

室蘭工業大学様 全学情報基盤システム

ServerProtect for Linux
インストール手順書

富士通 Japan 株式会社

目 次

はじめに	1
1. 準備	2
2. 依存パッケージの確認	6
3. ServerProtect for Linux のインストール.....	7
4. Kernel フックモジュールのインストール.....	8
5. インストール後の初期設定	10

はじめに

ServerProtect for Linux のインストール手順を示す。本手順書は Red Hat Enterprise Linux9.1 を例にした手順書になります。

1. 準備

- ① 以下の Trend Micro のダウンロードセンターより、「ハイブリッドクラウドセキュリティ」→「ServerProtect for Linux」を選択、対象 OS に合わせた ServerProtect for Linux のパッケージおよび Kernel フックモジュールをダウンロードし、サーバにコピーします。

<https://downloadcenter.trendmicro.com/>



The screenshot shows the Trend Micro download center website. The navigation bar includes links for 'ダウンロード', '購入・更新', '日本語 (日本)', 'ログイン', and 'お問い合わせ'. The main menu has 'Business', 'テーマ別対策', '製品・ソリューション', 'リサーチ', 'サービス', 'パートナー', and '会社概要'. The breadcrumb trail is 'Business > Products > 最新版ダウンロード'. The main content area features a banner for 'エンタープライズ製品アップデート' and 'パターンファイル情報'. Below the banner, there is a section titled 'エンタープライズ製品の最新版をダウンロード' and a heading 'ハイブリッドクラウドセキュリティ'. A grid of product options is displayed, with 'ServerProtect for Linux' highlighted by a red rectangular box.

Deep Security	ServerProtect for NetApp
ServerProtect for EMC Celerra	ServerProtect for Storage
ServerProtect for Linux	ServerProtect for Windows

- ② 「プロダクト・アップデート」タブを選択し、インストールプログラムをダウンロードします。ダウンロードファイルはOS 種別で異なりますので、OS に合わせてダウンロードしてください。

ServerProtect for Linux 3.0

[他のバージョンを見る](#)

プロダクト・アップデート Patch Kernel Support 検索エンジン

オペレーティングシステム: Linux

ダウンロード内容	リリース日付	ファイル名	サイズ (MB)
インストールプログラム English	0000-00-00	-	0

詳細情報

このモジュールについて

ファイル名: -

ServerProtect for Linuxは、UEFIセキュアブートと互換性がありません。
UEFIセキュアブートが有効になっている場合、Kernel Hook Module (カーネルフックモジュール, KHM)は正しくロードされません。

Red Hat 9	
リリース日付: 2022-12-23	ファイル名: SPLX30-X64-Redhat9.tar.gz ビルド: 3.0.1694
サイズ(MB): 85.2	SHA256: 32fbc503f65f819e19b844d906a2b1fa47279b065730c9a7eb513cc95b668f8
ドキュメント: 管理者ガイド , クイックスタートガイド , Readme(SJIS) , Readme(UTF-8)	
備考: 1. Service Pack 1 Patch 9 までの修正を含みます。 2. 各ドキュメントに記載のある「Trend Micro Control Manager」は 2021/05/31 にサポート終了しておりますので、「Trend Micro Apex Central」と読み替えていただきますようお願い申し上げます。	
Red Hat 8 / CentOS 8 / SUSE 15	
リリース日付: 2020-02-26	ファイル名: SPLX30-X64-Redhat8_CentOS8_Suse15-repack3.tar.gz ビルド: 3.0.1621

- ③ 「Kernel Support」タブを選択し、カーネルフックモジュールファイルをダウンロードします。ダウンロードファイルは OS およびカーネルバージョンで異なりますので、カーネルバージョンに合わせてダウンロードしてください。ここでは、Red Hat Enterprise Linux 9.1 のカーネルバージョン 5.14.0-162.23.1.el9_1.x86_64 を例として示しています。

