

XDR (eXtended Detection and Response)
ESET Inspect on-prem (V2.1)
導入手順書

第 1.0 版

2024 年 5 月 23 日

キヤノンマーケティングジャパン株式会社

改訂履歴

版数	発行日	改訂履歴
第 1 版	2024 年 5 月 23 日	初版発行

内容

1.はじめに	4
2.システム要件	5
3.導入の流れ	10
4.事前準備【EP on-prem 側作業】	11
5.データベースのインストール【EI on-prem 側作業】	19
6.EI Server のインストール【EI on-prem 側作業】	38
7.EI Connector の展開【EP on-prem 側作業】	47
8.EI Web Console の確認【EI on-prem 側作業】	61
9.EI on-prem 導入時の ESET Endpoint 製品の推奨設定.....	64

1. はじめに

- 本書は、XDR (eXtended Detection and Response)の「ESET Inspect on-prem」をご利用になるお客さま向けの導入手順書となります。
- 本書は、本書作成時のソフトウェア及びハードウェアの以下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搭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。また本書の内容は、将来予告なく変更することがあります。

【サーバー環境】

製品名	バージョン
Microsoft Windows Server	2019
MySQL	8.0.35 以降
Microsoft SQL Server	2017 以降

【ESET 環境】

製品名	バージョン
ESET Inspect on-prem	2.1 以降
ESET PROTECT on-prem	10.1 以降

- 本書内における名称は以下の通りです

略省	正式名称
EI on-prem	ESET Inspect on-prem
EI Connector	ESET Inspect Connector
EP on-prem	ESET PROTECT on-prem
EM Agent	ESET Management Agent
MSSQL	Microsoft SQL Server

- 本手順書の一部またはすべてを無断で複写、複製、改変することはその形態問わず、禁じます。
- ESET Inspect の名称が V2.0 以降より、ESET Inspect on-prem に名称が変更になりました。

※本手順書は EP on-prem V11.0 を使用して作成しています。

2. システム要件

EI on-prem を導入するにあたり、以下の要件をすべて満たしている必要があります。

2.1 EI Server 要件

(1). オンプレミス型セキュリティ管理ツールは V10.1 以降が導入されている必要があります。

(2). 規模別ハードウェア最小要件は以下となります。

【MySQL】

エンドポイント数	500	1000	5000
Memory	4GB	4GB	12GB
Disk Size	566GB	1.1TB	5.6TB
Disk IOPS (*1)	1000	2000	3000
CPU Cores	2	2	8

【MS SQL Sever】

エンドポイント数	500	1000	5000
Memory	4GB	4GB	12GB
Disk Size	566GB	1.24TB	6.2TB
Disk IOPS (*1)	1500	1500	3000
CPU Cores	2	2	10

(* 1) Disk Input Output per Second : 1秒あたりに処理できる「書き込み」と「読み込み」の数

注意事項

(a).この値は最小限要件を満たすための値です。今後これらの値は変わる可能性があります。

(b).ディスクスペースの計算は、データが 1 か月間保存されているという前提に基づいての数値になります。これは、現時点での EI on-prem のデフォルト値となっています。

(3). インストール可能なサポート OS とデータベースは以下となります。

【サポート OS】

サポート OS	アーキテクチャ
Windows Server 2012	x64
Windows Server 2012 R2 (*1)	x64
Windows Server 2016	x64
Windows Server 2019	x64
Windows Server 2022	X64

(*1)2014年4月リリースの更新プログラム KB2919355 の適用が必要

【データベース】

MySQL
MySQL5.7.44 以降、または MySQL8.0.35 以降、MySQL8.1 以降

Microsoft SQL Server
Microsoft SQL Server2017 Microsoft SQL Server2019 Microsoft SQL Server2022 ※ Microsoft SQL Server を使用する場合、次の ODBC ドライバーのいずれかが必要です。 <ul style="list-style-type: none">• ODBC driver11 for SQL Server• ODBC driver13 for SQL Server• ODBC driver17 for SQL Server

2.2 EI Connector 要件

- (1). EI Connector を導入するクライアント端末には、以下のプログラムが導入されている必要があります。

プログラム名	バージョン
ESET Endpoint Security / アンチウイルス	V11.0.2032.1 以降
ESET Endpoint Security for OS X	V6.11.616.0 以降
ESET Server Security for Microsoft Windows Server	V10.0.12014 以降
ESET Server Security for Linux	V10.2.41.0 以降
ESET Endpoint アンチウイルス for Linux	V10.2.2.0 以降

- (2) オンプレミス型セキュリティ管理ツールは V10.1 以降で管理されている必要があります。

- (3) インストール可能なサポート OS は以下となります。

サポート OS	アーキテクチャ
Windows Server 2012	x64
Windows Server 2012 R2	x64
Windows Server 2016	x64
Windows Server 2019	x64
Windows Server 2022	x64
Windows 10 version 21H1 以降	x86/x64
Windows 11 version 21H1 以降	x86/x64
Mac OS 10.15 (Catalina)	x64
Mac OS 11 (Big Sur)	x64
Mac OS 12 (Monterey)	x64
Mac OS 13 (Ventura)	x64
Mac OS 14 (Sonoma)	x64
Red Hat Enterprise Linux 7.6 以降	x64
Red Hat Enterprise Linux 8	x64
Red Hat Enterprise Linux 9	x64
CentOS 7.6 以降	x64
Ubuntu 18.04	x64

Ubuntu 20.04	x64
Ubuntu 22.04	x64
SUSE Linux Enterprise Server 15	x64
Amazon Linux 2	x64
Alma Linux 8	x64
Alma Linux 9	x64
Rocky Linux 8	x64
Rocky Linux 9	X64

2.3 導入前推奨設定

EI on-prem を導入するにあたり、以下の内容を実施することを推奨します。

推奨 1 : EI on-prem のインストール対象のサーバーには固定 IP アドレスを設定することを推奨します。

推奨 2 : Microsoft Windows Server には最新の更新プログラムを適用することを推奨します。

推奨 3 : EI on-prem のインストール対象のサーバーには ESET Server Security for Microsoft Windows Server 又は ESET Management Agent をインストールすることを推奨します。

(インストールされていないと EI on-prem がインストールできない場合がございます)

3. 導入の流れ

ESET Inspect on-prem を導入いただくにあたり、導入作業の流れは以下の通りです。必ず「2.システム条件」をご確認いただき、導入作業の流れ、必要な情報を確認の上、導入作業を進めるようにしてください。

4. 事前準備【EP on-prem 側作業】(P11)

・ **EI on-prem と EP on-prem を連携させるために以下の作業を実施します。**

- 4.1 高度なセキュリティの有効化
- 4.2 証明書の作成
- 4.3 権限設定
- 4.4 ユーザーアカウントの作成

5. データベースのインストール【EI on-prem 側作業】(P19)

・ **MySQL 8 または MSSQL Server 2019 のインストールを実施します。**

- 5.1 MySQL 8.0 のインストール
- 5.2 MSSQL Server 2019 のインストール

6. EI Server のインストール【EI on-prem 側作業】(P38)

・ **EI Server のインストール作業を実施します。**

- 6.1 EI Server のインストール

7. EI Agent のインストール【EP on-prem 側作業】(P47)

・ **EI on-prem ライセンスの登録および、EI Connector のインストール作業を実施します。**

- 7.1 EI on-prem ライセンスの登録
 - 7.2.1 クライアントタスクによる EI Connector のインストール
 - 7.2.2 オールインワンインストーラーによる一括インストール

8. EI Web Console の確認【EI on-prem 側作業】(P61)

・ **EI Web Console へのログイン確認を実施します。**

- 8.1 EI Web Console の確認

9. EI 導入時の ESET Endpoint 製品の推奨設定 (P64)

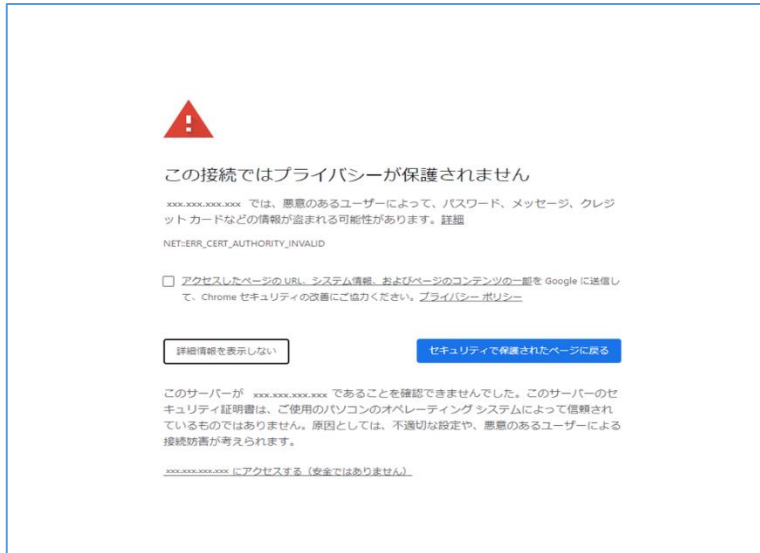
・ **高度なセキュリティを保ちつつ、EI on-prem をより効果的に活用いただくために以下の設定を推奨します。**

