd yyyy HH:mm:ss)	startTime=Jul 10 2020 17:03:42
endTime	イベントの終了時間 (MMM dd yyyy HH:mm:ss)	endTime=Jul 10 2020 17:03:42
deviceId	デバイス ID	deviceId={868057F8-ADDC-49AB-934C-B5B88E704521}
deviceName	デバイス名	deviceName=TMPS3
deviceVid	USB デバイスのベンダ ID	deviceVid=2203
devicePid	USB デバイスの製品 ID	devicePid=3838
deviceSid	USB デバイスのシリアル ID	deviceSid=BD0107089A38A920BD25
scannerVersion	検索サービスのバージョン	scannerVersion=1.61.1162
scanEngineVersion	ウイルス検索エンジンのバージョン	scanEngineVersion=12.0.1008

列	説明	例
patternVersion	ウイルスパターンファイルのバージョン	patternVersion=14.557.0
hostName	ホスト名	hostName=DESKTOP-2EOANGR
hostDomain	ホストドメイン	hostDomain=NT AUTHORITY
userName	ホストのログインユーザ名	userName=admin
hostIP	ホストの IPv4 アドレス	hostIP=192.168.137.129
hostMac	ホストの MAC アドレス	hostMac=00:0C:29:7A:88:6C
hostOS	ホストの OS	hostOS=Microsoft Windows 10 Enterprise Edition (build 16299), 64-bit
scannedStatus	結果のステータス (Scan completed、Scan canceled、Scan suspended)	scannedStatus=Scan completed
scannedFiles	検索されたファイルの結果	scannedFiles=23
infectedFiles	感染したファイルの数	infectedFiles=0
fixedFiles	修正済みファイルの数	fixedFiles=0
scanTarget	検索対象のオプション(All、Quick、Specified、SafeLockApplicationLockdown)	scanTarget=Specified
exclusionPath	除外されたパス	exclusionPath=Specified
exclusionFile	除外されたファイル	exclusionFile=c:\users\admin\downloads\test.txt
exclusionExtension	除外された拡張子	exclusionExtension=txt
comment	結果のコメント	comment=No threats found

scannedlog の例:

```
LEEF:2.0|TrendMicro|PortableSecurity|3.0|devTime=Jul 10 2020 17:01:08 devTimeFormat=MMM
dd yyyy HH:mm:ss sev=2 eventId=1000 logID={06BFDC81-8E9F-4A07-AE95-C079B452C19B}
logVersion=3.0 startTime=Jul 10 2020 17:01:08 endTime=Jul 10 2020 17:01:09
deviceID={868057F8-ADDC-49AB-934C-B5B88E704521} deviceName=TMPS3 deviceVid=2203
devicePid=3838 deviceSid=BD0107089A38A920BD25 scannerVersion=1.61.1162
scanEngineVersion= patternVersion=14.557.0 hostName=DESKTOP-2EOANGR hostDomain=NT
AUTHORITY userName=admin hostIP=192.168.137.129 hostMac=00:0C:29:7A:88:6C
```


hostOS=Microsoft Windows 10 Enterprise Edition (build 16299), 64-bit scannedStatus=Scan completed scannedFiles=23 infectedFiles=0 fixedFiles=0 scanTarget=Specified exclusionPath=Specified exclusionFile= exclusionExtension= comment=No threats found

- detectedlog

列	説明	例
devTime	日時	devTime=Jul 10 2020 17:01:08
devTimeFormat	日時の形式	devTimeFormat=MMM dd yyyy HH:mm:ss
sev	重大度	sev=2
eventId	イベント ID	eventId=1000
logID	ログ ID (一意でないキー)	logID={29FD789F-CA78-48FD-92B9-E598F1187C2E}
logVersion	ログのバージョン (3.0)	logVersion=3.0
startTime	イベントの開始時間 (MMM dd yyyy HH:mm:ss)	startTime=Jul 10 2020 17:09:04
endTime	イベントの終了時間 (MMM dd yyyy HH:mm:ss)	endTime=Jul 10 2020 17:09:05
deviceID	デバイス ID	deviceID={868057F8-ADDC-49AB-934CB5B88E704521}
deviceName	デバイス名	deviceName=TMPS3
deviceVid	USB デバイスのベンダ ID	deviceVid=2203
devicePid	USB デバイスの製品 ID	devicePid=3838
deviceSid	USB デバイスのシリアル ID	deviceSid=BD0107089A38A920BD25
hostName	ホスト名	hostName=WIN-JBFCTUNF08S
hostDomain	ホストドメイン	hostDomain=NT AUTHORITY
userName	ホストのログインユーザ名	userName=james_chang
hostIP	ホストの IPv4 アドレス	hostIP=192.168.137.251
hostMac	ホストの MAC アドレス	hostMac=00:0C:29:6C:12:C3
hostOS	ホストの OS	hostOS=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit

