Kaspersky Endpoint Security 11 for Linux
スタンドアロンインストールガイド

Ver11.3 対応

2023/04/10

株式会社カスペルスキー
セールスエンジニアリング本部

Ver 2.3

kaspersky

目次

1. はじめに

1.1. 本資料の目的

本資料では、スタンドアロン環境の Linux に対し「Kaspersky Endpoint Security for Linux」をインストールする手順についてご説明します。

1.2. 製品概要

それぞれの主な役割は以下の通りです。

- **Kaspersky Endpoint Security 11 for Linux (KESL) :**
  Linux OS（サーバー、ワークステーション）を対象としたアンチウイルス製品です。マルウェアのスキャンや駆除を行います。

1.3. 前提条件

・KESL が適切に動作するためにインストール先のコンピュータが最低システム要件を満たしていること。
<KESL システム要件>
https://support.kaspersky.com/help/KES4Linux/11.3.0/ja-JP/235168.htm

1.4. 注意事項

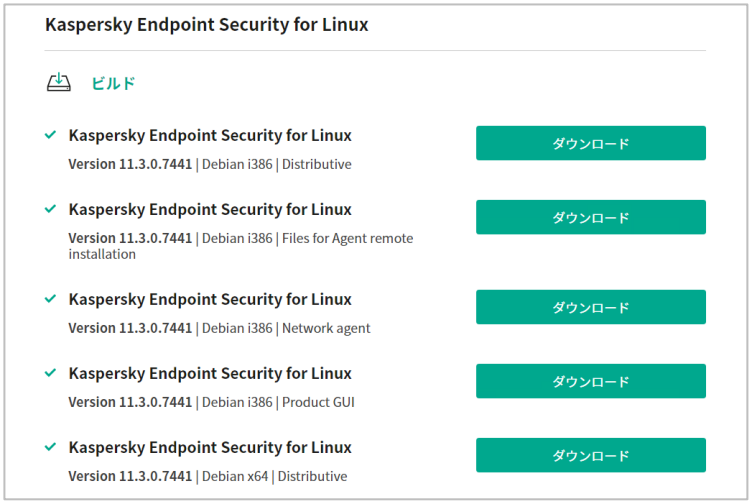
・必要なパッケージがインストールされていない場合、依存性の欠如のエラーが出力されます。
ソフトウェア要件を確認の上、本章の作業を実施してください。
・手順内ではバージョン表記を"x"と記載しています。
インストール実施時は弊社サポートサイトより最新のバージョンをダウンロードしてください。

2. KESL のインストール

本章では、Linux OS に対し、KESL をインストールする手順についてご説明します。
尚、本章では x64 ビットの OS に対するインストールを想定した手順となります。x86 ビットの OS にインストールする場合は x86 ビット OS 用のインストーラーをご利用ください。

(1) 以下サイトを開き、「最新版をダウンロード」をクリックします。
https://support.kaspersky.co.jp/kes11linux#downloads

(2) KESL、GUI のインストーラーを任意のフォルダーにダウンロードします。
ここでは/tmp/KESL にダウンロードします。



■RHEL 系 OS の場合
・KESL インストーラー
項目名：「Version xx.x.x.xxxx | Red Hat Enterprise Linux x64 | Distributive」
・GUI コンポーネント
項目名：「Version xx.x.x.xxxx | Red Hat Enterprise Linux x64 | Product GUI」

■Debian 系 OS の場合
・KESL インストーラー
項目名：「Version xx.x.x.xxxx | Debian x64 | Distributive」
・GUI コンポーネント
項目名：「Version xx.x.x.xxxx | Debian x64 | Product GUI」

(3) 以下のコマンドを実行します。

```
[root@localhost ~]# cd /tmp/KESL/
[root@localhost KESL]# rpm -ivh kesl-11.3.0-7441.x86_64.rpm
```

<コマンド>

■RHEL 系 OS の場合

cd /tmp/KESL

rpm –ivh kesl-xx.x.x-xxxx.x86_64.rpm

■Debian 系 OS の場合

cd /tmp/KESL

dpkg –i kesl_xx.x.x-xxxx_amd64.deb

(4) インストール完了後、「アプリケーション「Kaspersky Endpoint Security 11.3.0 for Linux」がインストールされました。ご使用の前には必ず設定を行ってください。」と表示されることを確認します。

```
[root@localhost KESL]# rpm -ivh kesl-11.3.0-7441.x86_64.rpm
準備しています...          ################################# [100%]
更新中 / インストール中...
   1:kesl-11.3.0-7441          ################################# [100%]

アプリケーション「Kaspersky Endpoint Security 11.3.0 for Linux」がインストールされました。ご使用の前には必ず設定を行ってください。

製品設定でスクリプト「/opt/kaspersky/kesl/bin/kesl-setup.pl」を実行してください
```

(5) 以下のコマンドを実行します。

```
[root@localhost KESL]# /opt/kaspersky/kesl/bin/kesl-setup.pl

Kaspersky Endpoint Security 11.3.0 for Linux version 11.3.0.7441
```

<コマンド>

/opt/Kaspersky/kesl/bin/kesl-setup.pl

(6) ロケールの設定をします。

使用環境に合わせてロケールを設定します。

ここでは既定の「ja_JP.UTF-8」のまま Enter キーを押します。

```
Setting up the Anti-Virus Service default locale

Specified locale will be used to show user agreements in this script and
send events to Kaspersky Security Center.
List of available locales:
- ja_JP.UTF-8
- de_DE.UTF-8
- en_US.UTF-8
- fr_FR.UTF-8
- ru_RU.UTF-8
- zh_CN.UTF-8
[ja_JP.UTF-8]:
```