カーネルバージョンは以下のコマンドで確認出来ます。

```
# uname -r  
5.14.0-162.23.1.el9_1.x86_64
```

ServerProtect for Linux 3.0
他のバージョンを見る

プロダクト・アップデート Patch **Kernel Support** 検索エンジン

オペレーティングシステム: Linux

ダウンロード内容	リリース日付	ファイル名	サイズ (MB)
インストールプログラム English	2010-05-31	ダウンロードページへのリンク	0

Operating System

Red Hat Enterprise Linux 9.0

Download Description	Release Date	File Name	Size (MB)	Download Package
Kernel Update English	2023-11-08	rhel9-5.14.0-70.75.1.el9-0.x86-64	0.55	
+ More details				
Kernel Update English	2023-09-19	5.14.21-150500.53-default.x86-64	0.66	
+ More details				
Kernel Update English	2023-08-14	5.14.0-284.25.1.el9-2.x86-64	0.57	
+ More details				
Kernel Update English	2023-07-11	5.14.0-284.18.1.el9-2.x86-64	0.57	
+ More details				
Kernel Update English	2023-07-05	5.14.0-284.11.1.el9-2.x86-64	0.56	
+ More details				
Kernel Update English	2023-05-09	5.14.0-162.23.1.el9-1.x86-64	0.53	
+ More details				

2. 依存パッケージの確認

① ServerProtect for Linux は以下の依存するパッケージがあるので、対象システムにインストールされていることを確認します。インストールされていない場合は、インストールを実施してください。

- glibc
- libgcc
- zlib
- bzip2
- libuuid
- libstdc++ (Red Hat、CentOS のみ)
- nss-softokn-freebl (Red Hat、CentOS のみ)
- perl-Sys-Syslog (Red Hat、CentOS のみ)
- chkconfig (Red Hat 9 のみ)

3. ServerProtect for Linux のインストール

- ① Root 権限のユーザでログインします。
- ② 「1. 準備」で用意した ServerProtect for Linux のインストールファイルを対象サーバの任意のフォルダに転送します。
- ③ 転送したフォルダに移動し、ServerProtect for Linux をインストールします。

```
# unzip SProtectLinux.zip ←zip ファイルを解凍する
Archive: SProtectLinux.zip
  inflating: SServerProtect for Linux/splx_30_lx_en_sp1_patch9.tar.gz
  inflating: SServerProtect for Linux/splx_kernel_module-3.0.1.0026.rhel9_5.14.0-162.23.1.el9_1.x86_64.x86_64.tar.gz
  inflating: SServerProtect for Linux/SPLX30-X64-Redhat9.tar.gz
# mv SServerProtect¥ for¥ Linux SProtectLinux ←スペースが入っているフォルダ名をリネームする
# cd SProtectLinux
# ls
SPLX30-X64-Redhat9.tar.gz
splx_30_lx_en_sp1_patch9.tar.gz
splx_kernel_module-3.0.1.0026.rhel9_5.14.0-162.23.1.el9_1.x86_64.x86_64.tar.gz
# tar zxvf SPLX30-X64-Redhat9.tar.gz
SProtectLinux-3.0-1694.bin
# ./SProtectLinux-3.0-1694.bin
NOTICE: Trend Micro licenses . . . . .
  . ←ライセンス条項が表示されるので「--続きます--」という表示が出たらスペースキーを押す
  .
Do you agree to the above license terms? (yes or no)yes
  .
  .
SPLX server name or IP address: 自 IP アドレス指定
Do you wish to connect to Control Manager server using HTTPS? (y/n) [n] y
Control Manager server name or IP address: 157.19.221.9
Control Manager server port [443]: 443
Do you access Control Manager through a proxy server? (y/n) [n] n
*****PRODUCT*****
Please specify the name you would like to display on the Control Manager console
[SPLX server name or IP address]: 自ホスト名指定
Please specify a folder name for this product (for example: /SPLX) [New entity]:
New entity

(次ページに続く)
```

(前ページの続き)

```
*****  
Control Manager network/product information entered  
Control Manager server name or IP: 157.19.221.9  
Control Manager port: 443  
Connect using HTTPS: yes  
Display Name on Control Manager: 自ホスト名  
Installation folder: New entity  
*****  
Is the above information correct? (y/n) [n] y  
Saving information to the configuration file...done.  
.  
.  
ServerProtect for Linux installation completed.
```