- 9.1 推奨設定の実施

4. 事前準備【EP on-prem 側作業】

4-1 高度なセキュリティの有効化

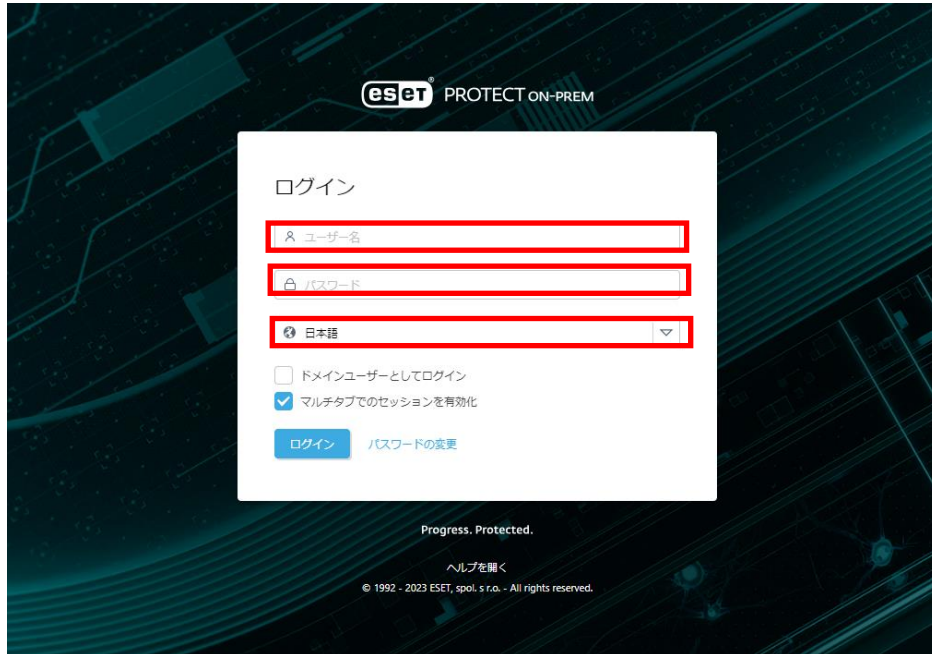
- (1). [https://\(EP on-prem Server を導入したサーバーの IP アドレス\)/era](https://(EP on-prem Server を導入したサーバーの IP アドレス)/era) にアクセスします。以下の画面が表示されますので、「xxx.xxx.xxx.xxx にアクセスする (安全ではありません)」をクリックします。



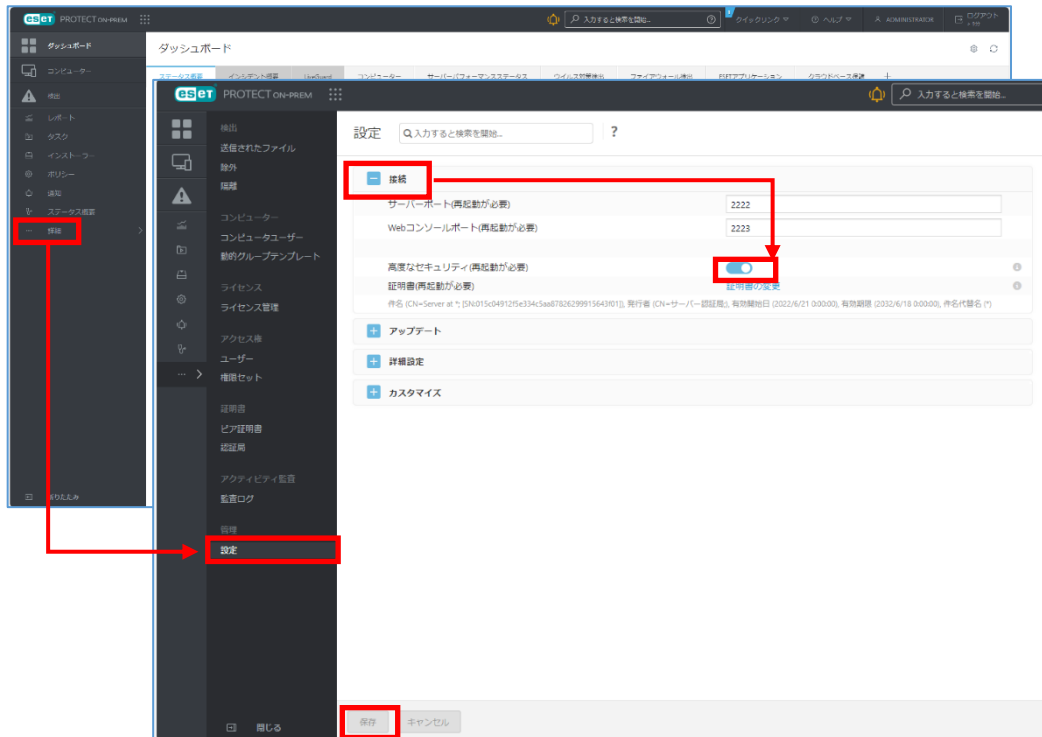
注意

ここでは、ESET PROTECT on-prem のインストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。お使いのブラウザにより、表示内容が異なります。

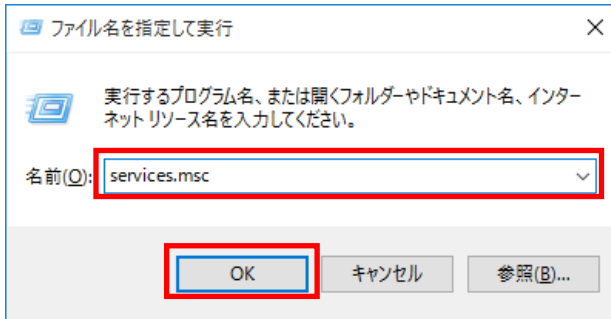
- (2). EP Web Console に管理者権限のあるアカウントでログインします。
 「日本語」 選択して 「EP ログイン名」・「EP ログインパスワード」 を入力し、
 「ログイン」 をクリックします。



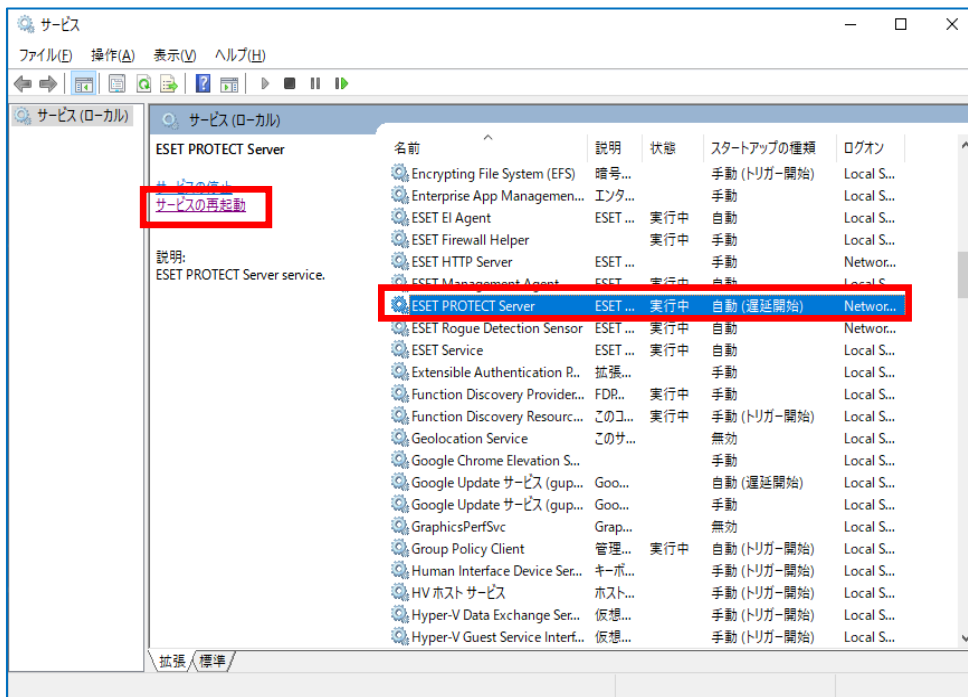
- (3). [詳細]->[設定]->[接続]->[高度なセキュリティ(再起動が必要)]を有効化し、[保存] をクリックします。



- (4). 「Windows キー」 + 「R」 を押下、「ファイル名を指定して実行」ダイアログで、「services.msc」と入力し、「OK」をクリックします。



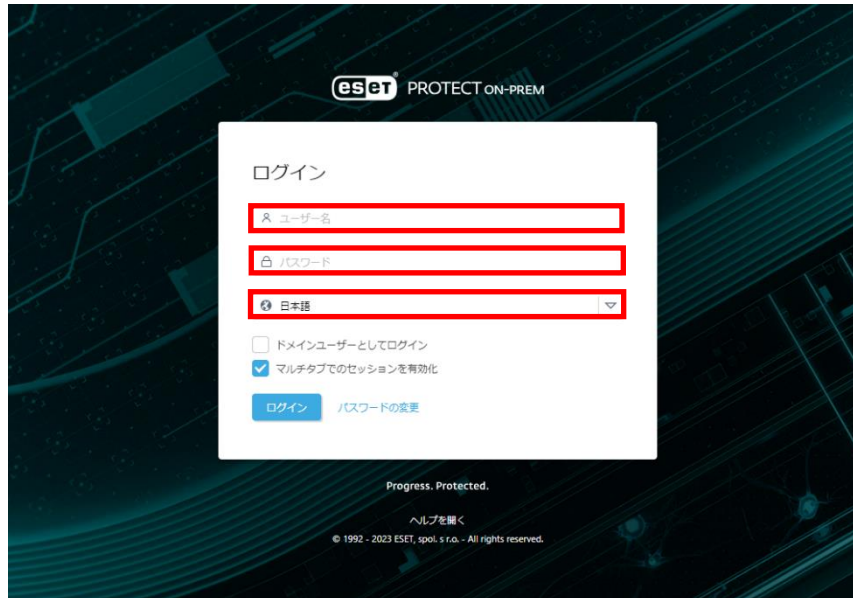
- (5). 「ESET PROTECT Server」を選択し、[サービスの再起動]をクリックします。「ESET PROTECT Server」サービスの状態が、実行中であることを確認します。