(7) EULA の確認をします。
確認後、[y]を入力して Enter キーを押します。

```
Accepting the End User License Agreement (EULA) and Privacy Policy

Please confirm that you have fully read, understand, and accept the End
User License Agreement (EULA) and Privacy Policy to continue.

NOTE: To quit the EULA and Privacy Policy viewer, press the Q key.

Press ENTER to display the EULA and Privacy Policy:


Read EULA and Privacy Policy from file "/opt/kaspersky/kesl/doc/license.ja"
(utf-8) if it cannot be read here.

I confirm that I have fully read, understand, and accept the terms and
conditions of this End User License Agreement [y/n]: y
```

(8) プライバシーポリシーを確認します。
確認後、[y]を入力して Enter キーを押します。

```
I am aware and agree that my data will be handled and transmitted
(including to third countries) as described in the Privacy Policy. I
confirm that I have fully read and understand the Privacy Policy [y/n]: y
```

(9) KSN の設定をします。
「y」を入力して Enter キーを押します。

```
Configuring KSN

I confirm that I have fully read, understand, and accept the terms and
conditions of the Kaspersky Security Network Statement (KSN Statement is
available here: '/opt/kaspersky/kesl/doc/ksn_license.ja') [y/n]: y
```

(10) 管理者権限の設定をします。
管理者権限を設定したいロールがある場合、ロール名を入力します。
ここではそのまま Enter キーを押してスキップします。

```
Granting the Administrator role

Only users with the Administrator role have full access to the program
management by command line and GUI.

Specify user to grant the 'admin' role to (leave empty to skip):
```

(11) SELinux の設定と fanotify の確認をします。
「y」を入力して Enter キーを押します。

```
SELinux configuration

Do you want to configure SELinux automatically? [y]: y

Attempting to compile module 'kesl'
Attempting to install module
'/var/opt/kaspersky/kesl/common/temp/selinux/kesl.pp'
Attempting to enable module 'kesl'
Marking
/var/opt/kaspersky/kesl/11.3.0.7441_1680143888/opt/kaspersky/kesl/libexe
c/kesl with security type kesl_exec_t
Marking
/var/opt/kaspersky/kesl/11.3.0.7441_1680143888/opt/kaspersky/kesl/bin/k
esl-control with security type kesl_control_exec_t
Marking
/var/opt/kaspersky/kesl/11.3.0.7441_1680143888/opt/kaspersky/kesl/share
d/kesl with security type kesl_control_exec_t
Application executables were labeled automatically
Starting Kaspersky Endpoint Security 11.3.0 for Linux. This can take some
time. Please wait.
```

(12) アップデート元の設定をします。
ここではそのまま Enter キーを入力し、既定の「KLServers」を設定します。

```
Configuring the update source

Specify the update source. Possible values: KLServers|SCServer|<url>:
[KLServers]:
```

(13) プロキシの設定をします。
ご利用環境にプロキシが存在する場合、プロキシ情報を入力します。
ここでは既定のまま Enter キーを押します。

```
Configuring proxy server settings to connect to the updates source

If you use an HTTP proxy server to access the Internet, please enter
the address in one of the following formats:
proxyIP:port or user:pass@proxyIP:port, or enter 'no' [n]:
```

(14)　定義データベースを取得します。
Enter キーを押して最新版の定義データベースをダウンロードします。

```
Updated databases are an essential part of your server protection.
Please note that the application may be restarted during the update
process.
Do you want to download the latest databases now? [y]:
```

(15)　最新版の定義データベースがダウンロードされ、KESL が自動的に再起動されることを確認します。

```
Downloading the latest application databases

タスクの進捗状況：
[##################################################]100%
Latest databases are downloaded.
Restarting Kaspersky Endpoint Security 11.3.0 for Linux. This can take some
time. Please wait.
```

(16)　定義データベース更新のスケジュール設定をします。
既定のまま Enter キーを入力し、1 時間ごとに定義データベースが更新されるよう設定します。

```
Enabling automatic updates of the application databases

Do you want to enable scheduled updates? [y]:

Scheduled updates are enabled.
The application databases are scheduled to be updated hourly.
```

(17)　アクティベーションコードを入力し、製品をアクティベートします。
アクティベート完了後、「Activation completed successfully」と表示されます。

```
Activate the application

You must activate the application to use it.
To activate the application now, enter the path to your key file or an
activation code. Enter an empty string to add the built-in trial key: xxxxx-
xxxxx-xxxxx-xxxxx

Activation completed successfully.
[root@localhost KESL]#
```

(18)　GUI コンポーネントをインストールします。
以下のコマンドを実行します。

```
[root@localhost KESL]#
[root@localhost KESL]# rpm -ivh kesl-gui-11.3.0-7441.x86_64.rpm
```

<コマンド>

■RHEL 系 OS の場合

rpm –ivh kesl-gui_xx.x.x-xxxx.x86_64.rpm

■Debian 系 OS の場合

dpkg –i kesl-gui_xx.x.x-xxxx_amd64.deb

(19)　インストール完了後、KESL の GUI が表示可能になります。

本章は以上です。

3. タスク管理

インストール後、デフォルトではファイル脅威対策、ウェブ脅威対策、デバイスコントロール、ふるまい検知タスクのみ有効です。
本章では、コマンドラインにて各タスクを管理する方法をご説明いたします。