←正常終了メッセージを確認する

4. Kernel フックモジュールのインストール

- ① Root 権限のユーザでログインします。
- ② 「1. 準備」で用意した Kernel フックモジュールを対象サーバの任意のフォルダに転送します。
- ③ ServerProtect for Linux のフォルダに移動し、Kernel フックモジュールをコピーします。
以下の例では /root/SProtectLinux フォルダ 配下に配置しています。

```
# cd /root/SProtectLinux  
# ls  
SPLX30-X64-Redhat9.tar.gz  
SProtectLinux-3.0-1694.bin  
splx_30_lx_en_sp1_patch9.tar.gz  
splx_kernel_module-3.0.1.0026.rhel9_5.14.0-162.23.1.el9_1.x86_64.x86_64.tar.gz  
↑  
このファイルが Kernel フックモジュールです。  
# cd /opt/TrendMicro/SProtectLinux/SPLX.module/  
# tar zxvf /root/SProtectLinux/splx_kernel_module-3.0.1.0026.rhel9_5.14.0-  
162.23.1.el9_1.x86_64.x86_64.tar.gz  
splxmod-5.14.0-162.23.1.el9_1.x86_64.x86_64.o  
splxmod-5.14.0-162.23.1.el9_1.x86_64.x86_64.o.md5  
#
```

④ ServerProtect for Linux サービスの再起動

```
# /etc/init.d/splx restart
Shutting down ServerProtect for Linux:
Shutting down splxcore:
Shutting down vsapiapp[FAILED]
Unloading splx kernel module:[FAILED]
Shutting down entity: [ OK ]
ServerProtect for Linux core stopped normally.
[ OK ]
Shutting down splxhttpd:
Shutting down splxhttpd: [ OK ]
ServerProtect for Linux httpd stopped normally.
[ OK ]
ServerProtect for Linux stopped normally.
Starting ServerProtect for Linux:
Checking configuration file: [ OK ]
Starting splxcore:
Starting Entity: [ OK ]
Loading splx kernel module: [ OK ]
Starting vsapiapp: [ OK ]
ServerProtect for Linux core started.
[ OK ]
Starting splxhttpd:
Starting splxhttpd: [ OK ]
ServerProtect for Linux httpd started.
[ OK ]
ServerProtect for Linux started. ←正常起動メッセージを確認
```