列	説明	例
aggressiveLevel	アグレッシブレベル	aggressiveLevel=0
threatName	脅威の名前	threatName=FILE_ADS
threatType	脅威の種類:	threatType=Other
threatRisk	脅威のリスクレベル (0: 低、1: 中、2: 高)	threatRisk=2
takenAct	処理の種類 (Fix、Ignore)	takenAct=Fix
takenActionResult	処理の結果 (Fixed、Unable to fix、Fixed at restart、Ignored)	takenActionResult=Fixed
threatPath	脅威のパス	threatPath=C:\Users\james_chang\Desktop\test.zip

detectedlog の例:

```
LEEF:2.0|TrendMicro|PortableSecurity|3.0|devTime=Jul 10 2020 17:09:04 devTimeFormat=MMM
dd yyyy HH:mm:ss sev=2 eventId=2008 logID={29FD789F-CA78-48FD-92B9-E598F1187C2E}
logVersion=3.0 startTime=Jul 10 2020 17:09:04 endTime=Jul 10 2020 17:09:05
deviceId={868057F8-ADDC-49AB-934C-B5B88E704521} deviceName=TMPS3 deviceVid=2203
devicePid=3838 deviceSid=BD0107089A38A920BD25 hostName=WIN-JBFCTUNF08S
hostDomain=NT AUTHORITY userName=james_chang hostIP=192.168.137.251
hostMac=00:0C:29:6C:12:C3 hostOS=Microsoft Windows 7 Enterprise Edition Service Pack 1 (build
7601), 32-bit aggressiveLevel=0 threatName=Eicar_test_file threatType=Other threatRisk=2
takenAct=Fix takenActionResult=Fixed
threatHash=542f0327d3c2d3d2d6095321e80ca8850ac83816436df87fa9a87957cf774e 7e
threatPath=C:\
```

- assetinfo

列	説明	例
sev	重大度	sev=2
eventId	イベント ID	eventId=3000
hostID	ホスト ID (TMPS で定義)	hostID=554328661
hostName	ホスト名	hostName=DESKTOP-DQVS8QS
domain	ドメイン	domain=DESKTOP-DQVS8QS
Mac	MAC アドレス	Mac=00:0C:29:DC:07:3A
IP	IPv4 アドレス	IP=192.168.137.235
OS	OS	OS=Microsoft Windows 10 Enterprise Edition (build 19041), 32-bit
OSType	Windows または Linux	OSType=WINDOWS
vendorName	ベンダ名	vendorName=VMware, Inc.
hwModel	ハードウェアモデル	hwModel=VMware Virtual Platform
hwSerialNum	ハードウェアのシリアル番号	hwSerialNum=VMware-56 4d 7e 74 92 98 22 24-39 26 f9 86 65 dc 07 3a
biosVersionAndDate	BIOS のバージョンと日付	biosVersionAndDate={INTEL - 6040000, PhoenixBIOS 4.0 Release 6.0 }{Release Date: 2017-05-19 00:00:00.000}
biosType	BIOS の種類	biosType=UEFI
secureBoot	セキュアブート	secureBoot=False
CPU	CPU	CPU=Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz
CPUArchitecture	CPU アーキテクチャ	CPUArchitecture=X64
processorsAndCores	プロセッサとコア	processorsAndCores=NumberOfCores: 1 ,NumberOfLogicalProcessors: 1
physicalMemory	物理メモリ	physicalMemory=2096628KB
availableMemory	使用可能メモリ	availableMemory=929560KB
OSVersionAndBuild	OS のバージョンとビルド	OSVersionAndBuild=Microsoft Windows 10 Enterprise 10.0.19041
OSServicePack	OS の Service Pack	OSServicePack=1.0