※タスクとは
カスペルスキー製品によって実行される機能は、タスクとして実装されます。
例：ファイルのリアルタイム保護、コンピュータの完全スキャン、定義データベースのアップデートなどが該当します。

3.1. ネットワーク脅威対策の有効化

ネットワーク脅威対策を有効にすることで受信ネットワークトラフィックにネットワーク攻撃特有の動作が含まれていないかスキャンします。

(1) ネットワーク脅威対策タスクを有効化します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --start-task 17

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --start-task 17
タスクが開始されました
[root@localhost ~]#
```

(2) 特定の IP アドレスのネットワーク活動をブロックしたくない場合、下記コマンドを実行することで除外設定が可能です。
ここでは IP アドレス「192.168.1.0/24」を除外リストに追加します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 17 UseExcludeIPs="Yes" ExcludeIPs.item_0000="192.168.1.0/24"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 17 UseExcludeIPs="Yes" ExcludeIPs.item_0000="192.168.1.0/24"
[root@localhost ~]#
```

(3) 下記コマンドを実行し、設定が正しいことを確認します。

<コマンド>
/opt/Kaspersky/kesl/bin/kesl-control --get-setting 17

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 17
ActionOnDetect=Block
BlockAttackingHosts=Yes
BlockDurationMinutes=60
UseExcludeIPs=Yes
ExcludeIPs.item_0000=192.168.1.0/24
[root@localhost ~]#
```

本節は以上です。

3.2. ファイアウォール管理タスクの有効化

ファイアウォール管理タスクを有効にすることでネットワークパケットルールに従いすべてのネットワーク活動をフィルタリングします。

※ファイアウォール管理タスクを有効にする前に、OS のファイアウォール管理ツールを無効にしてください。

(1) ファイアウォール管理タスクを有効化します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --start-task 12

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --start-task 12
タスクが開始されました
[root@localhost ~]#
```

(2) 制御したいネットワークパケットのルールを設定します。

ここでは全てのネットワークゾーンの TCP ポート 23 に対する接続をブロックするルールを作成します。

<コマンド>
/opt/Kaspersky/kesl/bin/kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
[root@localhost ~]#
```

(3) 下記コマンドを実行し、設定が正しいことを確認します。

<コマンド>
/opt/Kaspersky/kesl/bin/kesl-control --get-setting 12

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --get-setting 12
DefaultIncomingAction=Allow
DefaultIncomingPacketAction=Allow
OpenNagentPorts=Yes
[PacketRules.item_0000]
Name=Block_Telnet
FirewallAction=Block
Direction=Incoming
Protocol=TCP
RemotePorts=Any
LocalPorts=23
ICMPType=Any
ICMPCode=Any
RemoteAddress=Any
LocalAddress=Any
LogAttempts=No
[NetworkZonesTrusted]
[NetworkZonesLocal]
[NetworkZonesPublic]
[root@localhost ~]#
```

本節は以上です。

3.3. デバイスコントロールタスクの有効化

デバイスコントロールではデバイス種別、接続バスに応じたアクセスルールの設定が可能です。

3.3.1. デバイス種別ごとアクセス設定

DeviceClass セクションを設定することで、デバイスの種別に応じたアクセスルールの設定が可能です。
デバイスの種別は以下の通りです。

・ハードディスク
・リムーバブルドライブ
・フロッピーディスク
・CD/DVD ドライブ
・シリアルポートで接続されたデバイス
・パラレルポートで接続されたデバイス
・プリンター
・モデム
・テープデバイス
・多機能デバイス
・スマートカードリーダー
・Wi-Fi アダプター
・外部ネットワークアダプター
・ポータブルデバイス
・Bluetooth デバイス
・イメージングデバイス

また、デバイスの種別ごとに以下の値の設定が可能です。

・許可(Allow)
・接続バスのアクセスルールに依存(DependsOnBus)
・拒否(Block))
・アクセスルールに依存(ByRule)

本項ではリムーバブルドライブに対するアクセスをブロックする手順をご説明します。

(1) アクセスルールを設定します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceClass.RemovableDrive="Block"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceClass.RemovableDrive="Block"
[root@localhost ~]#
```

(2) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 15

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 15
RulesAction=ApplyRules
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=Block
Printer=DependsOnBus
FloppyDrive=DependsOnBus
OpticalDrive=DependsOnBus
Modem=DependsOnBus
TapeDrive=DependsOnBus
MultifuncDevice=DependsOnBus
SmartCardReader=DependsOnBus
PortableDevice=DependsOnBus
WiFiAdapter=DependsOnBus
NetworkAdapter=DependsOnBus
BluetoothDevice=DependsOnBus
ImagingDevice=DependsOnBus
SerialPortDevice=DependsOnBus
ParallelPortDevice=DependsOnBus
InputDevice=DependsOnBus
SoundAdapter=DependsOnBus
```

本項は以上です。

3.3.2. 接続バスごとのアクセス設定

本項では USB に対するアクセスをブロックする手順をご説明します。

(1) アクセスルールを設定します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceBus.USB="Block"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceBus.USB="Block"
[root@localhost ~]#
```

(2) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 15

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 15
RulesAction=ApplyRules
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=DependsOnBus
Printer=DependsOnBus
FloppyDrive=DependsOnBus
OpticalDrive=DependsOnBus
Modem=DependsOnBus
TapeDrive=DependsOnBus
MultifuncDevice=DependsOnBus
SmartCardReader=DependsOnBus
PortableDevice=DependsOnBus
WiFiAdapter=DependsOnBus
NetworkAdapter=DependsOnBus
BluetoothDevice=DependsOnBus
ImagingDevice=DependsOnBus
SerialPortDevice=DependsOnBus
ParallelPortDevice=DependsOnBus
InputDevice=DependsOnBus
SoundAdapter=DependsOnBus
[DeviceBus]
USB=Block
FireWire=Allow
```

