

**ESET PROTECT on-prem
for Linux V13.1
インストール手順書**

**第1版
作成 : 2026年9月**

Canon
キヤノンマーケティングジャパン株式会社

概要

- 本資料はLinux版のESET PROTECT on-prem(EP on-prem) V13.1 を構築するための手順をまとめた資料です。
以下に記載の<環境構成>を前提とした手順のフローや注意点を記載しております。
- 本資料は作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。
ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能及び名称が異なっている場合があります。また本資料の内容は、予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複製、改変することを禁止します。

<環境構成>

OS	Rocky Linux9 (64bit)
EP on-prem	EP on-prem 13.1
サーバ	MySQL8.4
	MySQL ODBC 9.6ドライバ
Webコンソール	Apache/Tomcat9

<前提条件>

本資料は以下の前提条件をもとに手順を記載しております。

事前に前提条件で記載した内容を準備いただくようお願いいたします。

※本手順書は2026年9月時点の情報で作成しております。手順内のリンクやコマンドが利用できない場合はサポート対象の新しいバージョンに読み替えて実施いただくようお願いいたします。

※本手順書はカレントディレクトリを/tmpとして実施しています。

※本手順ではfirewalldは無効化せず、必要な通信ポートのみ開放する構成としています。

- ・インターネットに接続可能な状態であること
- ・Rocky Linux9がインストール済みであること
- ・Rocky Linux9はISOイメージはMinimalイメージを利用していること
- ・Rocky Linux9は以下のESET PROTECT on-premの動作環境、前提条件を満たしていること
-動作環境 <https://canon.jp/business/solution/it-sec/lineup/eset/feature/onpremises-security>
- ・SELinuxが有効化されていること ※1

※1. 環境によっては、SELinuxが有効な状態では正常に動作しない場合があります。
その場合は、環境への影響をご確認のうえ、SELinuxを無効化することをご検討ください。

<インストール手順>

インストール手順の概要は以下の通りになります。インストールを行う際は、0～7の順に実施をお願いいたします。
詳細につきましては、各シートをご参照下さい。

0. 事前準備
1. MySQLのセットアップ
2. MySQL管理者アカウントの設定
3. MySQL ODBCドライバのセットアップ
4. EP on-premサーバのインストール
5. Tomcatのインストール
6. EMエージェントのインストール
7. バックアップ

<参考情報>

レポート出力に失敗する場合

「/var/log/eset/RemoteAdministrator/Server/trace.log」を確認し、出力されているレポートのエラーメッセージを確認し、不足しているパッケージを追加でインストールしてください。

▽コマンド例

```
tail -f /var/log/eset/RemoteAdministrator/Server/trace.log | grep "Report printer tool had stderr output"
```

資料名	シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書	0.事前準備	1.0	
No1 #コンソールイメージ	コマンド/確認事項	チェック	
0-1.リリースノート あらかじめリリースノートを確認しておく リリースノートを一読 マクリック リリースノート	このリリースノートにはESET PROTECT on-prem for Linux V13.1を正しく利用するための情報が記載されています。 本製品をインストールする前に必ずお読みください。 【確認】 リリースノートを一読		
No2 #コンソールイメージ	コマンド/確認事項	チェック	
0-2.コンポーネントプログラム導入 ユーザーズサイトからコンポーネントをダウンロード コンポーネントプログラムは以下URLのユーザーズサイトよりダウンロードすることが可能です。 Linux版をダウンロードください。 マクリック ユーザーズサイト 	【確認】 コンポーネントプログラムがダウンロードされたこと	□	
No3 #コンソールイメージ	コマンド/確認事項	チェック	
0-3.必要パッケージの導入 <pre>[root@localhost tmp]# dnf install -y openssl</pre> (HTTPS/TLS通信の接続確認に使用) <pre>[root@localhost tmp]# dnf install -y cifs-utils</pre> (cifs-utils:Windows OSへのエージェント展開で必要) <pre>[root@localhost tmp]# dnf install -y openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap</pre> (ldapsearch:AD同期タスクと認証で使用) <pre>[root@localhost tmp]# dnf install -y lshw</pre> (lshw:エージェントがハードウェアインベントリを正しく報告するために必要) <pre>[root@localhost tmp]# dnf install -y policycoreutils-devel</pre> (SELinux develパッケージ:アプリケーションインストール中にSELinuxポリシーモジュールを構築するために使用) <pre>[root@localhost tmp]# dnf install -y gtk3</pre> (gtk3パッケージ:レポートの印刷に必要) ～以下任意～ <pre>[root@localhost tmp]# dnf install -y krb5-workstation</pre> (kinit + klist:ログイン時のドメインユーザー認証とActive Directory同期タスクで使用) <pre>[root@localhost tmp]# dnf install -y net-snmp-utils net-snmp</pre> (snmptrap:SNMPトラップを送信するために使用されます。SNMPも構成が必要) <pre>[root@localhost tmp]# dnf install -y samba samba-winbind-clients</pre> (リモート展開でのみ必要)	以下のコマンドを実行してください 【コマンド】 # dnf install -y openssl 【コマンド】 # dnf install -y cifs-utils 【コマンド】 # dnf install -y openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap 【コマンド】 # dnf install -y lshw 【コマンド】 # dnf install -y policycoreutils-devel 【コマンド】 # dnf install -y gtk3 【コマンド】 # dnf install -y krb5-workstation 【コマンド】 # dnf install -y net-snmp-utils net-snmp 【コマンド】 # dnf install -y samba samba-winbind-clients ※詳細はオンラインヘルプやリリースノートのP3「ESET PROTECT SERVER (Linux版)」からご確認ください。 オンラインヘルプ リリースノート	□ □ □ □ □ □ □ □	
No4 #コンソールイメージ	コマンド/確認事項	チェック	
0-4.コマンド導入 unzip,xauth,tarコマンド導入 <pre>[root@localhost tmp]# dnf install -y unzip</pre> <pre>[root@localhost tmp]#</pre> <pre>[root@localhost tmp]# dnf install -y xauth</pre> <pre>[root@localhost tmp]#</pre> <pre>[root@localhost tmp]# dnf install -y tar</pre>	以下のコマンドを実行してください 【コマンド】 # dnf install -y unzip 【コマンド】 # dnf install -y xauth 【コマンド】 # dnf install -y tar	□ □ 	