5. インストール後の初期設定

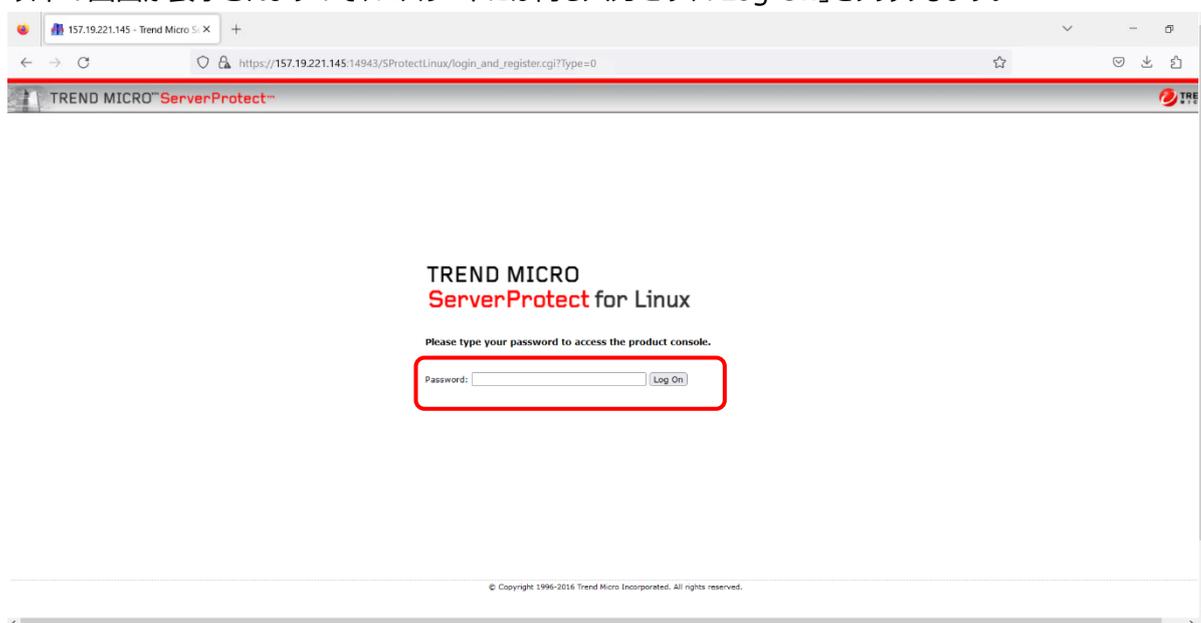
インストール後に以下の設定を実施します。

- パッケージやパターンファイルのダウンロード先の設定
- 管理コンソールのパスワード設定
- ライセンスコードの設定
- リアルタイムスキャンの除外設定（必要な場合）

① ブラウザから以下の URL にアクセスします。

<https://対象サーバ IP アドレス:14943/>

② 以下の画面が表示されますので、パスワードには何も入力せず、「Log On」をクリックします。



③ 以下の画面が表示されます。

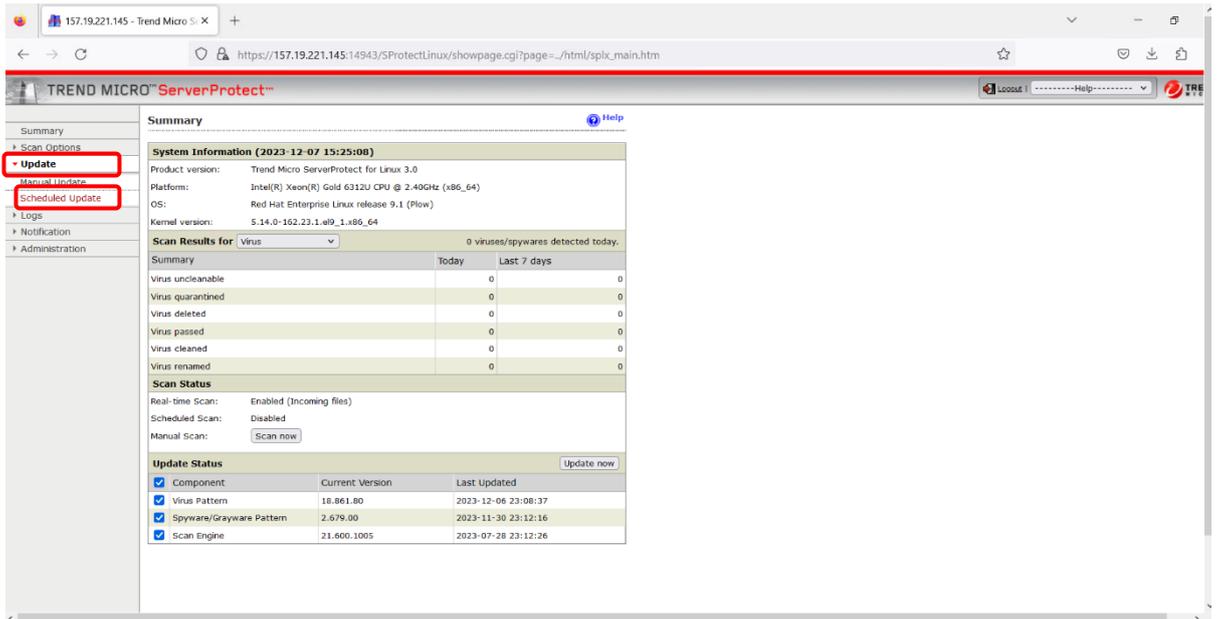
The screenshot displays the Trend Micro ServerProtect web interface. The browser address bar shows the URL: `https://157.19.221.145:14943/SProtectLinux/showpage.cgi?page=~/html/splx_main.htm`. The interface includes a navigation menu on the left with options like Summary, Scan Options, Update, Logs, Notification, and Administration. The main content area is titled "Summary" and contains the following sections:

- System Information (2023-12-07 14:07:40)**
 - Product version: Trend Micro ServerProtect for Linux 3.0
 - Platform: Intel(R) Xeon(R) Gold 6312U CPU @ 2.40GHz (x86_64)
 - OS: Red Hat Enterprise Linux release 9.1 (Plow)
 - Kernel version: 5.14.0-162.23.1.el9_1.x86_64
- Scan Results for Virus** (0 viruses/spywares detected today.)