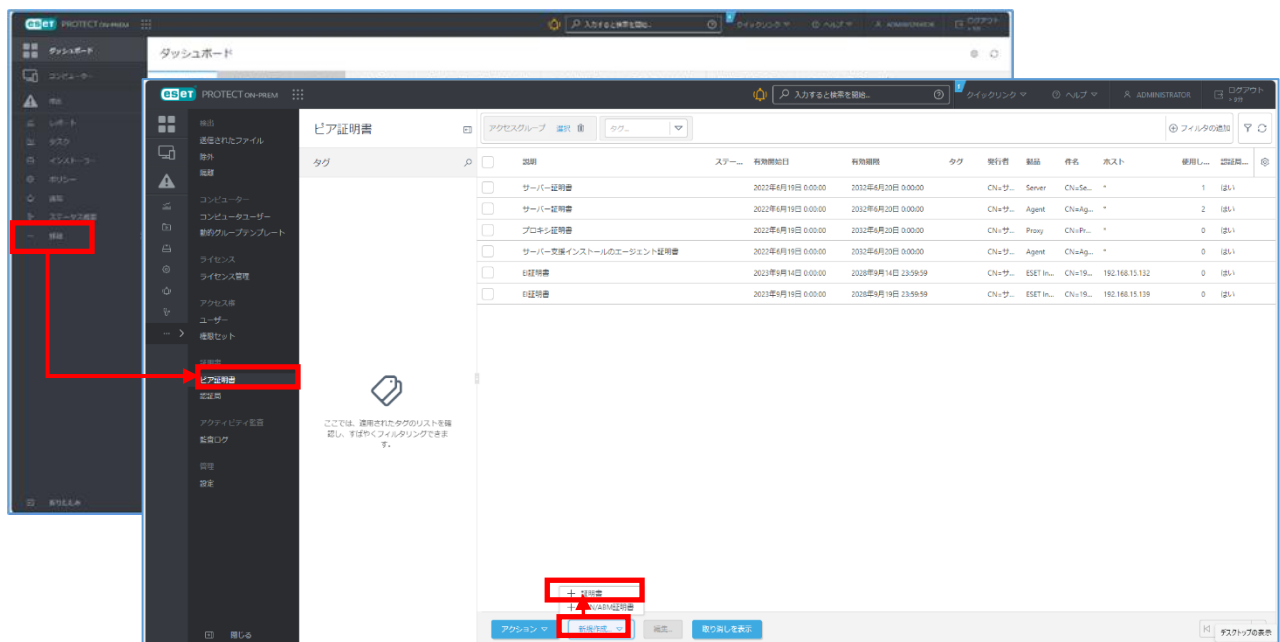
4.2 証明書作成

(1). EP Web Console に再ログインします。

「日本語」を選択して、「EP ログイン名」・「EP ログインパスワード」を入力し、「ログイン」をクリックします。



(2). [詳細]->[ピア証明書]->[新規作成]->[証明書]をクリックします。



(3). 次の通り、各セクションの設定値を入力し、[終了]をクリックします。

■ [基本]セクション

The screenshot shows the '証明書作成' (Certificate Creation) screen in the ESET Inspect on-prem web interface. The '基本' (Basic) section is selected in the left sidebar. The main content area contains the following fields:

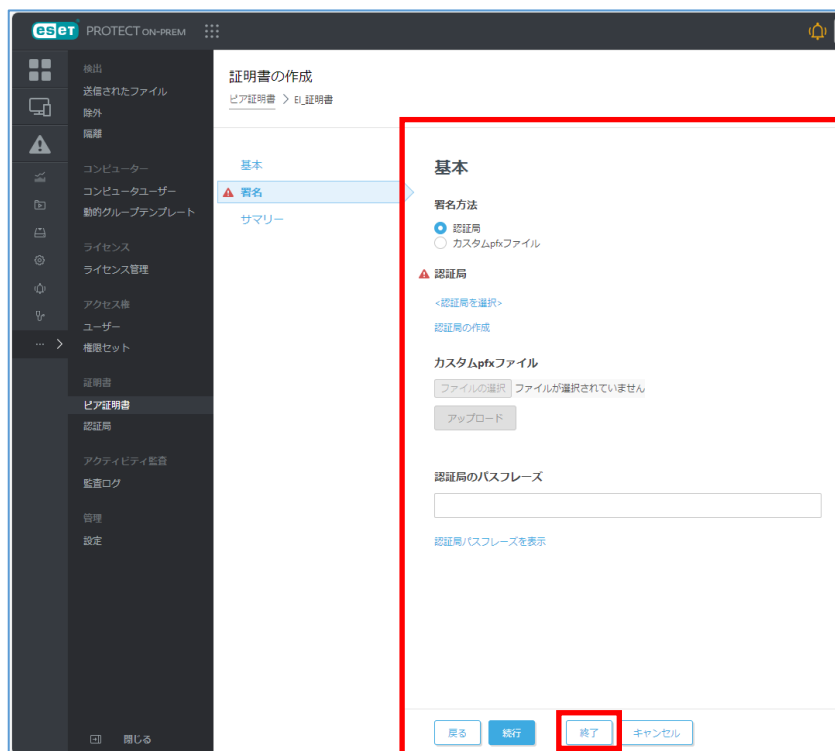
- 説明** (Description): Text input field.
- タグ** (Tag): Text input field.
- 製品** (Product): Dropdown menu with 'ESET INSPECTサーバー' selected.
- ホスト** (Host): Text input field with a red warning icon.
- パスフレーズ** (Passphrase): Text input field.
- パスワードの確認** (Password Confirmation): Text input field.
- 属性(件名)** (Attributes (Subject)): Text input field.

At the bottom of the form, there are four buttons: '戻る' (Back), '実行' (Execute), '終了' (End), and 'キャンセル' (Cancel). The '終了' button is highlighted with a red box.

■ 設定値

説明	既定値のまま、または任意の値を入力してください
製品	ESET Inspect サーバー
ホスト	EI on-prem サーバーの IP アドレス 注：値に「*」を使用することはできません
パスフレーズ	既定値のまま、または任意の値を入力してください
パスワード確認	同上
共通名	EI on-prem サーバーの IP アドレス_Server 証明書
国コード	JP
州または都道府県	既定値のまま、または任意の値を入力してください
組織名	既定値のまま、または任意の値を入力してください
組織単位	既定値のまま、または任意の値を入力してください
有効開始日	既定値のまま、または任意の値を入力してください
有効期限	既定値のまま、または任意の値を入力してください

■ [署名]セクション

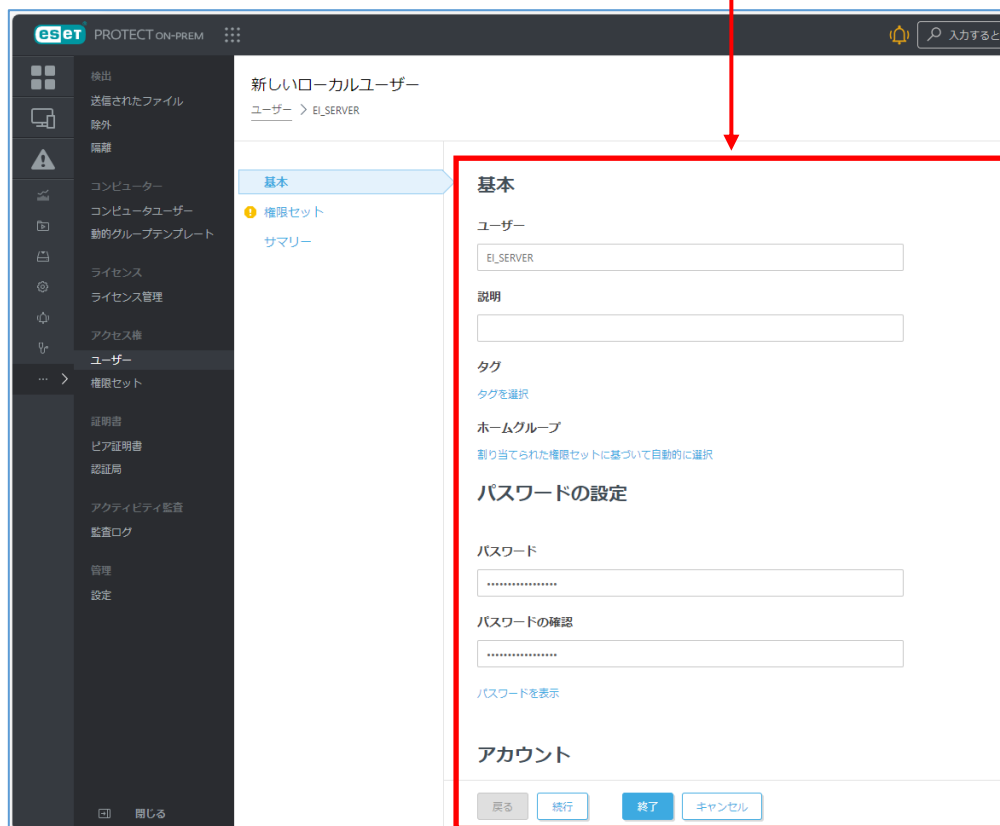
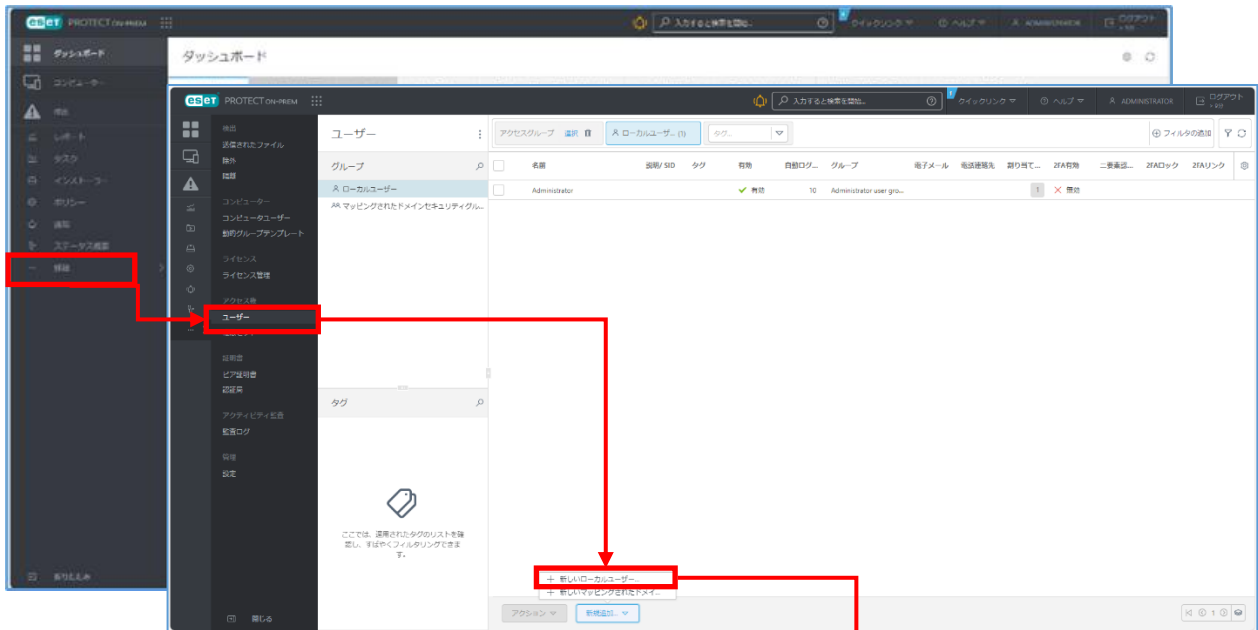