■資料名	■シート名	バージョン	備考
ESET PROTECT On-prem for Linux V13.1 インストール手順書	1.MySQLのセットアップ	1.0	
No1 #コンソールイメージ		コマンド/確認事項	チェック
1-1.MySQLサーバリポジトリのダウンロード 指定したURLからRPMファイルを取得する。(本手順書では/tmpを利用する) <pre>[root@localhost tmp]# dnf install -y https://dev.mysql.com/get/mysql84-community-release-el9-4.noarch.rpm</pre> ~~~~~途中省略~~~~~ インストール中 : mysql84-community-release-el9-4.noarch 1/1 検証中 : mysql84-community-release-el9-4.noarch 1/1 インストール済み: mysql84-community-release-el9-4.noarch 完了しました! <pre>[root@localhost tmp]# dnf config-manager --disable mysql-9.7-lts-community [root@localhost tmp]# dnf config-manager --disable mysql-tools-9.7-lts-community [root@localhost tmp]# dnf config-manager --enable mysql-8.4-lts-community [root@localhost tmp]# dnf config-manager --enable mysql-tools-8.4-lts-community</pre>		以下のコマンドを実行してください	
		【コマンド】# dnf install -y https://dev.mysql.com/get/mysql84-community-release-el9-4.noarch.rpm	☐
		【確認】エラー表記が表示されないこと ※インターネット接続できない環境の場合はエラー表記が表示されます。	☐
		【コマンド】# dnf config-manager --disable mysql-9.7-lts-community	☐
		【コマンド】# dnf config-manager --disable mysql-tools-9.7-lts-community	☐
		【コマンド】# dnf config-manager --enable mysql-8.4-lts-community	☐
		【コマンド】# dnf config-manager --enable mysql-tools-8.4-lts-community	☐
No2 #コンソールイメージ		コマンド/確認事項	チェック
1-2.MySQLサーバのインストール 1-1でインストールしたリポジトリを使用してMySQLサーバをインストールする。 <pre>[root@localhost tmp]# dnf install -y mysql-community-server</pre> ~~~~~途中省略~~~~~ インストール済み: <pre>mysql-community-client-8.4.9-1.el9.x86_64 mysql-community-plugin-8.4.9-1.el9.x86_64 mysql-community-common-8.4.9-1.el9.x86_64 mysql-community-icon-data-files-8.4.9-1.el9.x86_64 mysql-community-lib-8.4.9-1.el9.x86_64 mysql-community-server-8.4.9-1.el9.x86_64</pre> 完了しました! <pre>[root@localhost tmp]# mysql --version mysql Ver 8.4.9 for Linux on x86_64 (MySQL Community Server - GPL)</pre>		以下のコマンドを実行してください	
		【コマンド】# dnf install -y mysql-community-server	☐
		【確認】インストールが完了していること	☐
		【コマンド】# mysql --version	☐
		【確認】MySQL 8.4系がインストールされていること	☐
No3 #コンソールイメージ		コマンド/確認事項	チェック
1-3.MySQLサーバ起動/稼働確認 MySQLサーバインストール直後はデーモンが起動していないため、デーモンのステータスは確認せず起動から実施する。		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# systemctl start mysqld [root@localhost tmp]#</pre> <pre>[root@localhost tmp]# systemctl status mysqld</pre> mysqld.service – MySQL Server Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; preset: d> Active: active (running) since Thu 2025-12-25 09:26:55 JST; 9s ago Docs: man:mysqld(8) http://dev.mysql.com/doc/refman/en/using-systemd.html Process: 3264 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=exited, status> Main PID: 3333 (mysqld) Status: "Server is operational" Tasks: 38 (limit: 23022) Memory: 486.5M CPU: 2.759s CGroup: /system.slice/mysqld.service └─3333 /usr/sbin/mysqld <pre>Dec 26 09:26:51 localhost.localdomain systemd[1]: Starting MySQL Server... Dec 26 09:26:55 localhost.localdomain systemd[1]: Started MySQL Server.</pre>		【コマンド】# systemctl start mysqld	☐
		【コマンド】# systemctl status mysqld	☐
		【確認】MySQLサーバが起動(active)していること	☐
No4 #コンソールイメージ		コマンド/確認事項	チェック
1-4.MySQLサーバの自動起動設定 自動起動設定がされていない場合は、自動起動設定を実施する。		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# systemctl enable mysqld [root@localhost tmp]#</pre> <pre>[root@localhost tmp]# systemctl status mysqld</pre> mysqld.service – MySQL Server Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; preset: d> Active: active (running) since Thu 2024-12-26 09:40:37 JST; lmin 50s ago Docs: man:mysqld(8) http://dev.mysql.com/doc/refman/en/using-systemd.html Process: 3455 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=exited, status> Main PID: 3483 (mysqld) Status: "Server is operational" Tasks: 37 (limit: 23022) Memory: 363.1M CPU: 1.146s CGroup: /system.slice/mysqld.service └─3483 /usr/sbin/mysqld <pre>Dec 26 09:40:36 localhost.localdomain systemd[1]: Starting MySQL Server... Dec 26 09:40:37 localhost.localdomain systemd[1]: Started MySQL Server.</pre>		【コマンド】# systemctl enable mysqld	☐
		【コマンド】# systemctl status mysqld	☐
		【確認】自動起動(enabled)になっていることを確認	☐

No5 #コンソールイメージ	コマンド/確認事項	チェック
1-5.データベースの設定変更(1) 設定ファイルのバックアップを取得する <pre>[root@localhost tmp]# cp -a /etc/my.cnf /etc/my.cnf.bk [root@localhost tmp]# [root@localhost tmp]# [root@localhost tmp]# ls -alt /etc/ grep my.cnf -rw-r--r-- 1 root root 1243 Sep 18 21:18 my.cnf -rw-r--r-- 1 root root 1243 Sep 18 21:18 my.cnf.bk drwxr-xr-x 2 root root 6 Sep 18 21:18 my.cnf.d [root@localhost tmp]#</pre>	以下のコマンドを実行してください 【コマンド】 <code># cp -a /etc/my.cnf /etc/my.cnf.bk</code> 【コマンド】 <code># ls -alt /etc/ grep my.cnf</code> 【確認】バックアップファイルが作成されていること	☐ ☐ ☐
No6 #コンソールイメージ 1-6.データベースの設定変更(2) 設定ファイルの内容を変更する(MySQL 8系の場合) <pre>[root@localhost tmp]# vi /etc/my.cnf</pre> 途中省略 <pre># default-authentication-plugin=mysql_native_password datadir=/var/lib/mysql socket=/var/lib/mysql/mysql.sock log-error=/var/log/mysqld.log pid-file=/var/run/mysqld/mysqld.pid max_allowed_packet=33M default_password_lifetime=0 log_bin_trust_function_creators=1 innodb_log_file_size=100M innodb_log_files_in_group=2 [root@localhost tmp]# diff /etc/my.cnf /etc/my.cnf.bk 32,37d31 < max_allowed_packet=33M < default_password_lifetime=0 < log_bin_trust_function_creators=1 < innodb_log_file_size=100M < innodb_log_files_in_group=2 [root@localhost tmp]#</pre> 編集モード	【コマンド】 <code># vi /etc/my.cnf</code> 以下の値を追加する max_allowed_packet=33M default_password_lifetime=0 log_bin_trust_function_creators=1 innodb_log_file_size=100M innodb_log_files_in_group=2 【コマンド】 <code># diff /etc/my.cnf /etc/my.cnf.bk</code> ※MySQL8.0からバイナリログの取得がデフォルトでONになっているため、ストレージの負荷が懸念される場合は以下の値を追記する。 disable-log-bin=0 【確認】追加した内容が正しいこと	☐ ☐ ☐
No7 #コンソールイメージ 1-7.MySQLサーバを再起動/稼働確認 変更した設定ファイルを反映させるために、MySQLを再起動し、正常に稼働することを確認する。 <pre>[root@localhost tmp]# systemctl restart mysqld [root@localhost tmp]# [root@localhost tmp]# systemctl status mysqld</pre> ● mysqld.service – MySQL Server Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; preset: d) Active: active (running) since Thu 2025-12-26 09:40:37 JST; 10s ago Docs: man:mysqld(8) http://dev.mysql.com/doc/refman/en/using-systemd.html Process: 3455 ExecStartPre=usr/bin/mysqld_pre_systemd (code=exited, status> Main PID: 3483 (mysqld) Status: "Server is operational" Tasks: 38 (limit: 23022) Memory: 363.2M CPU: 1.006s CGroup: /system.slice/mysqld.service └─3483 /usr/sbin/mysqld Dec 26 09:40:36 localhost.localdomain systemd[1]: Starting MySQL Server... Dec 26 09:40:37 localhost.localdomain systemd[1]: Started MySQL Server.	以下のコマンドを実行してください 【コマンド】 <code># systemctl restart mysqld</code> 【コマンド】 <code># systemctl status mysqld</code> 【確認】MySQLサーバが起動(active)していること	☐ ☐ ☐