本項は以上です。

3.3.3. 信頼するデバイスの設定

本項ではユーザーによるフルアクセスがいつでも可能な信頼するデバイスを設定する手順をご説明します。

(1) 信頼するデバイスを設定します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 TrustedDevices.item_0000.DeviceId=<信頼するデバイスの ID>

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 TrustedDevices.item_0000.DeviceId=xxxx:xxxx
```

(2) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 15

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 15
RulesAction=ApplyRules
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=DependsOnBus
Printer=DependsOnBus
FloppyDrive=DependsOnBus
OpticalDrive=DependsOnBus
Modem=DependsOnBus
TapeDrive=DependsOnBus
MultifuncDevice=DependsOnBus
SmartCardReader=DependsOnBus
PortableDevice=DependsOnBus
WiFiAdapter=DependsOnBus
NetworkAdapter=DependsOnBus
BluetoothDevice=DependsOnBus
ImagingDevice=DependsOnBus
SerialPortDevice=DependsOnBus
ParallelPortDevice=DependsOnBus
InputDevice=DependsOnBus
SoundAdapter=DependsOnBus
[DeviceBus]
USB=Block
FireWire=Allow
[TrustedDevices.item_0000]
DeviceId=xxxx:xxxx
Comment=
```

本項は以上です。

3.3.4. スケジュール設定

デバイスの種別がハードディスク、リムーバブルドライブ、フロッピーディスクおよび CD/DVD ドライブの場合、デバイスアクセスのスケジュール設定が可能です。
本項ではリムーバブルドライブに対する土日のアクセスを終日ブロックする手順をご説明します。

(1) リムーバブルドライブに対するアクセス可否をアクセスルールに準拠するよう設定を変更します。
下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceClass.RemovableDrive="ByRule"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 DeviceClass.RemovableDrive="ByRule"
[root@localhost ~]#
```

(2) デバイスアクセスのスケジュールを設定します。

ここではスケジュール名：「Holiday」、土、日曜日の終日が対象となるように設定します。
<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 Schedules.item_0001.ScheduleName="Holiday" Schedules.item_0001.DaysHours="Saturday-Sunday:0..24"

尚、曜日は完全な曜日名(例：Monday)または省略形(例：Mo、Mon)で使用することが可能です。
時間は[0:24]で指定し、間隔による指定のみ可能です。
(例：9-12 時を指定する場合：9..12)

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 Schedules.item_0001.ScheduleName="Holiday" Schedules.item_0001.DaysHours="Saturday-Sunday:0..24"
[root@localhost ~]#
```

(3) (2)で作成したスケジュールを適用するユーザー(ユーザーグループ)、デバイスの種別およびアクセス可否を設定します。
ここでは作成したスケジュール"Holiday"の間、リムーバブルドライブへのアクセスをブロックするよう設定します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 15 RemovableDrivePrincipals.item_0000.AccessRules.item_0000.UseRule="Yes" RemovableDrivePrincipals.item_0000.AccessRules.item_0000.ScheduleName="Holiday" RemovableDrivePrincipals.item_0000.AccessRules.item_0000.Access="Block"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 15 RemovableDrivePrincipals.item_0000.AccessRules.item_0000.UseRule="Yes" RemovableDrivePrincipals.item_0000.AccessRules.item_0000.ScheduleName="Holiday" RemovableDrivePrincipals.item_0000.AccessRules.item_0000.Access="Block"
[root@localhost ~]#
```

(4) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 15

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 15
RulesAction=ApplyRules
[DeviceClass]
HardDrive=DependsOnBus
RemovableDrive=ByRule
Printer=DependsOnBus
-------------------Omitted-----------------------------
[Schedules.item_0001]
ScheduleName=Holiday
DaysHours=Sat-Sun:0..24
[RemovableDrivePrincipals.item_0000]
Principal=¥Everyone
[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]
UseRule=Yes
ScheduleName=Holiday
Access=Block
[FloppyDrivePrincipals.item_0000]
Principal=¥Everyone
[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]
[root@localhost ~]#
```

本節は以上です。

3.4. アンチクリプタータスク設定

アンチクリプタータスクを設定することにより、SMB/NFS プロトコルで共有化したディレクトリに対するリモートからの悪意ある暗号化通信をブロックします。

例えば、何等かのデバイスがランサムウェアに感染した場合、ネットワーク上の共有フォルダーに対しても暗号化を試みます。アンチクリプター機能により、この通信を検知しブロックすることができます。

本節では SMB/NFS プロトコルによって共有される全てのローカルディレクトリのファイルに対してアンチクリプタータスクを設定する方法をご説明します。

(1) 下記コマンドを実行し、アンチクリプタータスクを設定します。

ここではブロック時間を 30 分で設定します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 13 UseHostBlocker=Yes BlockTime=30 UseExcludeMasks=No

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --set-setting 13 UseHostBlocker=Yes
BlockTime=30 UseExcludeMasks=No
[root@localhost ~]#
```

(2) 下記コマンドを実行し、アンチクリプタータスクを開始します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --start-task 13

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --start-task 13
タスクが開始されました
[root@localhost ~]#
```