■ 設定値

署名方法	認証局を指定する
<認証局を選択>	既定の認証局を選択する
認証局のパスフレーズ	EP on-prem インストール時に設定したパスフレーズ (既定値は空欄)

4.3 ユーザーアカウント作成

(1). [詳細]->[ユーザー]->[新規追加]-> [新しいローカルユーザー]をクリックします。



(2). [新しいローカルユーザー]画面に、以下の通り入力します。

■ [基本]セクション

ユーザー	例：EI_SERVER
ホームグループ	任意の静的グループを指定
パスワード	8文字以上の任意のパスワード
パスワード確認	再入力
アカウント	有効
パスワード変更が必要	無効
自動ログアウト	既定値または任意の値
氏名	既定値または任意の値
メールアドレス	既定値または任意の値
電話番号	既定値または任意の値

■ [権限]セクション



EP on-prem に用意されている定義済み権限セット「ESET Inspect Server 権限セット」を指定します。

(2). [終了]をクリックします。

5. データベースのインストール【EI on-prem 側作業】

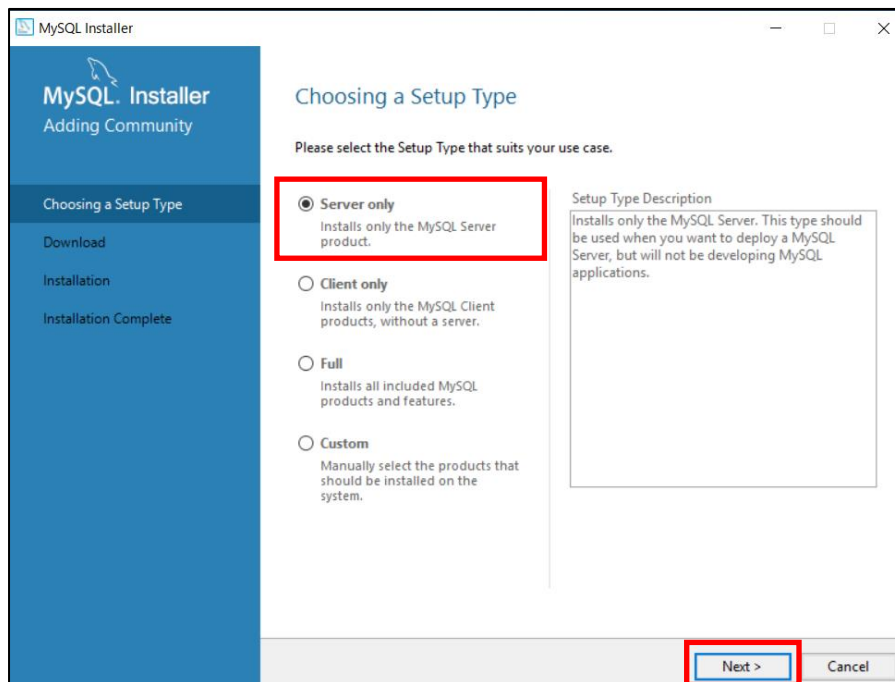
利用可能なデータベースは、MySQL か MSSQL Sever のいずれかとなります。

MySQL を利用する場合は「5.1 MySQL8 のインストール」を、MSSQL Sever を利用する場合は「5.2 MSSQL Server2019 のインストール」を実施してください。

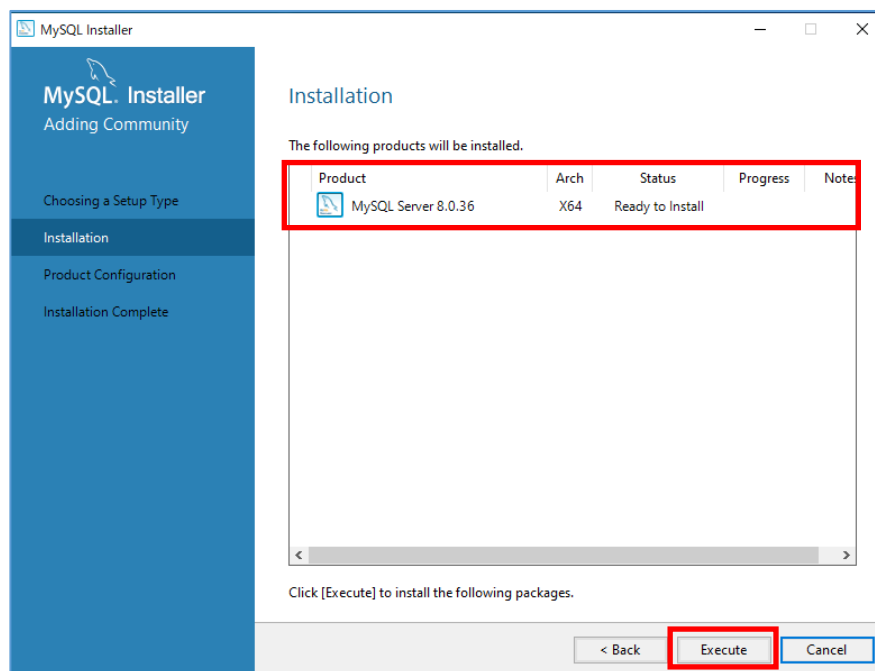
5.1 MySQL8 のインストール

MySQL8 を利用する場合は以下の手順を実施後、「6.EI サーバーのインストール」を行ってください。

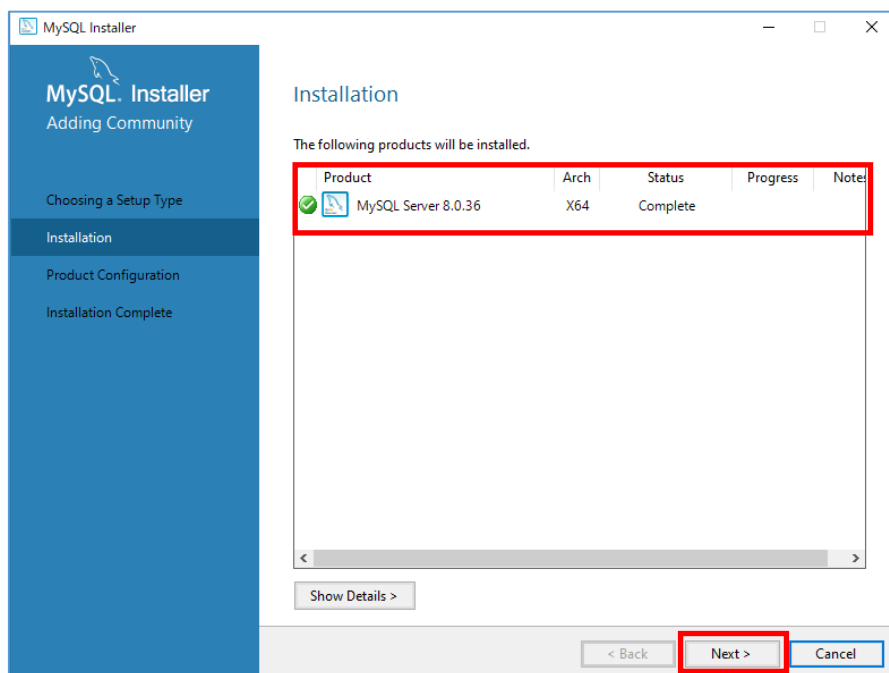
- (1). MySQL を導入するサーバーに「Microsoft Visual C++ 2015 redistributable Package(x64)」がインストールされていない場合は、以下 URL よりダウンロード、およびインストールを完了させます。
<https://learn.microsoft.com/ja-jp/cpp/windows/latest-supported-vc-redist?view=msvc-170>
- (2). 以下 URL より、MySQL のインストーラー(mysql-installer-community-8.0.xx.msi) をダウンロード、およびインストールを開始します。
<https://dev.mysql.com/downloads/windows/installer/8.0.html>
- (3). Choosing a Setup Type 画面で[Server Only]を選択し[Next]をクリックします。