■ 資料名		■ シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書		2.MySQL管理者アカウントの設定	1.0	
No1	#コンソールイメージ	コマンド/確認事項	チェック	
2-1.MySQL管理者アカウントの初期パスワード確認 MySQL8.4では管理者アカウントに初期パスワードが設定されているため確認する。 [root@localhost tmp]# grep "temporary password" /var/log/mysqld.log 2024-12-26T00:26:52.856573Z 6 [Note] [MY-010454] [Server] A temporary password is generated for root@localhost: AKH:5YDgi#aE (例) [root@localhost tmp]#		以下のコマンドを実行してください 【コマンド】 # grep "temporary password" /var/log/mysqld.log 【確認】 「:」後のパスワードを確認する。 ※後述の手順で利用します。 2-1 パスワードメモ欄	☐ ☐	
No2	#コンソールイメージ	コマンド/確認事項	チェック	
2-2.管理者アカウントのパスワード変更 2-1で確認した管理者アカウントの初期パスワードを変更する。 [root@localhost tmp]# mysql_secure_installation Securing the MySQL server deployment. Enter password for user root: The existing password for the user account root has expired. Please set a new password. New password: Re-enter new password: The 'validate_password' component is installed on the server. The subsequent steps will run with the existing configuration of the component. Using existing password for root. Estimated strength of the password: 100 Change the password for root ? ((Press y Y for Yes, any other key for No) : n ... skipping. By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? (Press y Y for Yes, any other key for No) : y Success. Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? (Press y Y for Yes, any other key for No) : y Success. By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? (Press y Y for Yes, any other key for No) : y - Dropping test database... Success. - Removing privileges on test database... Success. Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? (Press y Y for Yes, any other key for No) : y Success. All done! [root@localhost tmp]#		以下のコマンドを実行してください 【コマンド】 # mysql_secure_installation Enter password for user root:= 2-1で確認した初期パスワード New password:= 任意のパスワード ※後続の手順で利用します。 Re-enter new password:= New passwordと同様のパスワード ※MySQL8.4ではパスワードポリシーの初期値が「MEDIUM」のため、パスワードには以下の条件を満たす必要があります。 ・パスワード長 8文字以上 ・大文字小文字 1文字以上 ・数字 1文字以上 ・記号 1文字以上 ※MySQL の管理者パスワードに、以下の文字を利用すると、EP のインストールに失敗することを確認しております。 { } 上記文字を利用しないよう、ご注意ください。 2-2 New password メモ欄	☐ ☐	

No3 #コンソールイメージ	コマンド/確認事項	チェック
2-3.MySQLに接続確認 2-2で変更したパスワードでMySQLにログインをする。 <pre>[root@localhost tmp]# mysql -u root -p Enter password: Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 20 Server version: 8.4.9 MySQL Community Server - GPL Copyright (c) 2000, 2026, Oracle and/or its affiliates. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. mysql> mysql> QUIT Bye [root@localhost tmp]#</pre>	以下のコマンドを実行してください 【コマンド】 # mysql -u root -p Enter password:= 2-2で設定したパスワード 【確認】 ログインできることを確認する。 【コマンド】 QUIT	☐ ☐ ☐