(3) 特定のディレクトリを除外設定する場合、下記コマンドを実行します。

ここでは共有フォルダー/home/public 内の拡張子：doc のファイルをスキャン対象外に設定します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 13 UseExcludeMasks=Yes ExcludedFromScanScope.item_0000.AreaDesc=SampleExcludedScope ExcludedFromScanScope.item_0000.UseScanArea=Yes ExcludedFromScanScope.item_0000.Path=/home/public ExcludedFromScanScope.item_0000.AreaMask.item_0000=*.doc

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 13 UseExcludeMasks=Yes
ExcludedFromScanScope.item_0000.AreaDesc=SampleExcludedScope
ExcludedFromScanScope.item_0000.UseScanArea=Yes
ExcludedFromScanScope.item_0000.Path=/home/public
ExcludedFromScanScope.item_0000.AreaMask.item_0000=*.doc
[root@localhost ~]#
```

(4) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 13

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 13
UseHostBlocker=Yes
BlockTime=30
UseExcludeMasks=Yes
[ScanScope.item_0000]
AreaDesc=All shared folders
UseScanArea=Yes
Path=AllShared
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=SampleExcludedScope
UseScanArea=Yes
Path=/home/public
AreaMask.item_0000=*.doc
[root@localhost ~]#
```

本章は以上です。

4. スキャン設定

KESL ではスキャンタスクに対して定期または時間指定での実行スケジュールを設定することが可能です。
本章では、コマンドラインでタスク ID2:ウイルススキャンに対して毎週月曜日の 12:00 にタスクを実行するようスケジュールを設定する手順をご説明いたします。

4.1. スキャンスケジュール設定

(1) 下記のコマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-schedule 2 RuleType="Weekly" StartTime="12:00:00;Mon"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --set-schedule 2 RuleType="Weekly"
StartTime="12:00:00;Mon“
[root@localhost ~]#
```

(2) 下記のコマンドを実行し、正しく設定が反映されているか確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 2

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --get-schedule 2
RuleType=Weekly
StartTime=12:00:00;Mon
RandomInterval=99
RunMissedStartRules=Yes
[root@localhost ~]#
```

本節は以上です。

4.2. 除外設定

業務で使用しているアプリケーションやファイルがマルウェアとして検知しないよう除外設定をすることで、ディレクトリ配下のファイルを KESL のスキャン対象から除外することが可能です。

(1) 下記コマンドを実行します。
ここでは「/opt/kaspersky」配下のすべてのオブジェクトをリアルタイムスキャンの除外対象に設定します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-setting 2 --add-exclusion /opt/kaspersky

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-setting 2 --add-exclusion /opt/kaspersky
[root@localhost ~]#
```

(2) 下記コマンドを実行し、正しく設定されていることを確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-setting 2

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-setting 2
ScanFiles=Yes
ScanBootSectors=Yes
ScanComputerMemory=Yes
ScanStartupObjects=Yes
ScanArchived=Yes
ScanSfxArchived=Yes
----------------Omitted----------------------------------
UseExcludeMasks=No
UseExcludeThreats=No
ReportCleanObjects=No
ReportPackedObjects=No
ReportUnprocessedObjects=No
UseAnalyzer=Yes
HeuristicLevel=Recommended
UseIChecker=Yes
ScanPriority=Normal
DeviceNameMasks.item_0000=/**
[ScanScope.item_0000]
AreaDesc=All objects
UseScanArea=Yes
Path=/
AreaMask.item_0000=*
[ExcludedFromScanScope.item_0000]
AreaDesc=
UseScanArea=Yes
Path=/opt/kaspersky
AreaMask.item_0000=*
[root@localhost ~]#
```

本章は以上です。

5. アップデート設定

KESL ではアップデートのタスクに対する実行スケジュールを設定することが可能です。
本章ではコマンドラインでタスク ID6:アップデートを 30 分ごとに実行するようスケジュールを設定する手順をご説明いたします。

(1) 下記のコマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-schedule 6 RuleType="Minutely" StartTime="00:00:00;30"

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --set-schedule 6 RuleType="Minutely"
StartTime="00:00:00;30"
[root@localhost ~]#
```

(2) 下記のコマンドを実行し、正しく設定が反映されているか確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 6

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-
control --get-schedule 6
RuleType=Minutely
StartTime=00:00:00;30
RandomInterval=99
RunMissedStartRules=Yes
[root@localhost ~]#
```

本章は以上です。

6. Syslog 設定

監視やログ保存のために Syslog を設定することが可能です。
Syslog 設定を行うと/var/log/message にログを出力します。

※スタンドアロン環境では出力するログの選択は出来ず、全てのログを出力します。

(1) 下記コマンドを実行して Syslog 設定を有効にします。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --set-app-setting UseSyslog=Yes

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --set-app-setting UseSyslog=Yes
[root@localhost ~]#
```

(2) 下記コマンドを実行して Syslog 設定が正しく反映されているか確認します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-app-setting

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-app-setting
SambaConfigPath=/etc/samba/smb.conf
NfsExportPath=/etc/exports
TraceFolder=/var/log/kaspersky/kesl/
TraceLevel=None
TraceMaxFileCount=5
TraceMaxFileSize=500
BlockFilesGreaterMaxFileNamePath=16384
DetectOtherObjects=No
UseKSN=Extended
UseMDR=No
UseProxy=No
ProxyServer=
MaxEventsNumber=500000
LimitNumberOfScanFileTasks=0
UseSyslog=Yes
EventsStoragePath=/var/opt/kaspersky/kesl/private/storage/events.db
InterceptorProtectionMode=Block
NamespaceMonitoring=Yes
[root@localhost ~]#
```