Summary	Today	Last 7 days
Virus uncleanable	0	0
Virus quarantined	0	0
Virus deleted	0	0
Virus passed	0	0
Virus cleaned	0	0
Virus renamed	0	0
- Scan Status**
 - Real-time Scan: Enabled (Incoming files)
 - Scheduled Scan: Disabled
 - Manual Scan:
- Update Status** (Update now)

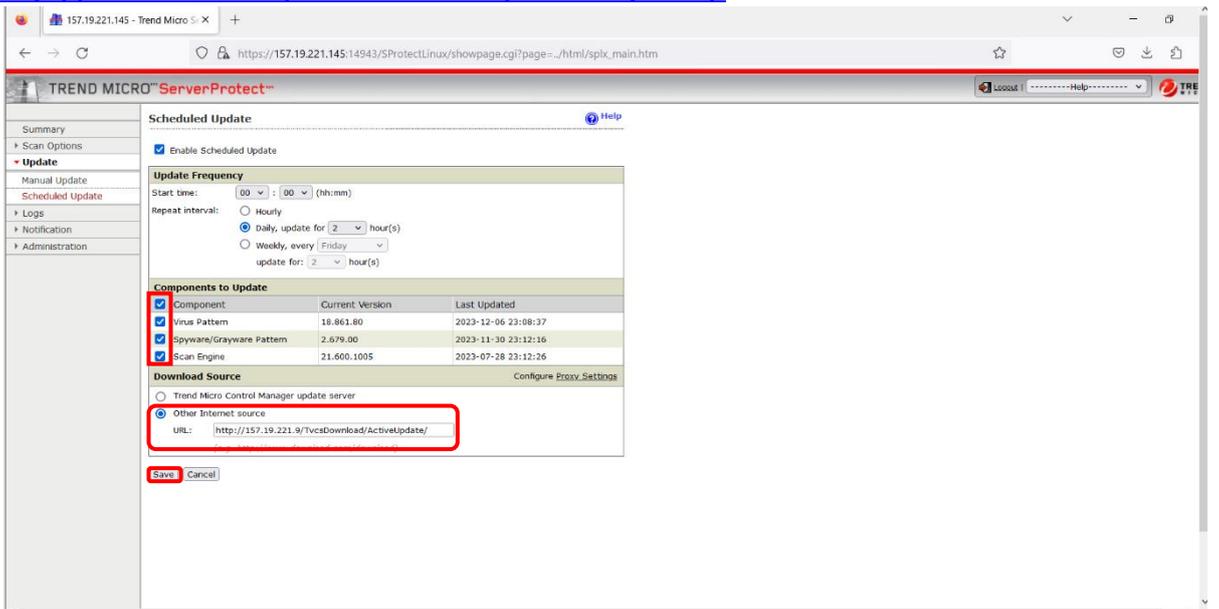
Component	Current Version	Last Updated
<input checked="" type="checkbox"/> Virus Pattern	18.861.80	2023-12-06 23:08:37
<input checked="" type="checkbox"/> Spyware/Grayware Pattern	2.679.00	2023-11-30 23:12:16
<input checked="" type="checkbox"/> Scan Engine	21.600.1005	2023-07-28 23:12:26