■資料名	■シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書	3.MySQL ODBCドライバのセットアップ	1.0	
No1 #コンソールイメージ	コマンド/確認事項	チェック	
3-1.ODBCドライバのインストール dnfコマンドでODBCドライバのインストールをする			
[root@localhost tmp]# dnf install -y mysql-connector-odbc-9.6.0	【コマンド】# dnf install -y mysql-connector- odbc-9.6.0	☐	
~~~~~途中省略~~~~~ 検証中 : mysql-connector-odbc-9.6.0-1.el9.x86_64                  3/3	【確認】ドライバがインストールされたこと	<input type="checkbox"/>	
インストール済み: mysql-connector-odbc-9.6.0-1.el9.x86_64 unixODBC-2.3.9-4.el9.x86_64			
完了しました!			
[root@localhost tmp]# [root@localhost tmp]# dnf list installed   grep odbc mysql-connector-odbc.x86_64                  9.6.0-1.el9 @mysql-connectors-community	【コマンド】# dnf list installed   grep odbc	<input type="checkbox"/>	
[root@localhost tmp]#	【確認】MySQL Connector/ODBC 9.6系がインス トールされていること	<input type="checkbox"/>	
No2 #コンソールイメージ	コマンド/確認事項	チェック	
3-2.ODBCドライバの設定ファイルのバックアップ 設定ファイルのバックアップを取得する			
[root@localhost tmp]# cp -a /etc/odbcinst.ini /etc/odbcinst.ini.bk	【コマンド】# cp -a /etc/odbcinst.ini /etc/odbcinst.ini.bk	<input type="checkbox"/>	
[root@localhost tmp]#			
[root@localhost tmp]# ls -alt /etc/   grep odbcinst.ini	【コマンド】# ls -alt /etc/   grep odbcinst.ini	<input type="checkbox"/>	
-rw-r--r--      1 root root        928 DEC 25   2025 odbcinst.ini			
-rw-r--r--      1 root root        928 DEC 25   2025 odbcinst.ini.bk	【確認】バックアップファイルが作成されていること	<input type="checkbox"/>	
[root@localhost tmp]#			
No3 #コンソールイメージ	コマンド/確認事項	チェック	
3-3.ODBCドライバの設定ファイル変更 ODBCドライバの設定ファイルをドライバが利用可能な状態に修正する			
[root@localhost tmp]# vi /etc/odbcinst.ini	【コマンド】# vi /etc/odbcinst.ini	<input type="checkbox"/>	
(変更前) [MySQL] Description = ODBC for MySQL 8 Driver = /usr/lib/libmyodbc8.so Driver64 = /usr/lib64/libmyodbc8.so FileUsage = 1	(変更前)の内容を変更して(変更後)のようにする	<input type="checkbox"/>	
(変更後) [MySQL] Description = MySQL ODBC 9.6 Unicode Driver Driver = /usr/lib64/libmyodbc9w.so                  (モジュール名変更) #Driver64 = /usr/lib64/libmyodbc8.so                  (コメントアウト) UsageCount = 1			
[root@localhost tmp]#			

No4	#コンソールイメージ	コマンド/確認事項	チェック
<b>3-4.ODBCドライバの設定ファイル変更箇所の確認</b> ODBCドライバの設定ファイルの変更箇所を確認する		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# diff /etc/odbcinst.ini /etc/odbcinst.ini.bk 11,14c11,14 &lt; Description = MySQL ODBC 9.6 Unicode Driver &lt; Driver = /usr/lib64/libmyodbc9w.so &lt; #Driver64 = /usr/lib64/libmyodbc8.so &lt; UsageCount = 1 --- &gt; Description = ODBC for MySQL 8 &gt; Driver = /usr/lib/libmyodbc8.so &gt; Driver64 = /usr/lib64/libmyodbc8.so &gt; FileUsage = 1 [root@localhost tmp]#</pre>		<b>【コマンド】</b> # diff /etc/odbcinst.ini /etc/odbcinst.ini.bk  <b>【確認】</b> 修正箇所と変更内容が正しいか確認する 11,14c11,14 < Description = MySQL ODBC 9.6 Unicode Driver < Driver = /usr/lib64/libmyodbc9w.so < #Driver64 = /usr/lib64/libmyodbc8.so < UsageCount = 1 --- > Description = ODBC for MySQL 8 > Driver = /usr/lib/libmyodbc8.so > Driver64 = /usr/lib64/libmyodbc8.so > FileUsage = 1	<input type="checkbox"/>  <input type="checkbox"/>
No5	#コンソールイメージ	コマンド/確認事項	チェック
<b>3-5.ODBCドライバの設定ファイル変更の更新</b> 3-4で変更した設定を更新する		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# odbcinst -i -d -f /etc/odbcinst.ini odbcinst: Driver installed. Usage count increased to 2. Target directory is /etc odbcinst: Driver installed. Usage count increased to 2. Target directory is /etc odbcinst: Driver installed. Usage count increased to 2. Target directory is /etc odbcinst: Driver installed. Usage count increased to 2. Target directory is /etc odbcinst: Driver installed. Usage count increased to 2. Target directory is /etc [root@localhost tmp]#</pre>		<b>【コマンド】</b> # odbcinst -i -d -f /etc/odbcinst.ini	<input type="checkbox"/>

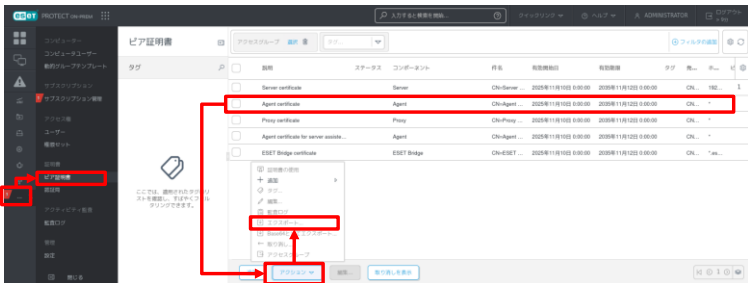
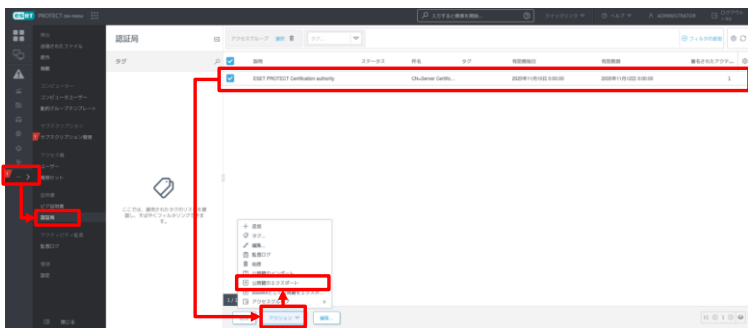
資料名	シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書	4.EP on-premサーバのインストール	1.0	
<b>No1 #コンソールイメージ</b>		<b>コマンド/確認事項</b>	<b>チェック</b>
<b>4-1.Firewalldの設定</b>		以下のコマンドを実行してください	
Firewalldに必要なポートを開放する			
[root@localhost tmp]# <b>firewall-cmd --permanent --add-port=2222/tcp</b>		<b>【コマンド】 # firewall-cmd --permanent --add-port=2222/tcp</b>	
[root@localhost tmp]#			
[root@localhost tmp]# <b>firewall-cmd --permanent --add-port=8443/tcp</b>		<b>【コマンド】 # firewall-cmd --permanent --add-port=8443/tcp</b>	□
[root@localhost tmp]#			
[root@localhost tmp]# <b>firewall-cmd --permanent --add-port=8080/tcp</b>		<b>【コマンド】 # firewall-cmd --permanent --add-port=8080/tcp</b>	
[root@localhost tmp]#			
[root@localhost tmp]# <b>firewall-cmd --reload</b>		<b>【コマンド】 # firewall-cmd --reload</b>	
[root@localhost tmp]#			
[root@localhost tmp]# <b>firewall-cmd --list-ports</b>		<b>【コマンド】 # firewall-cmd --list-ports</b>	
2222/tcp 8443/tcp 8080/tcp			
[root@localhost tmp]#		2222: クライアント (EMエージェント) 接続用 8080: Webコンソール(http)用(※1) 8443: Webコンソール(https)用(※1)	
		※1 Tomcatの設定により変わります	
		上記は最小構成となっております。詳細は以下リンクをご確認ください。 <a href="#">通信要件について</a>	□