(3) アプリケーションを再起動します。
以下コマンドは RHEL 系 7.x のコマンドとなります。ご利用環境に応じて再起動のコマンドを実行してください。

<コマンド>
systemctl restart kesl.service

```
[root@localhost ~]# systemctl restart kesl.service
[root@localhost ~]#
```

本章は以上です。

1. GUI 機能

KESL は GUI コンポーネントをインストールすることで GUI からも KESL を操作することが可能です。(スキャン、保管領域、設定は管理者権限の場合可能です。)
本章では、GUI から設定および確認が可能なステータスについてご説明します。

1.1. ライセンスの確認

現在のライセンス情報の確認手順及びアクティベーションコードを使用したライセンスの追加手順をご説明します。

(1) KESL の GUI を開き、「ライセンス：～」をクリックします。

(2) 現在のライセンスの情報が確認できます。
ライセンスを追加する場合、「追加」をクリックしてください。

<ライセンス未登録の場合>

<ライセンス登録済みの場合>

(3) アクティベーションコードを入力し、「次へ」をクリックします。

(4) ライセンスの情報が表示されます。「アクティベート」をクリックします。

(5) ライセンスがアクティベートされます。

本節は以上です。

1.2.　レポート確認

統計情報及び各タスクのイベントログの確認方法についてご説明します。

(1) KESL の GUI を開き、「レポート」をクリックします。

(2) 各タスクをクリックすることでレポートの確認が可能です。

本節は以上です。

1.3.　保管領域の確認

駆除プロセス中に削除または変更されたファイルのバックアップコピーの情報の確認方法をご説明します。

※バックアップコピー：
ファイルの駆除または削除を最初に施行したときに作成されたファイルのコピー。
特別な形式で保存されているため、脅威はありません。

(1) KESL の GUI を開き、「保管領域」をクリックします。

(2) 保管領域にあるオブジェクトの総数及び各オブジェクトの詳細情報を確認可能です。保管領域にあるオブジェクトを削除したい場合、削除したいオブジェクトのチェックボックスを ON にして「削除」をクリックします。

(3) 選択したオブジェクトが削除されます。

本節は以上です。

1.4.　各タスクの有効化

各タスクの有効/無効の設定を変更する方法をご説明します。

(1) KESL の GUI を開き、「設定」をクリックします。

(2) KSN の使用/未使用設定及び各タスクのステータスが確認できます。
以下各タスクを有効化する場合、「有効にする」をクリックします。
(既に有効化されている場合、「無効にする」と表示されています。)

・ファイル脅威対策
・システム変更監視
・ファイアウォール管理
・アンチクリプター
・ウェブ脅威対策
・デバイスコントロール
・リムーバブルドライブの監視
・ネットワーク脅威対策
・ふるまい検知

本節は以上です。

1.5.　ステータスの確認

KESL のバージョン、ライセンス及び定義データベースの公開日時の確認方法をご説明します。

(1) KESL の GUI を開き、「サポート」をクリックします。

(2) ライセンスのステータス及び定義データベースの公開日時を確認できます。
ライセンスの詳細及びライセンスの設定を行う場合、ライセンスをクリックしてください。
(クリック後の設定方法については
1.1. ライセンスの確認ご参照ください。)

本節は以上です。

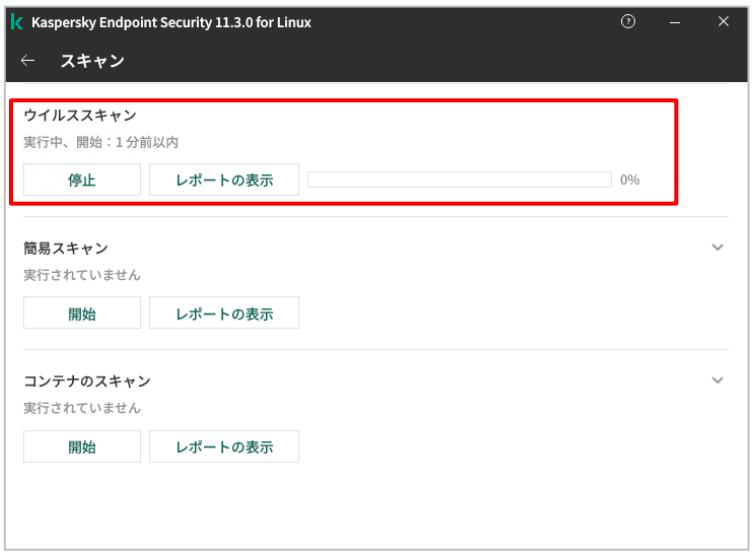
1.6.　手動スキャン

KESL の手動スキャン方法をご説明します。

(1) KESL の GUI を開き、「スキャン」をクリックします。

(2) GUI から「ウイルススキャン」「簡易スキャン」が実施可能です。

(3) スキャンを開始する場合、実施したいスキャンの「開始」をクリックします。
スキャンが開始されるとステータスバーが表示されます。



(4) スキャン終了後、「前回の開始日時」のステータスが更新されます。「スキャン済みのオブジェクト」及び「検知されたオブジェクト」の詳細情報を確認する場合は、「∨」をクリックしてください。