- ④ 左タブの「Update」-「Scheduled Update」を選択します。

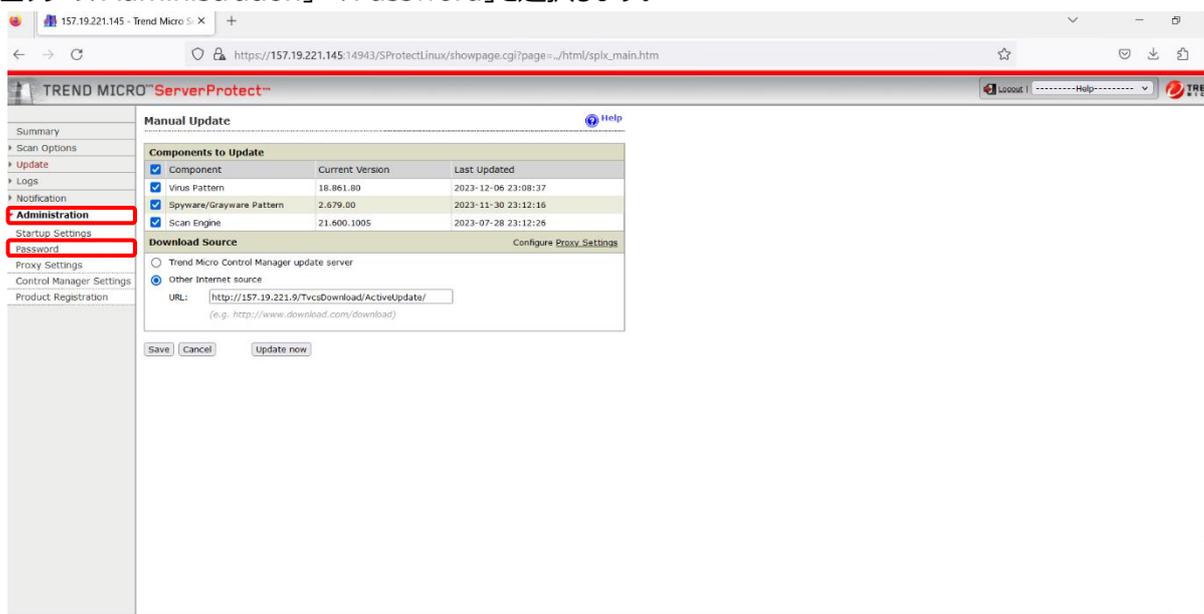


- ⑤ 「Update Status」の項目全てにチェックを入れます。「Download Source」に以下の URL を設定し、Save ボタンをクリックします。

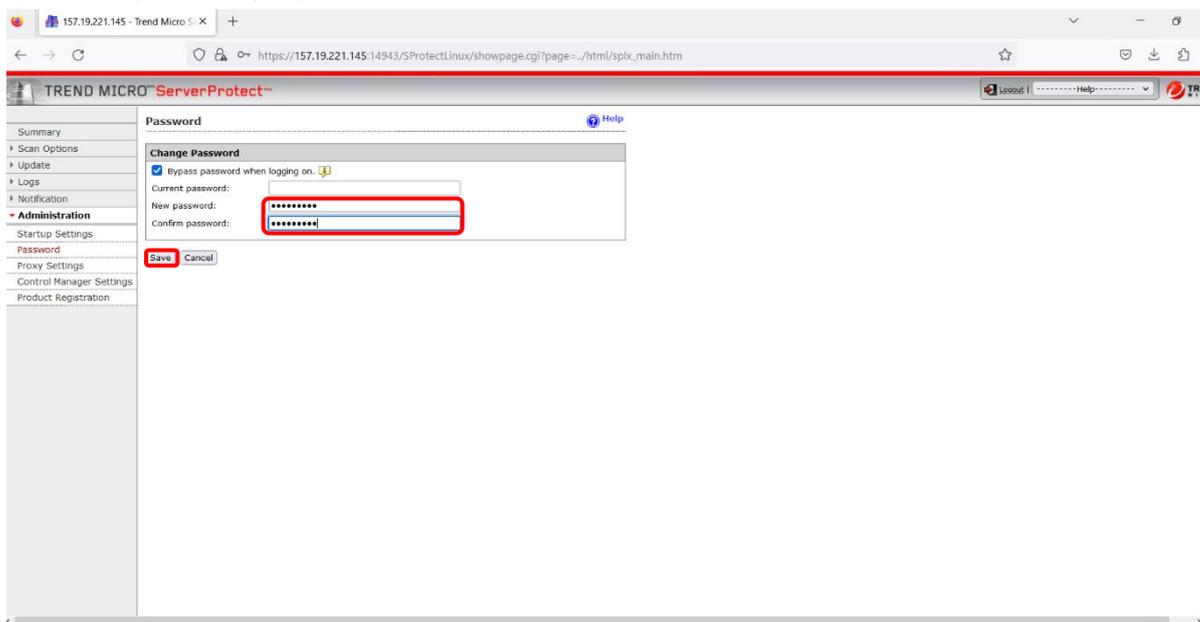
<http://157.19.221.9/TvcsDownload/ActiveUpdate/>