<b>No2 #コンソールイメージ</b>			<b>チェック</b>
<b>4-2. OpenSSL のバージョン確認</b>		以下のコマンドを実行してください	
OpenSSL のバージョンがサポートされているもの確認する。			
[root@localhost tmp]# <b>openssl version</b>		<b>【コマンド】 # openssl version</b>	
OpenSSL X.X.X.X Nov20XX (Library:OpenSSL X.X.X. X XX XXXX )		<b>【確認】</b> サポートされているバージョンであるか確認する ※詳細は以下をご参照ください。 マクロック <a href="#">リリースノート</a>	
[root@localhost tmp]#		サポート対象外のバージョンの場合は「 <a href="https://openssl-library.org/source/">https://openssl-library.org/source/</a> 」より、対象のバージョンのプログラムをダウンロードしてください。サポート対象バージョンについては以下オンラインヘルプにてご確認ください。 <a href="#">マクロック</a> <a href="#">オンラインヘルプ</a>	
[root@localhost tmp]#		※複数のバージョンの OpenSSL を同時にインストールできるため、複数表示される場合があります。	
<b>No3 #コンソールイメージ</b>		<b>コマンド/確認事項</b>	<b>チェック</b>
<b>4-3. インストーラーに実行権限を付与</b>		以下のコマンドを実行してください	
インストーラーに実行権限を付与する(/tmpフォルダにLinux版EP on-premのコンポーネントプログラムを配置しております)			
[root@localhost tmp]# <b>unzip Component_Linux_x64.zip</b>		<b>【コマンド】 # unzip Component_Linux_x64.zip</b>	□
Archive: Component_Linux_x64.zip			
inflating: Agent-Linux-x86_64.sh			
inflating: era.war			
inflating: eset-bridge.x86_64.bin			
inflating: RDSensor-Linux-x86_64.sh			
inflating: Server-Linux-x86_64.sh			
[root@localhost tmp]#			
[root@localhost tmp]#			
[root@localhost tmp]# <b>chmod 700 Server-Linux-x86_64.sh</b>		<b>【コマンド】 # chmod 700 Server-Linux-x86_64.sh</b>	□
[root@localhost tmp]#			
[root@localhost tmp]# <b>ls -alt Server-Linux-x86_64.sh</b>		<b>【コマンド】 # ls -alt Server-Linux-x86_64.sh</b>	□
[root@localhost tmp]#			
-rwx----- 1 root root 88911629 6月 19 15:21 Component_Linux_x64/Server-Linux-x86_64.sh		<b>【確認】</b> パーMISSIONの確認をする。所有者に実行権限が付与されていること。	□
[root@localhost tmp]#			

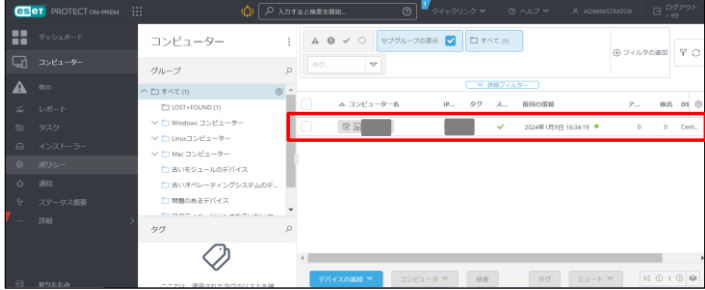
No4 #コンソールイメージ	コマンド/確認事項	チェック
<b>4-4.EP on-premサーバのインストーラーを実行</b> EP on-premサーバのインストーラーを実行しインストールを開始する  <pre>[root@localhost tmp]# ./Server-Linux-x86_64.sh --locale=ja-JP --skip-license --db-driver="MySQL" --db-hostname=127.0.0.1 --db-port=3306 --db-admin-username=root --db-admin-password=xxxxxxx --server-root-password=xxxxxxx --db-user-username=era-server-user --db-user-password=xxxxxxx --cert-hostname=*</pre>  ESET PROTECT On-Prem Server Installer (version: 13.1.443.0), Copyright © 1992-2025 ESET, spol. s r.o. - All rights reserved.   ~~~~~ 中略 ~~~~~   Removed backup directory: /opt/eset/RemoteAdministrator/.Server-936619589 <b>Product installed.</b> [root@localhost tmp]#	以下のコマンドを実行してください   【コマンド】# ./Server-Linux-x86_64.sh --locale=ja-JP --skip-license --db-driver="MySQL" --db-hostname=127.0.0.1 --db-port=3306 --db-admin-username=root --db-admin-password=xxxxxxx --server-root-password=xxxxxxx --db-user-username=era-server-user --db-user-password=xxxxxxx --cert-hostname=*   db-admin-password= &lt;手順2-2&gt;で設定した管理者アカウントのパスワード server-root-password= EP Webコンソールの管理者の初期パスワード db-user-password= EPが使用するデータベースのユーザーのパスワード   ※&lt;db-admin-password&gt;、&lt;server-root-password&gt;、&lt;db-user-password&gt;に以下の文字を利用する場合、文字の直前にエスケープシーケンスを入力する必要があります。 &lt;エスケープすれば使用できる文字&gt; ! " # \$ % ' ( ) * + , - . : ; &lt; &gt; [ \ ] ^ _ ` {   } ~ (エスケープシーケンスは ` を入力してください。)   ※エスケープシーケンス…一部の文字では、システム上特殊な役割を持つものがあります。これらの文字が持つ役割を無効化するために、その文字の直前に記載する文字をエスケープシーケンスと呼びます。   また、&lt;db-admin-password&gt;、&lt;server-root-password&gt;、&lt;db-user-password&gt;に以下の文字を利用すると、EP on-premのインストールに失敗するため、利用しないようご注意ください。 &lt;使用できない文字&gt; { }   ※&lt;server-root-password&gt;には、小文字、大文字、数字、特殊文字のうち3つのカテゴリを含む14文字以上で設定ください。   【確認】正常にインストールされたことを確認する。     4-4 server-root-password メモ欄   4-4 db-user-password メモ欄	□   □
<b>No5 #コンソールイメージ</b> <b>4-5.EP on-premサーバの起動確認</b> EP on-premサーバインストール完了後、正常に起動しているか確認する  <pre>[root@localhost tmp]# systemctl status eraserver ● eraserver.service - ESET PROTECT Server    Loaded: loaded (/etc/systemd/system/eraserver.service; enabled; preset: disabled)    Active: active (running) since Thu 2025-12-26 10:52:39 JST; 4min 43s ago      Process: 4623 ExecStart=/opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid (code=exited)     Main PID: 4624 (ERAServer)        Tasks: 49 (limit: 23022)       Memory: 269.6M          CPU: 7.038s     CGroup: /system.slice/eraserver.service             └─4624 /opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid</pre>  Dec 26 10:52:39 localhost.localdomain systemd[1]: Starting ESET PROTECT Server...   Dec 26 10:52:39 localhost.localdomain systemd[1]: Started ESET PROTECT Server.   ~~~~~ 以下、省略 ~~~~~   [root@localhost tmp]#	以下のコマンドを実行してください   【コマンド】# systemctl status eraserver   【確認】EPサービスが稼働しているか確認する。	□   □
<b>No6 #コンソールイメージ</b> <b>4-6.MySQLサーバの稼働確認</b> EP on-prem用のデータベースが作成されていること  <pre>[root@localhost tmp]# mysql -u era-server-user -p Enter password: Welcome to the MySQL monitor.  Commands end with ; or \g. Your MySQL connection id is 20 Server version: 8.4.9 MySQL Community Server - GPL ~~~~~ 中略 ~~~~~ Type 'help;' or '\h' for help. Type '\C' to clear the current input statement. mysql&gt; show databases; +-----+   Database   +-----+   era_db       information_schema     performance_schema   +-----+ 5 rows in set (0.00 sec) mysql&gt; QUIT Bye [root@localhost tmp]#</pre>	以下のコマンドを実行してください   【コマンド】# mysql -u era-server-user -p   Enter password:= 4-4で設定したパスワード   【コマンド】&gt; show databases;   【確認】era_dbが作成されていること   【コマンド】QUIT	□   □   □