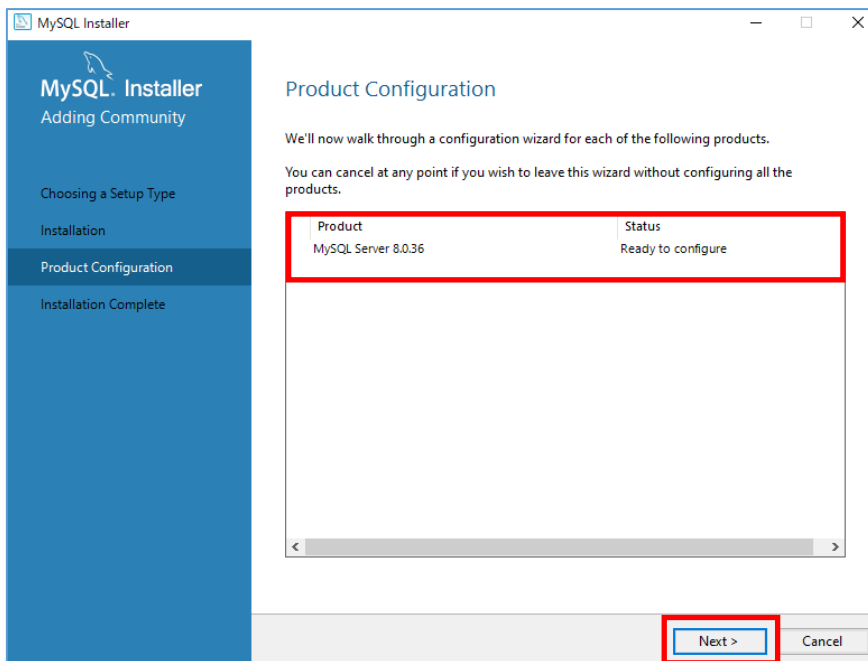
- (4). Installation 画面で[Product]が MySQL Sever 8.0.35 以降であること、Status 欄が「Ready to Install」であることを確認し[Execute]をクリックします。



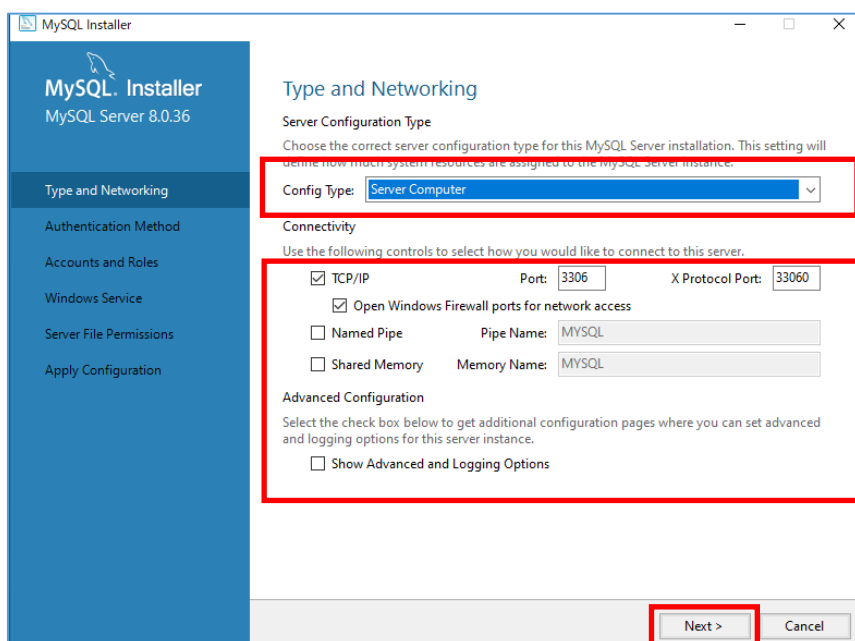
- (5). Installation 画面で[Product]が MySQL Sever 8.0.35 以降であること、Status 欄が「Complete」であることを確認し[Next]をクリックします。



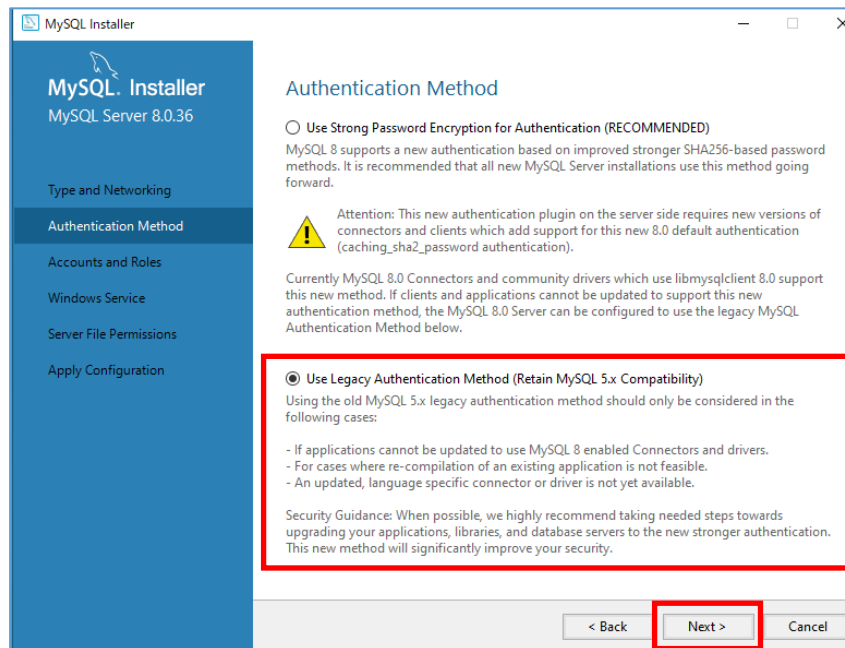
- (6). Product Configuration 画面で Status 欄が「Ready to configure」と表示されたら、[Next]をクリックします。



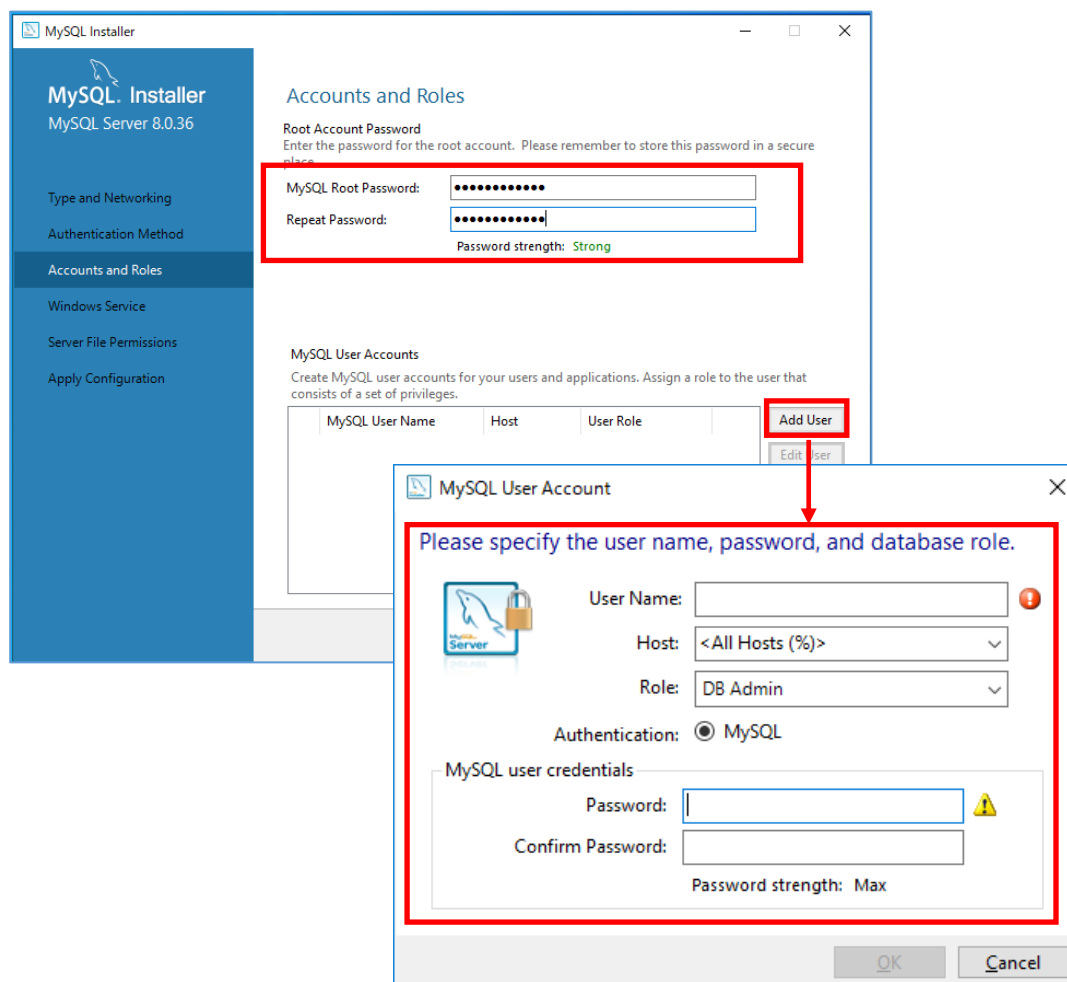
- (7). Type and Networking 画面で Config Type に[Server Computer]を選択します。その他は既定値のまま[Next]をクリックします。