列	説明	例
OSProductID	OS の製品 ID	OSProductID=00328-90000-00000-AAOEM
OSLanguage	OS の言語	OSLanguage=en-US
OSInstalledDateAndTime	OS がインストールされた日時	OSInstalledDateAndTime=05032020 11:18:20
IEVersionAndBuild	IE のバージョンとビルド	IEVersionAndBuild=11.329.19041.0
IEServicePack	IE の Service Pack	IEServicePack=KB4561603
IEUpdateVersion	IE のアップデートバージョン	IEUpdateVersion=11.0.195
windowsDirectory	Windows ディレクトリ	windowsDirectory=C:\Windows
systemDirectory	システムディレクトリ	systemDirectory=C:\Windows\system32
systemDriveSize	システムドライブサイズ	systemDriveSize=39GB
systemDriveAvailableSize	システムドライブの使用可能なサイズ	systemDriveAvailableSize=24GB
bootDrive	起動ドライブ	bootDrive=\Device\HarddiskVolume1
timezone	タイムゾーン	timezone=UTC +08:00
systemDateAndTime	システムの日時	systemDateAndTime=10072020 11:41:21
loggedinAccount	ログインアカウント	loggedinAccount=abc
loggedinDomain	ログインドメイン	loggedinDomain=DESKTOP-DQVS8QS

assetinfo の例:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|sev=2 eventId=3000 hostID=554328661
 hostName=DESKTOP-DQVS8QS domain=DESKTOP-DQVS8QS Mac=00:0C:29:DC:07:3A
 IP=192.168.137.235 OS=Microsoft Windows 10 Enterprise Edition (build 19041), 32-bit
 OSType=WINDOWS vendorName=VMware, Inc. hwModel=VMware Virtual Platform
 hwSerialNum=VMware-56 4d 7e 74 92 98 22 24-39 26 f9 86 65 dc 07 3a
 biosVersionAndDate={INTEL - 6040000, PhoenixBIOS 4.0 Release 6.0 }(Release Date: 2017-05-
 19 00:00:00.000) biosType=UEFI secureBoot=False CPU=Intel(R) Core(TM) i7-9700 CPU @
 3.00GHz CPUArchitecture=X64 processorsAndCores=NumberOfCores:
 1 ,NumberOfLogicalProcessors: 1 physicalMemory=2096628KB availableMemory=929560KB
 OSVersionAndBuild=Microsoft Windows 10 Enterprise 10.0.19041 OSServicePack=

OSProductID=00328-90000-00000-AAOEM OSLanguage=en-US
OSInstalledDateAndTime=05032020 11:18:20 IEVersionAndBuild=11.329.19041.0
IEServicePack=KB4561603 IEUpdateVersion=11.0.195 windowsDirectory=C:\Windows
systemDirectory=C:\Windows\system32 systemDriveSize=39GB
systemDriveAvailableSize=24GB bootDrive=\Device\HarddiskVolume1 timezone=UTC +08:00
systemDateAndTime=10072020 11:41:21 loggedinAccount=abc loggedinDomain=DESKTOP-
DQVS8QS

- applicationinfo

列	説明	例
sev	重大度	sev=2
eventId	イベント ID	eventId=3000
hostID	ホスト ID (TMPS で定義)	hostID=554328661
name	アプリケーション名	name=7-Zip 19.00
publisher	発行元	publisher=Igor Pavlov
installedDate	インストール日	installedDate=22062020
size	ファイルサイズ	size=3772KB
version	アプリケーションのバージョン	version=19.00
installPath	アプリケーションのインストールパス	installPath=C:\Program Files\7-Zip\

applicationinfo の例:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|sev=2 eventId=3000 hostID=554328661 name=7-Zip
 19.00 publisher=Igor Pavlov installedDate= size=3772KB version=19.00 installPath=C:\Program
 Files\7-Zip\

- updateinfo

列	説明	例
sev	重大度	sev=2
eventId	イベント ID	eventId=3000
hostID	ホスト ID (TMPS で定義)	hostID=554328661
name	更新プログラム名	name=Update for Microsoft Windows (KB4557957)
program	プログラム名	program=Microsoft Windows
version	プログラムのバージョン	version=
publisher	プログラムの発行元	publisher=Microsoft Corporation
installedDate	インストール日	installedDate=16062020

updateinfo の例:

LEEF:2.0|TrendMicro|PortableSecurity|3.0|sev=2 eventId=3000 hostID=554328661
name=Update for Microsoft Windows (KB4552925) program=Microsoft Windows version=
publisher=Microsoft Corporation installedDate=16062020