資料名	シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書	5.Tomcatのインストール	1.0	
No1 #コンソールイメージ	コマンド/確認事項	チェック	
<b>5-1.Java17のインストール</b> Java実行環境をインストールする <pre>[root@localhost tmp]# dnf install -y https://corretto.aws/downloads/latest/amazon-corretto- 17-x64-linux-jdk.rpm</pre>  途中省略~~~~~  <pre>Installing      : java-17-amazon-corretto-devel-1:17.0.17.10-1.x86_64 l/1 Running scriptlet: java-17-amazon-corretto-devel-1:17.0.17.10-1.x86_64 l/1 Verifying       : java-17-amazon-corretto-devel-1:17.0.17.10-1.x86_64 l/1  Installed: java-17-amazon-corretto-devel-1:17.0.17.10-1.x86_64</pre>  完了しました! [root@localhost tmp]#	コマンドを実行してください 【コマンド】# <code>dnf install -y https://corretto.aws/downloads/latest/amazon-corretto-17-x64-linux-jdk.rpm</code> ※本手順ではAmazon Correttoを利用します。 【確認】インストールされたことを確認する	<input type="checkbox"/>	<input type="checkbox"/>
No2 #コンソールイメージ	コマンド/確認事項	チェック	
<b>5-2.Tomcatのインストール</b> Tomcatをインストールする <pre>[root@localhost tmp]# dnf install -y tomcat</pre>  途中省略~~~~~  <pre>tomcat-jsp-2.3-api-1:9.0.117-2.el9_8.noarch tomcat-lib-1:9.0.117-2.el9_8.noarch tomcat-native-1:l/3.8-1.el9.x86_64 tomcat-servlet-4.0-api-1:9.0.117-2.el9_8.noarch tzdata-java-2026b-a.el9_8.noarch [root@localhost tmp]#</pre>	コマンドを実行してください 【コマンド】# <code>dnf install -y tomcat</code> ※表示されるTomcatのバージョンは、インストール時期やリポジトリの提供状況によって異なる場合があります。	<input type="checkbox"/>	
No3 #コンソールイメージ	コマンド/確認事項	チェック	
<b>5-3.webコンソールパッケージの設定</b> 任意のディレクトリに事前に用意したファイルを所定の場所に配置する <pre>[root@localhost tmp]# cp era.war /var/lib/tomcat/webapps/ [root@localhost tmp]# [root@localhost tmp]# ls -alt /var/lib/tomcat/webapps/   grep era.war</pre>  <code>-rw-r--r-- 1 root root    166310575   6月 19 16:18 era.war</code>  <pre>[root@localhost tmp]#</pre>	コマンドを実行してください 【コマンド】# <code>cp era.war /var/lib/tomcat/webapps/</code> 【コマンド】# <code>ls -alt /var/lib/tomcat/webapps/   grep era.war</code> 【確認】所定の場所にera.warが配置されたこと	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
No4 #コンソールイメージ	コマンド/確認事項	チェック	
<b>5-4.WEBコンソールをSSL通信で使用するための鍵の生成（実際は1行で続けて実行）</b> 鍵を生成し、所定の場所に配置する <pre>[root@localhost tmp]# keytool -genkeypair -keystore RSA -keysize 4096 -dname "CN=Unknown, OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=Unknown"-alias tomcat -keystore .keystore -storepass xxxxxx -validity 3650</pre> <pre>[root@localhost tmp]# mv .keystore /etc/tomcat/.keystore</pre> <pre>[root@localhost tmp]# ls -alt /etc/tomcat/.keystore   grep .keystore</pre>  <code>-rw-r--r-- 1 root root     3913   6月 19 16:18 .keystore</code>  <pre>[root@localhost tmp]#</pre>	コマンドを実行してください 【コマンド】# <code>keytool -genkeypair -keystore RSA -keysize 4096 -dname "CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown" -alias tomcat -keystore .keystore -storepass xxxxxx -validity 3650</code> ※ -dname 内のユーザー情報は環境に合わせて設定してください。 ※ -storepassには、キーストアに設定する任意のパスワードを指定してください。このパスワードは、後述のTomcatのSSL設定で使用します 【コマンド】# <code>mv .keystore /etc/tomcat/.keystore</code> 【コマンド】# <code>ls -alt /etc/tomcat/.keystore   grep .keystore</code> 【確認】所定の場所に.keystoreが配置されたこと  5-4 キーストアパスワード (storepass) メモ欄	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
No5 #コンソールイメージ	コマンド/確認事項	チェック	
<b>5-5.Tomcat設定ファイルのバックアップ</b> Tomcatの設定ファイルのバックアップを取得する <pre>[root@localhost tmp]# cp -a /etc/tomcat/server.xml /etc/tomcat/server.xml.bk</pre> <pre>[root@localhost tmp]# ls -alt /etc/tomcat/   grep server.xml</pre>  <code>-rw----- 1 tomcat tomcat 8022 Dec 6 04:50 server.xml</code>   <code>-rw----- 1 tomcat tomcat 8022 Dec 6 04:50 server.xml.bk</code>  <pre>[root@localhost tmp]#</pre>	コマンドを実行してください 【コマンド】# <code>cp -a /etc/tomcat/server.xml /etc/tomcat/server.xml.bk</code> 【コマンド】# <code>ls -alt /etc/tomcat/   grep server.xml</code> 【確認】バックアップファイルが作成されていること	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

No6	#コンソールイメージ	コマンド/確認事項	チェック
<b>5-6. TomcatのSSLの設定</b> SSL設定を有効にするため、設定ファイルを修正する		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# vi /etc/tomcat/server.xml</pre> (変更前)           <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443           . . .           -->           <!--           <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"             maxThreads="150" SSLEnabled="true"             maxParameterCount="1000"             >             <SSLHostConfig>               <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"                 type="RSA" />             </SSLHostConfig>           </Connector>           -->           (変更後)           <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443           . . .           -->           <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"             maxThreads="150" SSLEnabled="true"             maxParameterCount="1000"             >             <SSLHostConfig>               <Certificate                 certificateKeystoreFile="/etc/tomcat/.keystore"                 certificateKeystorePassword="キーストアのパスワード"                 type="RSA" />             </SSLHostConfig>           </Connector>		<b>【コマンド】</b> # vi /etc/tomcat/server.xml	<input type="checkbox"/>