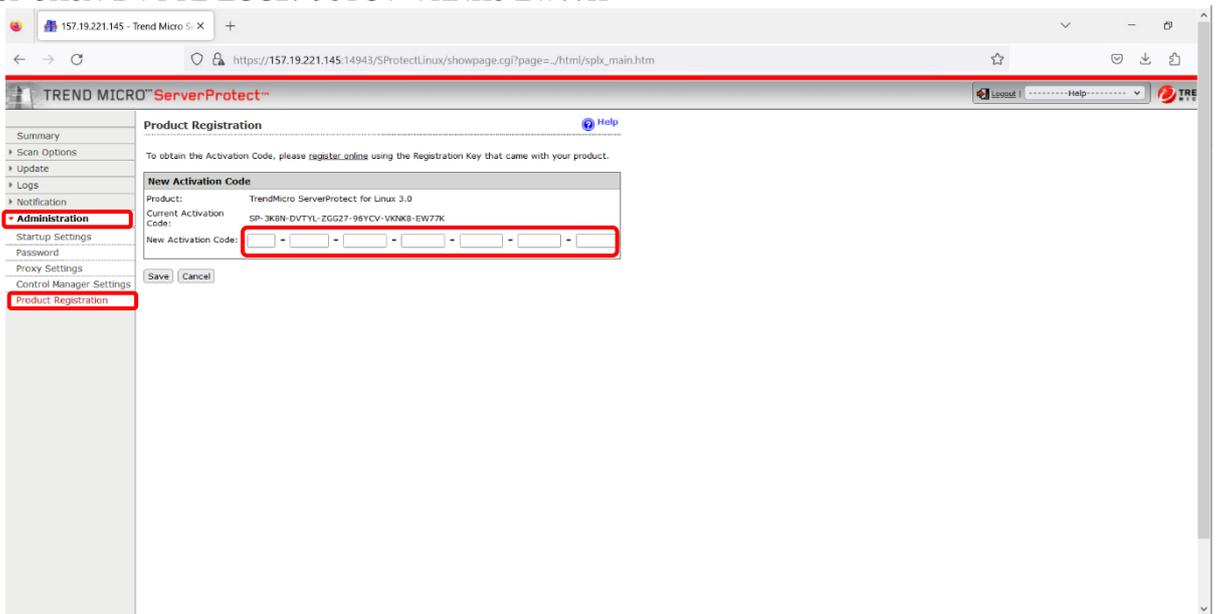
- ⑥ 左タブの「Administration」-「Password」を選択します。



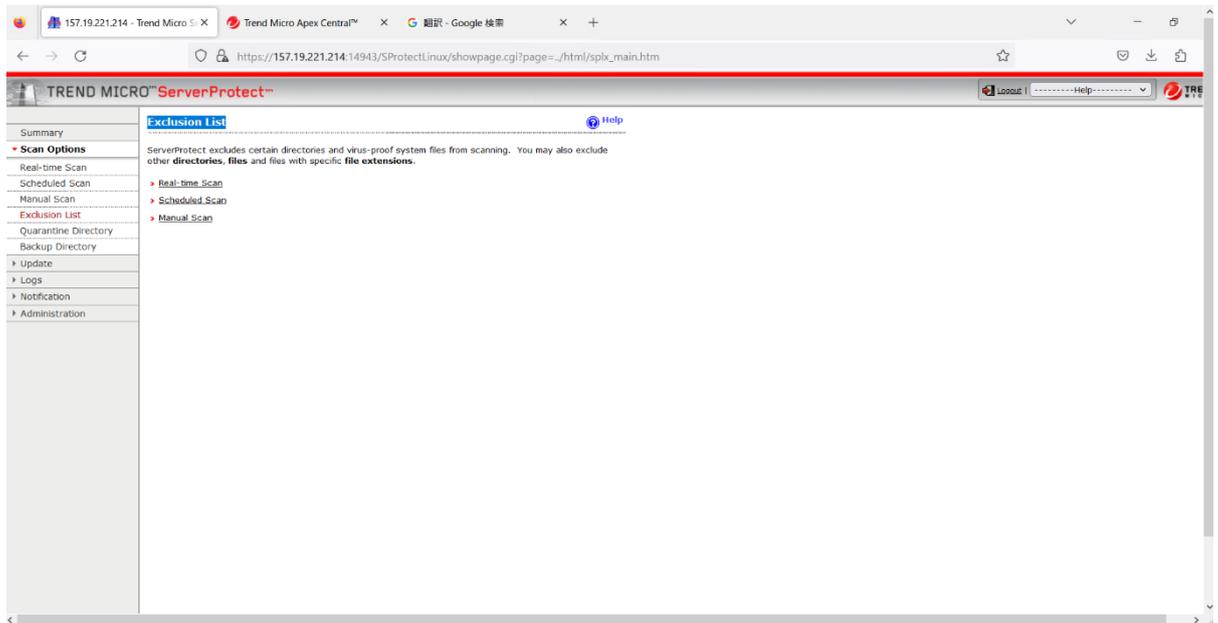
- ⑦ Change Password の「New Password」と「Confirm Password」に任意のパスワードを入力し、Save ボタンをクリックします。