本節は以上です。

1.7. 手動アップデート

KESL の手動アップデート方法をご説明します。

(1) KESL の GUI を開き、「アップデート」をクリックします。

(2) アップデートを開始する場合、「開始」をクリックします。
アップデートが開始されるとステータスバーが表示されます。

(3) アップデート終了後、「前回の開始日時」のステータスが更新されます。

本章は以上です。

2. アプリケーション、ライセンスのステータス確認

コマンドラインにて KESL のステータスを確認することができます。

(1) アプリケーションのステータスを確認する場合、下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --app-info

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --app-info
名前:                                Kaspersky Endpoint Security 11.3.0 for Linux
バージョン:                          11.3.0.7441
ポリシー:                            適用できません

ライセンスの情報:                    ライセンスが有効です
ライセンスの有効期限:                2023-12-28 00:00:00
MDR BLOB ファイルのステータス:       読み込まれていません

保管領域の状態:                      保管領域にオブジェクトがありません
保管領域の使用量:                    保管領域のサイズは無制限です

「Scan_My_Computer」タスクを前回実行した日付: 2023-03-30 13:34:24

定義データベースの前回の公開日時:    2023-03-30 13:37:00
定義データベースが読み込まれました:  はい

Kaspersky Security Network のステータス:  拡張

Managed Detection and Response のステータス: 非アクティブ

ファイル脅威対策:                    使用可能、実行中

コンテナ監視:                        ライセンスの制限により使用不可

システム変更監視:                    ライセンスの制限により使用不可

ファイアウォール管理:                使用可能、停止
```

(2) ライセンス情報を確認する場合、下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control -L --query

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control -L --query
現在のライセンスの情報:
  有効期限                    : 2023-12-28 00:00:00
  有効期間の残り日数          : 272
  保護                        : 完全な保護
  アップデート                : 完全なアップデート
  ライセンスの情報            : ライセンスが有効です
  ライセンス種別              : 製品版
  使用制限                    : 300
  アプリケーション名          : Kaspersky Endpoint Security 11.3.0 for
Linux
  現在のライセンス            : CBADD548-76C8-4CA8-B467-
30939323A97A
  アクティベーション日        : 2022-12-26 05:05:18
予備のライセンスは追加されていません
[root@localhost ~]#
```

本章は以上です。

3. 関連ディレクトリ/ファイル

KESL 関連のディレクトリ及びファイルのリストは以下の通りとなります。

用途	ディレクトリ/ファイル
インストールディレクトリ	/opt/kaspersky
関連ディレクトリ	/var/opt/kaspersky
Log 関連ディレクトリ	/var/log/kaspersky

本章は以上です。

4. イベント DB 参照

KESL に関するログの参照方法についてご説明します。
ログを参照する場合、以下の状況に応じてコマンドの実行が必要です。

参照内容	実行コマンド
すべてのログを参照	/opt/kaspersky/kesl/bin/kesl-control -E --query
すべてのログをファイル出力	/opt/kaspersky/kesl/bin/kesl-control -E --query --file TestLog.txt
アップデートログのみ表示	/opt/kaspersky/kesl/bin/kesl-control -E --query "TaskType=='Update'" ※「Update」部分は大文字小文字を一致させる
指定したタスク ID のログのみ表示	/opt/kaspersky/kesl/bin/kesl-control -E --query "TaskId=='1'"
フィルタリングしたログのファイル出力	/opt/kaspersky/kesl/bin/kesl-control -E --query "TaskId=='1'" --file TestLog2.txt
取得するログの数量指定 (ログ量が多い場合に有効)	/opt/kaspersky/kesl/bin/kesl-control -E --query -n 2000

5. コマンドリファレンス

/opt/kaspersky/kesl/bin/kesl-control のオプションにつきましては以下の通りです。

※以下項目は Online Help より抜粋された内容となります。
https://support.kaspersky.com/KES4Linux/11.3.0/ja-JP/236935.htm

Kaspersky Endpoint Security のコマンドヘルプの表示	
オプション	説明
--help	Kaspersky Endpoint Security のコマンドのヘルプを表示します。
Kaspersky Endpoint Security のイベントの表示	
オプション	説明
-W	Kaspersky Endpoint Security のイベントの表示を有効にします。
Kaspersky Endpoint Security の設定とタスクを管理するためのコマンド	
オプション	説明
--app-info	Kaspersky Endpoint Security に関する全般設定を表示します。
--get-app-settings --file <ファイル名とディレクトリ>	Kaspersky Endpoint Security の全般設定を返します。
--set-app-settings --file <ファイル名とディレクトリ>	Kaspersky Endpoint Security の全般設定を設定します。
--get-task-list	既存の Kaspersky Endpoint Security タスクのリストを返します。
--get-task-state <タスク ID>|<タスク名>	指定されたタスクのステータスを表示します。
--create-task <タスク名> --type <タスクの種別> --file <ファイル名とディレクトリ>	指定した種別のタスクを作成します。指定した設定ファイルからタスクに設定を読み込みます。
--delete-task <タスク ID>|<タスク名>	タスクを削除します。
--start-task <タスク ID>|<タスク名> [-W] [--progress] [--file <ファイル名とディレクトリ>]	タスクを開始します。
--stop-task <タスク ID>|<タスク名>	タスクを停止します。