		<b>【確認】</b> 以下の2項目が追加され、コメントアウト(<!-- -->)を削除していること ①certificateKeystoreFile="/etc/tomcat/.keystore" ②certificateKeystorePassword="【5-4で設定したキーストアのパスワード】" ※似たような箇所が多いので間違った所に記載しないよう注意	<input type="checkbox"/>
<b>No7 #コンソールイメージ</b> <b>5-7. Tomcatの起動</b> Tomcatが正常に起動するか確認する		以下のコマンドを実行してください	
<pre>[root@localhost tmp]# systemctl start tomcat</pre> <pre>[root@localhost tmp]#</pre> <pre>[root@localhost tmp]# systemctl status tomcat</pre> <pre>● tomcat.service - Apache Tomcat 9    Loaded: loaded (/etc/systemd/system/tomcat.service; disabled; vendor preset: disabled)    Active: active (exited) since Thu 2025-12-26 12:39:51 JST; 43s ago      Process: 54400 ExecStart=/var/lib/tomcat/bin/startup.sh (code=exited, status=0/SUCCESS)     Main PID: 54400 (code=exited, status=0/SUCCESS)       CGroup: /system.slice/tomcat.service               mq54414 /usr/bin/java -Djava.util.logging.config.file=/var/lib/tom...</pre> 以下省略           [root@localhost tmp]#		<b>【コマンド】</b> # systemctl start tomcat <b>【コマンド】</b> # systemctl status tomcat	<input type="checkbox"/> <input type="checkbox"/>
		<b>【確認】</b> Tomcatが稼働しているか確認する。	<input type="checkbox"/>
<b>No8 #コンソールイメージ</b> <b>5-8-1.Webコンソール接続の確認(1)</b> WebブラウザよりEP on-premにアクセスする(本手順で利用しているブラウザはChromeです)			
<a href="https://[サーバのIPアドレス]:8443/era/webconsole">https://[サーバのIPアドレス]:8443/era/webconsole</a>			<input type="checkbox"/>
		https://「IPアドレス」:8443/era/webconsole ※以下、Chromeで説明します。 左記画面が表示されたら「詳細設定」ボタンを押下する	
<b>No8 #コンソールイメージ</b> <b>5-8-2.Webコンソール接続の確認(2)</b> WebブラウザよりEP on-premにアクセスする			
		<b>「IPアドレス」にアクセスする(安全ではありません)」</b> <b>ボタンを押下する</b>	<input type="checkbox"/>

No8 #コンソールイメージ	コマンド/確認事項	チェック
<b>5-8-3.Webコンソール接続の確認(3)</b> WebブラウザよりEP on-premにアクセスする   	<b>【確認】</b> ESET PROTECT on-premのTOP画面が表示されること ※ESET PROTECT on-premのログイン画面が表示されたら管理者ユーザでログイン ・ユーザ名 : Administrator ・パスワード : 4-4で設定したserver-root-passwordの値、言語は「日本語」を選択します。   ※初回ログイン時に、サブスクリプションの登録画面が表示される場合があります。 サブスクリプションの登録は、ESET PROTECT On-Prem サーバーの構築において必須ではありません。 ただし、管理対象端末へESETセキュリティ製品を導入・アクティベーションする際に必要です。登録方法の詳細は、以下のオンラインヘルプをご確認ください。 マククリック <a href="#">オンラインヘルプ</a>	<input type="checkbox"/>
<b>No9 #コンソールイメージ</b>   <b>5-9. Tomcatの自動起動の設定</b> Tomcatは初期設定ではサーバ起動時に自動起動する設定になっていないため、自動起動するように設定する   <pre>[root@localhost tmp]# <b>systemctl enable tomcat</b> Created symlink from /etc/systemd/system/multi-user.target.wants/tomcat.service to /etc/systemd/system/tomcat.service. [root@localhost tmp]# <b>systemctl status tomcat</b> ● tomcat.service - Apache Tomcat 9    Loaded: loaded (/etc/systemd/system/tomcat.service; <b>enabled</b>; vendor preset: disabled)    Active: active (exited) since Thu 2025-12-26 12:39:51 JST; 19min ago    Main PID: 53926 (code=exited, status=0/SUCCESS)    CGroup: /system.slice/tomcat.service            mq53940 /usr/bin/java -  ~~~~~以下省略~~~~~ [root@localhost tmp]#</pre>	以下のコマンドを実行してください   <b>【コマンド】</b> # <b>systemctl enable tomcat</b>  <b>【コマンド】</b> # <b>systemctl status tomcat</b>  <b>【確認】</b> 自動起動のための設定が反映されていること	<input type="checkbox"/>   <input type="checkbox"/>   <input type="checkbox"/>

■ 資料名		■ シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書		6. EMIエージェントのインストール	1.0	
No1 #コンソールイメージ		コマンド/確認事項	チェック	
<b>6-1. WebブラウザよりEP on-premにアクセスする</b> 前提条件として、エージェントの証明書およびサーバー認証機関公開鍵が任意の場所に保存してある必要があるため、Webコンソールよりエージェントの証明書およびサーバー認証機関公開鍵のエクスポートを行います		【確認】EP on-premのTOP画面が表示されること   ※EP on-premのログイン画面が表示されたら管理者ユーザでログイン      ・ユーザ名：Administrator    ・パスワード：4-4で設定したserver-root-passwordの値、言語は「日本語」を選択します。	<input type="checkbox"/>	
				
No2 #EMIエージェントの証明書と認証局のエクスポート		コマンド/確認事項	チェック	
<b>6-2-1. 証明書のエクスポート</b> EP on-premのWebコンソールからEMIエージェントの証明書をエクスポートします。		【確認】EP on-premの画面左側のメインセクションより、「詳細」-「ピア証明書」を選択し、「エージェント証明書」がエクスポートできることを確認します。	<input type="checkbox"/>	
1. [詳細] - [ピア証明書] より、エクスポートを行う、[Agent certificate (コンポーネント：Agent)]を選択し、「アクション」より「エクスポート」をクリックします。				
2.エクスポートした証明書を任意の保存先に保存します。 ※保存した証明書は、「6-3-2.EMIエージェントのインストーラーを実行」で使用します。 また、障害発生時や再構築に備え、任意の保存先の保管したうえで、適切にバックアップしてください。		【確認】任意の場所に保存できている	<input type="checkbox"/>	
No2 #EMIエージェントの証明書と認証局のエクスポート		コマンド/確認事項	チェック	
<b>6-2-2. 認証局のエクスポート</b> 手順5-8で接続した、EP on-premのWebコンソールから公開鍵（認証局）をエクスポートします。		【確認】EP on-premの画面左側のメインセクションより、「詳細」-「認証局」を選択し、「公開鍵（認証局）」がエクスポートできることを確認します。	<input type="checkbox"/>	
1. [詳細] - [認証局] より、エクスポートを行う認証局、[ESET PROTECT Certification authority] を選択し、「アクション」より「公開鍵のエクスポート」をクリックします。				