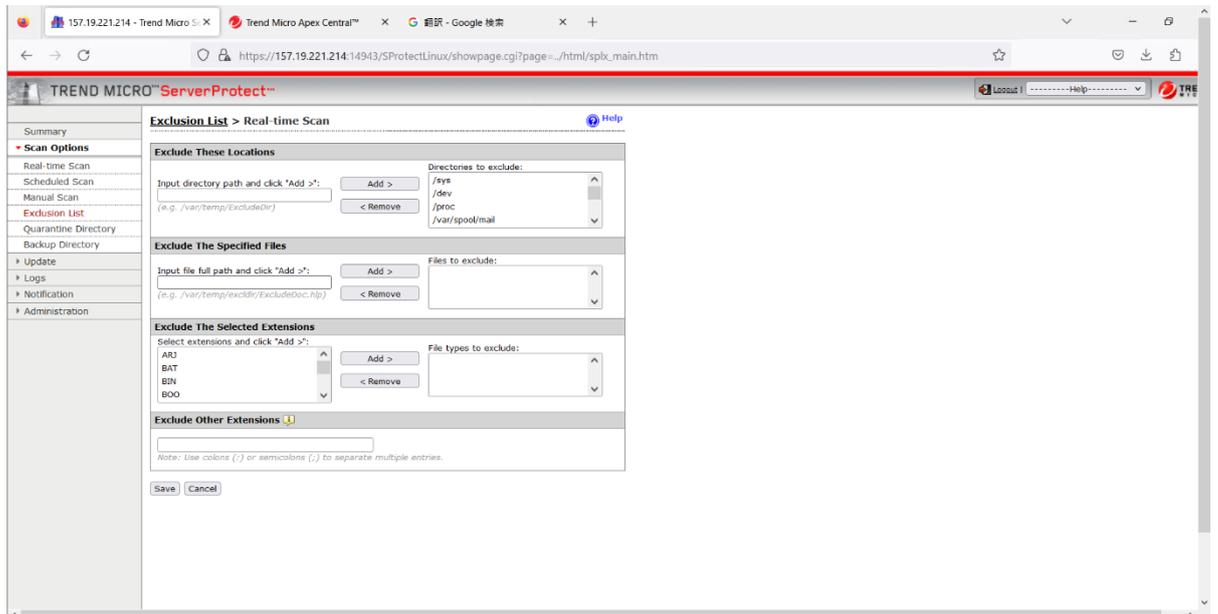
- ⑧ 左タブの「Administration」-「Product Registration」を選択します。
「Activation Code」に以下のライセンスコードを入力し、Register ボタンをクリックします。
SP-3K8N-DVTYL-ZGG27-96YCV-VKNK8-EW77K



- ⑨ リアルタイムスキャンを除外する設定をする場合は、左タブの「Scan Options」-「Exclusion List」を選択し、「Real-Time Scan」をクリックします。



- ⑩ 「Exclude These Locations」には除外フォルダ、「Exclude The Specified Files」は除外ファイルを設定し、Save ボタンをクリックします。



改版履歴

2023年11月6日	初版作成

2023年11月16日 初版発行

富士通 Japan 株式会社