オプション	説明
--suspend-task <タスク ID>|<タスク名>	タスクを一時停止します。アップデートタスクの一時停止はできません。
--resume-task <タスク ID>|<タスク名>	タスクを再開します。アップデートタスクの再開はできません。
--get-settings <タスク ID>|<タスク名> --file <ファイル名とディレクトリ>	タスクの設定を返します。
--set-settings <タスク ID>|<タスク名> [<パラメータ>] [--file <ファイル名とディレクトリ>] [--add-path <パス>] [--del-path <パス>] [--add-exclusion <実行>] [--del-exclusion <実行>]	タスクの設定を指定します。
--scan-file <パス> [--action <処理>]	一時的な Scan_File タスクを作成して開始します。
--import-settings <--file file>	製品設定を設定ファイルにインポートします。
--update-application	製品をアップデートします。
--set-settings {<タスク ID>|<タスク名>} --set-to-default	タスクの設定を既定値に設定します。
--omsinfo --file <パス>	Microsoft Operations Management Suite と統合するためのファイルを JSON 形式で作成します。
ライセンス管理コマンド	
オプション	説明
--add-active-key <アクティベーションコード>|<ライセンス情報ファイル>	現在のライセンスを追加します。
--add-reserve-key <アクティベーションコード>|<ライセンス情報ファイル>	予備のライセンスを追加します。
--revoke-active-key	現在のライセンスを削除します。
-L --query	ライセンスに関する情報を表示します。
--revoke-reserve-key	予備のライセンスを削除します。

ファイアウォール管理タスクのコマンド	
オプション	説明
--add-rule [--name <文字列>] [--action <処理>] [--protocol <プロトコル>] [--direction <ディレクトリ>] [--remote <リモート>] [--local <ローカル>] [--at <インデックス>]	新しいルールを追加します。
--del-rule [--name <文字列>] [--index <インデックス>]	ルールを削除します。
--move-rule [--name <文字列>] [--index <インデックス>] [--at <インデックス>]	ルールの優先度を変更します。
--add-zone --zone <ゾーン> [--address <アドレス>]	ゾーンに IP アドレスを追加します。
--del-zone [--zone <ゾーン>] [--address <アドレス>] [--index <インデックス>]	ゾーンから IP アドレスを削除します。
-F --query	情報を表示します。
アンチクリプタータスクのコマンド	
オプション	説明
--get-blocked-hosts	ブロックされるコンピュータの一覧を表示します。
--allow-hosts	信頼しないコンピュータのブロックを解除します。
Docker コンテナとイメージのスキャンのコマンド	
オプション	説明
--scan-container <コンテナ|イメージ[:tag]>	Docker コンテナの一時スキャンタスクを、コンテナのカスタムスキャンタスクの設定で作成します（タスク名 : Custom_Container_Scan、task ID : 19）。スキャンの完了後、一時的なタスクは自動的に削除されます。
ユーザー管理コマンド	
オプション	説明
--get-user-list	ユーザーとロールのリストを取得します。
--grant-role <ロール> <ユーザー>	指定したユーザーにロールを付与します。
--revoke-role <ロール> <ユーザー>	指定したユーザーのロールを取り消します。

保管領域を管理するためのコマンド	
オプション	説明
-B --mass-remove --query	保管領域を完全に、または選択してクリアします。
-B --query	保管領域内のオブジェクトに関する情報を表示します：
-B --restore <オブジェクト ID> --file <ファイル名とディレクトリ>	保管領域からオブジェクトを復元します。
イベントログを管理するために使用されるコマンド	
オプション	説明
-E --query <フィルター>--db <データベースファイル> -n <数値> --file <ファイル名とパス>	フィルター条件に一致するイベントに関する情報をイベントログデータベースから指定するファイルへ出力します。
タスクスケジュールの管理コマンド	
オプション	説明
--set-schedule <タスク ID>|<タスク名> --file <ファイル名とパス>	タスクスケジュールを設定するか、設定ファイルからタスクスケジュール設定をタスクに読み込みます。
--get-schedule <タスク ID>|<タスク名> --file <ファイル名とパス>	タスクスケジュールの設定を返します。

本章は以上です。

6. タスク ID 確認

タスク ID の確認方法についてご説明します。

(1) 下記コマンドを実行します。

<コマンド>
/opt/kaspersky/kesl/bin/kesl-control --get-task-list

```
[root@localhost ~]# /opt/kaspersky/kesl/bin/kesl-control --get-task-list
タスクの数：20
名前: File_Threat_Protection
   ID   : 1
   種別 : OAS
   状態 : 開始済み
名前: Scan_My_Computer
   ID   : 2
   種別 : ODS
   状態 : 停止
名前: Scan_File
   ID   : 3
   種別 : ODS
   状態 : 停止
名前: Critical_Areas_Scan
   ID   : 4
   種別 : ODS
   状態 : 停止
名前: Update
   ID   : 6
   種別 : Update
   状態 : 停止
```

上記コマンドを実施することで以下のタスク情報が確認可能です。

1) タスクの数：<値>
   作成済みのタスクの総数です。
2) タスク名：<値>
   タスクに設定された名称です。
3) ID: <値>
   KESL が作成時にタスクに割り当てる数値です。事前に定義されたタスクは 1~20、ユーザタスクは 100 からは始まる一意の ID を持っています。
4) 種別：<値>
   KESL にによって事前に定義されたタスクの種別です。
   例)File_Threat_Protection, Scan_My_Computer, Scan_File, Boot_Scan などが該当します。
5) 状態：<開始済み|開始中|停止|停止中>
   タスクの状態です。

本章は以上です。

株式会社カスペルスキー

〒101-0021 東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F

www.kaspersky.co.jp | kasperskylabs.jp/biz/