2.エクスポートした証明書を任意の保存先に保存します。 ※保存した公開鍵（認証局）は、「6-3-2.EMIエージェントのインストーラーを実行」で使用します。 また、障害発生時や再構築に備え、任意の保存先の保管したうえで、適切にバックアップしてください。		【確認】任意の場所に保存できている	<input type="checkbox"/>	

<b>No3 #コンソールイメージ</b>   <b>6-3-1. インストーラーに実行権限を付与</b>   インストーラーに実行権限を付与する(/tmpフォルダにLinux版EP on-premのコンポーネントプログラムを配置し)  <pre>[root@localhost tmp]# chmod 700 Agent-Linux-x86_64.sh [root@localhost tmp]# [root@localhost tmp]# ls -alt Agent-Linux-x86_64.sh -rwx----- 1 root root 48615366 6月 19 17:13 Agent-Linux-x86_64.sh [root@localhost tmp]#</pre>	<b>コマンド/確認事項</b>   以下のコマンドを実行してください   【コマンド】 # <code>chmod 700 Agent-Linux-x86_64.sh</code>   【コマンド】 # <code>ls -alt Agent-Linux-x86_64.sh</code>   【確認】 パーMISSIONの確認をする。所有者に実行権限が付与されていること   チェック
<b>No3 #コンソールイメージ</b>   <b>6-3-2. EMIエージェントのインストーラーを実行</b>   EMIエージェントのインストーラーを実行しインストールを開始する(エクスポートした証明書と認証局を指定します)  <pre>[root@localhost tmp]# ./Agent-Linux-x86_64.sh --skip-license --cert-path=/tmp/agent.pfx --cert-auth-path=/tmp/CA.der --hostname=127.0.0.1 --port=2222</pre>  Initialized log file: /var/log/eset/RemoteAdministrator/EraAgentInstaller.log   ESET Management Agent Installer (version: 11.2.2076.0), Copyright c 1992-2025 ESET, spol. s r.o. - All rights reserved.   ~~~~~途中省略~~~~~   Service started. Product installed. [root@localhost tmp]#	<b>コマンド/確認事項</b>   以下のコマンドを実行してください   【コマンド】 # <code>./Agent-Linux-x86_64.sh --skip-license --cert-path= [(例)/tmp/agent.pfx] --cert-auth-path=[(例)/tmp/CA.der] --hostname=127.0.0.1 --port=2222</code>   --cert-path= 証明書を保存したパスを指定 --cert-auth-path= 公開鍵(認証局)を保存したパスを指定   【確認】 EMエージェントのインストールが完了していること   チェック
<b>No4 #コンソールイメージ</b>   <b>6-4-1. 管理されていることの確認 (1)</b>   WebブラウザよりEP on-premにアクセスする  	<b>コマンド/確認事項</b>   【確認】 EP on-premのTOP画面が表示されること ※EP on-premのログイン画面が表示されたら管理者ユーザでログイン ・ユーザ名: Administrator ・パスワード: 4-4で設定した--server-root-passwordの値、言語は「日本語」を選択します。   チェック
<b>No4 #コンソールイメージ</b>   <b>6-4-2. 管理されていることの確認 (2)</b>   EP on-premのメインセクション「コンピュータ」より、EP on-premサーバ自身が管理されていることを確認する  	<b>コマンド/確認事項</b>   【確認】 EP on-premの画面左側のメインセクションより、「コンピュータ」を選択し、EP on-premサーバ自身が管理されていることを確認します。   チェック

■ 資料名		■ シート名	バージョン	備考
ESET PROTECT on-prem for Linux V13.1 インストール手順書		7.バックアップ	1.0	
No1 #コンソールイメージ		コマンド/確認事項		チェック
<b>7-1-1.DBのバックアップ(1)</b> EP on-premのサービスを停止する		以下のコマンドを実行してください。		
<pre>[root@localhost tmp]# systemctl stop eraserver [root@localhost tmp]# [root@localhost tmp]# systemctl status eraserver systemctl status eraserver ● eraserver.service - ESET PROTECT Server    Loaded: loaded (/etc/systemd/system/eraserver.service; enable; vender preset; disabled)    Active: inactive (dead) since 火 2024-06-18 11:36:13 JST; 6s ago  Main PID: 18024 (code=exited, status=0/SUCCESS)  1月 09 16:03:45 localhost.localdomain systemd [1] stopped ESET PROTECT Server. 1月 09 16:03:45 localhost.localdomain systemd [1] starting ESET PROTECT Ser... ~~~~~ 以下、省略 ~~~~~</pre>		【コマンド】 # systemctl stop eraserver  【コマンド】 # systemctl status eraserver		<input type="checkbox"/>  <input type="checkbox"/>
No1 #コンソールイメージ		コマンド/確認事項		チェック
<b>7-1-2. DBのバックアップ (2)</b> DBをバックアップする		以下のコマンドを実行してください。		
<pre>[root@localhost tmp]# mysqldump --disable-keys --extended-insert --routines -u root -p era_db &gt; /tmp/mysqldump Enter password: [root@localhost tmp]# [root@localhost tmp]# ls -alt mysqldump -rw-r--r-- 1 root root 12282921  6月  18  11:39 mysqldump</pre>		【コマンド】 # mysqldump --disable-keys --extended-insert --routines -u root -p era_db > /tmp/mysqldump Enter password: 「Enter password:」にて2-2で設定したDBのパスワードを入力する 【コマンド】 # ls -alt mysqldump 【確認】 mysqldumpが作成されていることを確認する		<input type="checkbox"/>  <input type="checkbox"/> <input type="checkbox"/>
No1 #コンソールイメージ		コマンド/確認事項		チェック
<b>7-1-3.DBのバックアップ(3)</b> EP on-premのサービスを再起動する		以下のコマンドを実行してください。		
<pre>[root@localhost tmp]# systemctl start eraserver  [root@localhost tmp]# systemctl status eraserver ● eraserver.service - ESET PROTECT Server    Loaded: loaded (/etc/systemd/system/eraserver.service; enabled; preset: disabled)    Active: active (running) since Tue 2024-06-18 22:04:15 JST; 50s ago  Process: 6749 ExecStart=/opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid  Main PID: 6751 (ERAServer)    Tasks: 50 (limit: 10900)   Memory: 219.3M     CPU: 15.464s    CGroup: /system.slice/eraserver.service            mq6751 /opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid  6月 18 22:04:15 localhost.localdomain systemdStarting ESET PROTECT Server... ~~~~~ 以下 省略 ~~~~~</pre>		【コマンド】 # systemctl start eraserver  【コマンド】 # systemctl status eraserver		<input type="checkbox"/>  <input type="checkbox"/>

No2	#コンソールイメージ	コマンド/確認事項	チェック
7-2.定期バックアップ	定期的にバックアップ取得し、任意の場所に移動する	以下のコマンドを実行してください。	
	不測の事態が発生したときに、Webコンソールを利用できない（ログインできない）可能性や再作成・エクスポートもできない可能性を考慮する必要があります。	【確認】 任意の保存場所にバックアップ、証明書が保管されていること	<input type="checkbox"/>
	6-2-1および6-2-2で取得した証明書と、7-1で取得したデータベースのバックアップは、ESET PROTECT サーバーとは別の安全な保管先に保存してください。また、データベースのバックアップは定期的に取得することを推奨します。		
以上で、手順は終了となります。			