(8). Authentication Method 画面が表示されます。[Use Legacy Authentication Method (Retain MySQL 5.x Compatibility)]を選択し、[Next]をクリックします。



(9). Accounts and Roles 画面で、MySQL が使用する root パスワードを設定し、続いて [Add User] をクリックします。



MySQL User Account ダイアログで、以下の通り入力します。

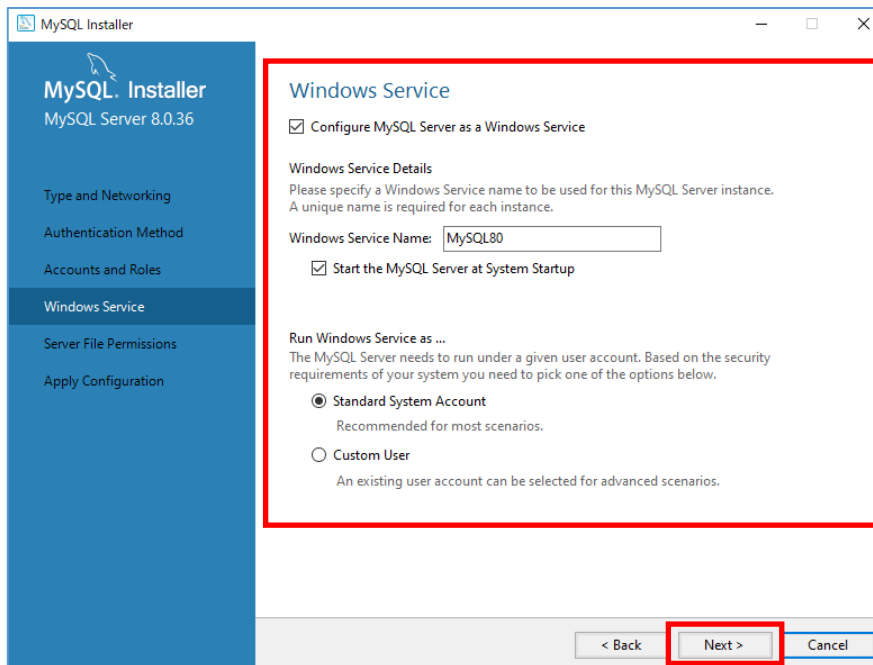
User Name	(任意のユーザー名を入力)
Host	<All Hosts (%)>
Role	DB Admin
Authentication	MySQL
Password	(任意のパスワードを入力)
Confirm Password	(上記と同一のパスワードを入力)

※本項番で入力した MySQL ユーザーアカウントとパスワードをメモしてください。

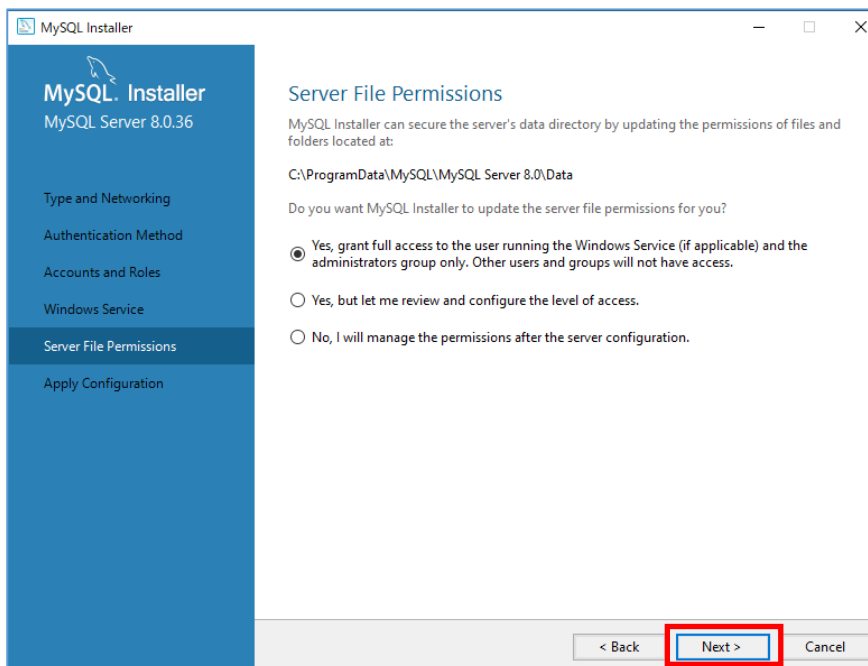
MySQL ユーザーアカウントとパスワードは項番 6-1 (7)で使用します。

(10).Accounts and Roles ダイアログに戻るので、[Next]をクリックします。

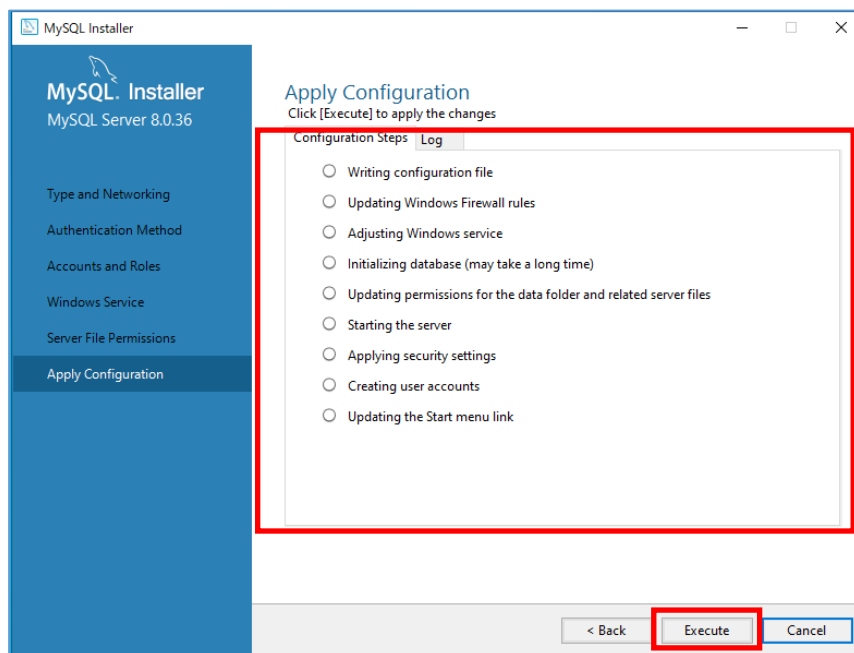
(11).Windows Service 画面は既定値のまま、[Next]をクリックします。



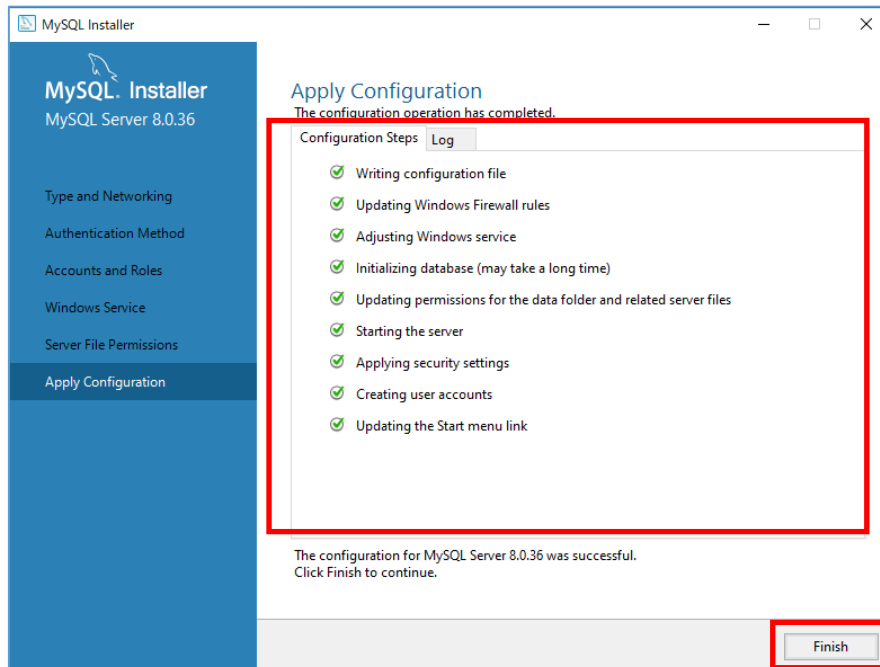
(12).Server File Permissions 画面で[Next]をクリックします。



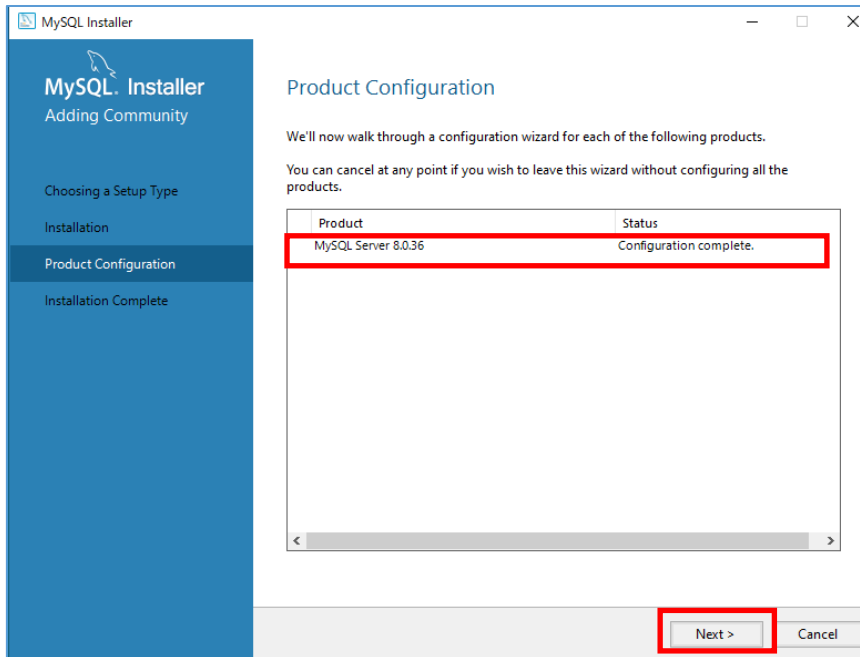
(13).Apply Configuration 画面で[Execute]をクリックします。進捗が表示されるのでしばらく待ちます。



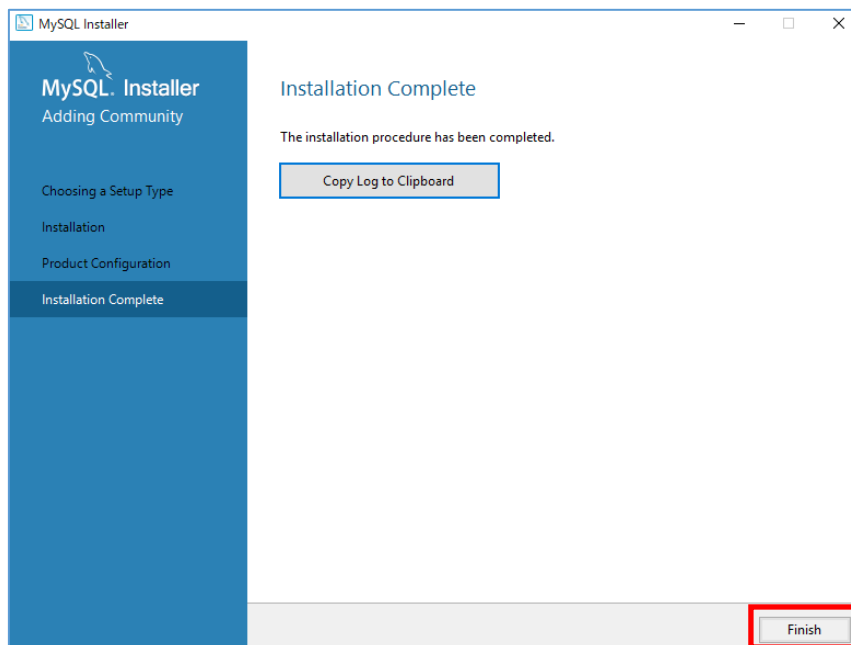
(14).Apply Configuration 画面で、[Finish]をクリックします。



(15).Product Configuration 画面で Configuration complete の表示を確認し、[Next]をクリックします。

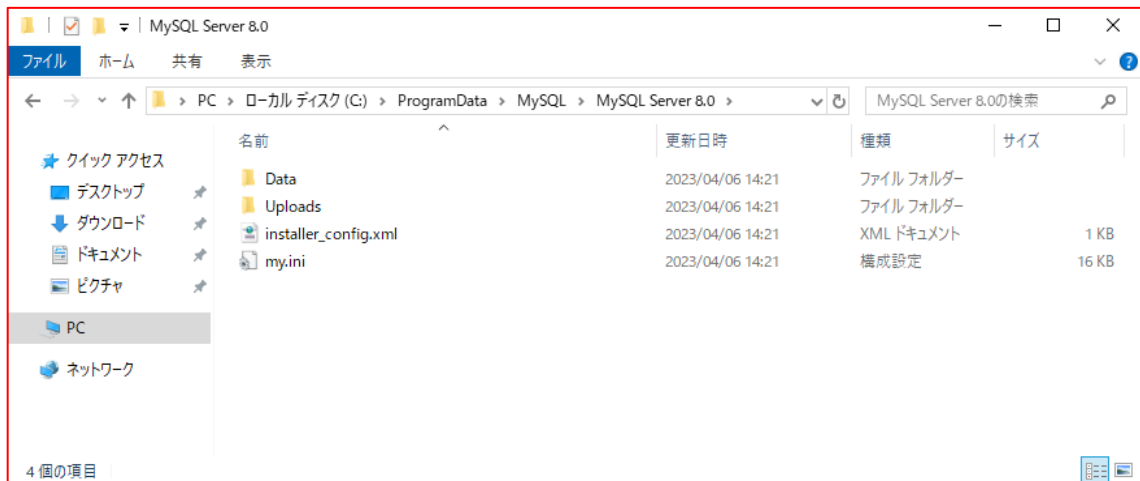


(16).Installation Complete 画面で[Finish]をクリックしインストーラーを終了します。



(17).C:\ProgramData\MySQL\MySQL Server (バージョン番号)\my.ini をテキストエディタで開きます。

※「ProgramData」は隠しフォルダのため、「表示」タブより「隠しファイル」にチェックをして表示させてください。



(18).my.ini ファイル内の以下の設定項目の記述を以下のように変更します。存在しない設定値は追記してください。また、my.ini ファイルを編集する際、使用するテキストエディタは Windows のメモ帳以外のエディタを使用します。

※環境により以下の項目がない場合がありますので、状況に応じて追記してください。

```

1 # Other default tuning values
2 # MySQL Server Instance Configuration File
3 #-----
4 # Generated by the MySQL Server Instance Configuration Wizard
5 #
6 #
7 # Installation Instructions
8 #-----
9 #
10 # On Linux you can copy this file to /etc/my.cnf to set global options,
11 # mysql-data-dir/my.cnf to set server-specific options
12 # (@localstatedir@ for this installation) or to
13 # ~/.my.cnf to set user-specific options.
14 #
15 # On Windows, when MySQL has been installed using MySQL Installer you
16 # should keep this file in the ProgramData directory of your server
17 # (e.g. C:\ProgramData\MySQL\MySQL Server X.Y). To make sure the server
18 # reads the config file, use the startup option "--defaults-file".

```

[my.ini]ファイル

*** INNODB Specific options ***

slow-query-log=0 ※必要に応じて設定変更ください

innodb_buffer_pool_size= (※1)

innodb_flush_log_at_trx_commit=0

innodb_log_file_size= (※2)

open_files_limit=30000

innodb_redo_log_capacity=(※3)

***** Group Replication Related *****

lower_case_table_names=1

max_connections=300

*デフォルトでは以下設定項目の記載が無いため、[mysqld]セクションの最終行に値を追記します。

event_scheduler=ON

log_bin_trust_function_creators=1

thread_stack=256K

local_infile=1

disable-log-bin

wait_timeout=900

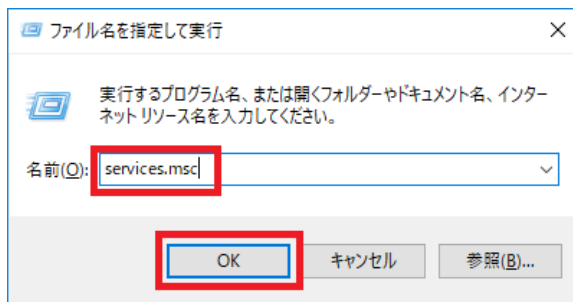
(※1) MySQL をインストールしたサーバーの搭載 RAM の 80%を設定します。例えば 16GB の RAM を搭載するサーバーでは 12G を指定します。最小値は 1G、整数で指定します。

(※2) innodb_buffer_pool_size (※1) に指定した値の 50% (小数点以下切捨て) を指定します。

(※3) innodb_buffer_pool_size (※1) に指定した値を指定します。

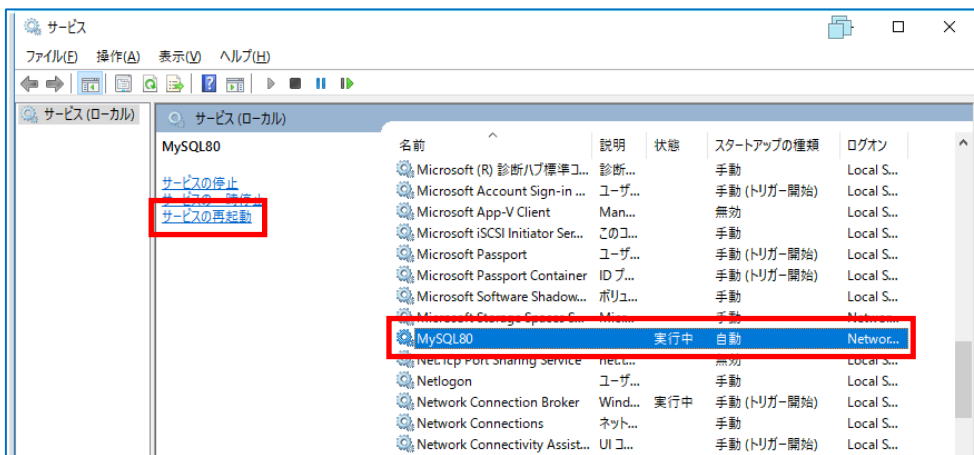
(18). my.ini を保存してテキストエディタを閉じます。

「Windows キー」 + 「R」を押下、「ファイル名を指定して実行」ダイアログで、「services.msc」と入力し、「OK」をクリックします。



(19). MySQL80 を選択し、[サービスの再起動]をクリックします。

MySQL80 サービスの状態が、起動中であることを確認します。



※MySQL サービスが正常に再起動しない場合は、my.ini の記述が正しいか確認してください。

5.2 MSSQL Server2019 のインストール

MSSQL Sever2019 Standard エディション、または Enterprise エディションを利用する場合は以下の手順を実施後、「6.EI サーバーのインストール」を行ってください。

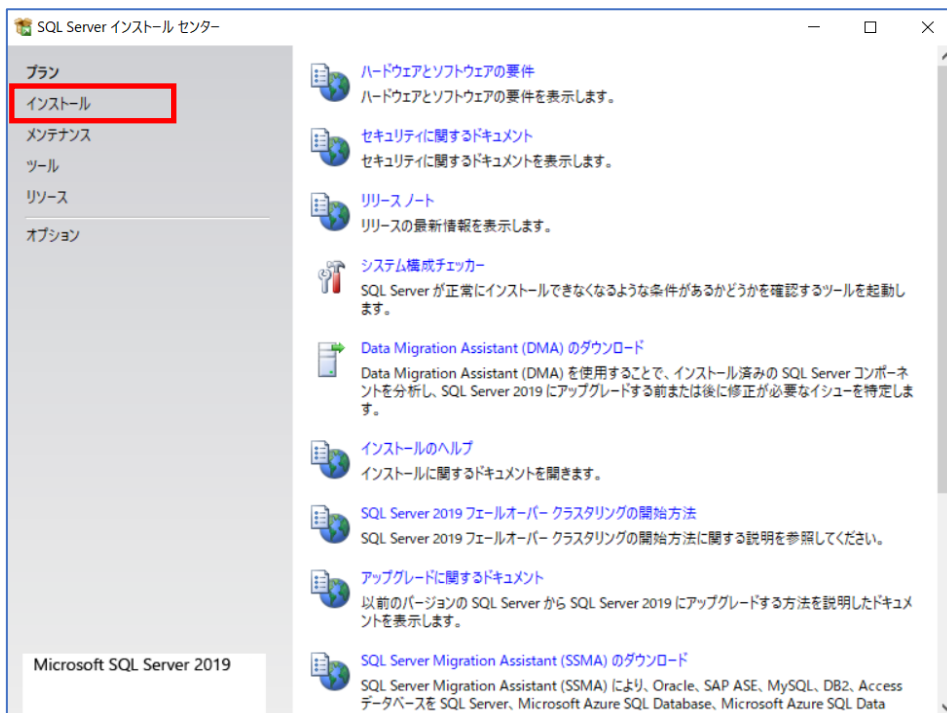
- (1). EI Sever を導入するサーバーに「Microsoft Visual C++ 2015 redistributable Package(x64)」インストールされていない場合は、以下 URL よりダウンロードしインストールします。

<https://learn.microsoft.com/ja-jp/cpp/windows/latest-supported-vc-redist?view=msvc-170>

- (2). 任意の場所に setup.exe を配置し実行します。

- (3). 「インストールの種類を選びます」で「カスタム」を選択しインストールを実行します。

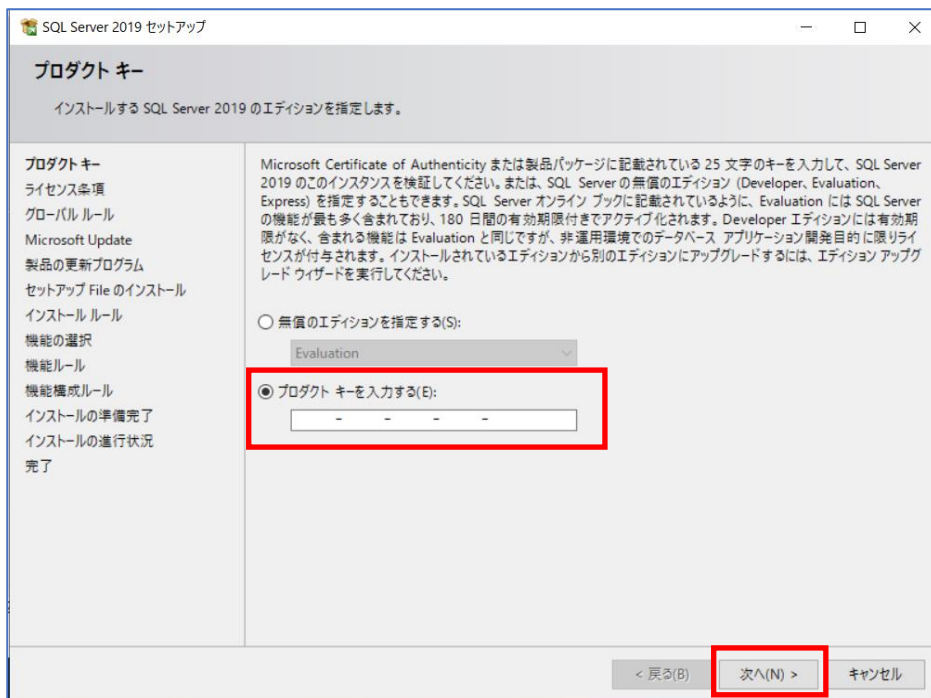
- (4). 「SQL Server インストールセンター」画面が表示されたら、左メニュー「インストール」をクリックします。



- (6). 「SQL Sever の新規スタンドアロンインストールを実行するか、既存のインストールに機能を追加」をクリックします。



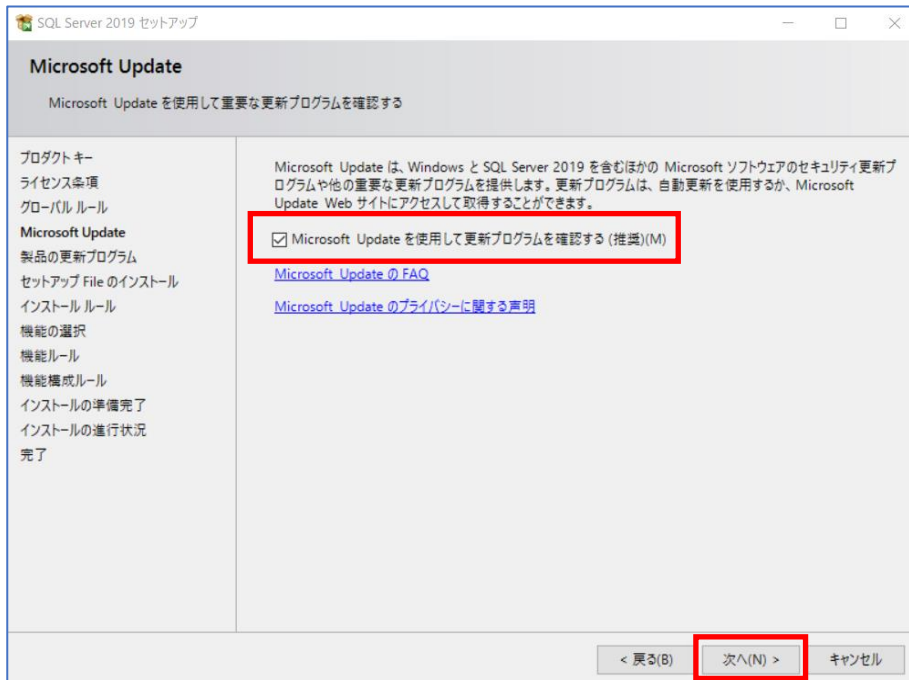
- (7). 「プロダクトキーを入力する (E)」にチェックを入れ、プロダクトキーを入力して「次へ」をクリックします。



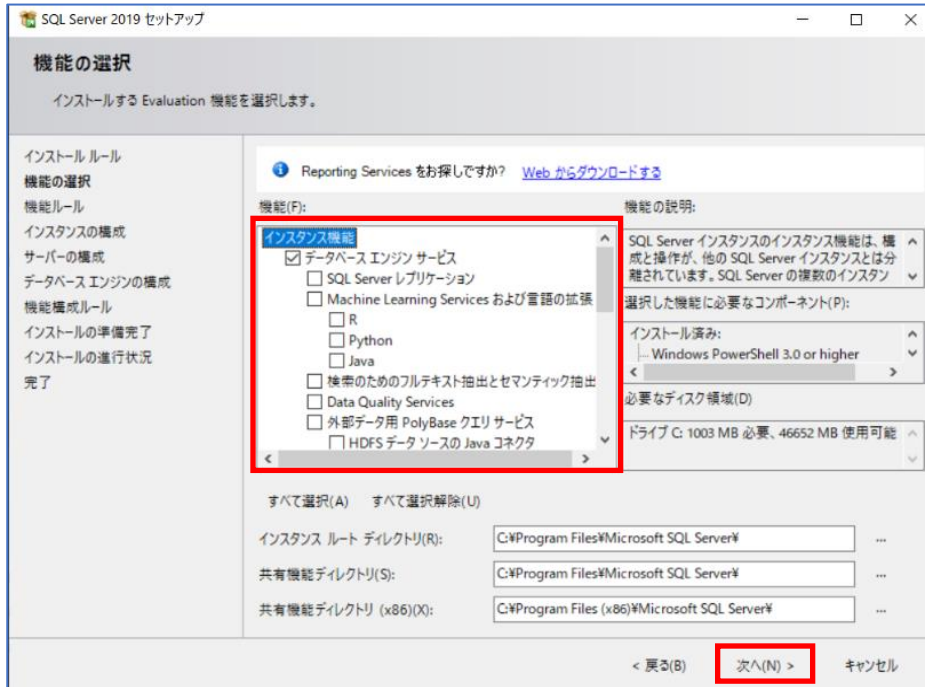
(8). ライセンス条項に同意します」にチェックを入れ、「次へ」をクリックします。



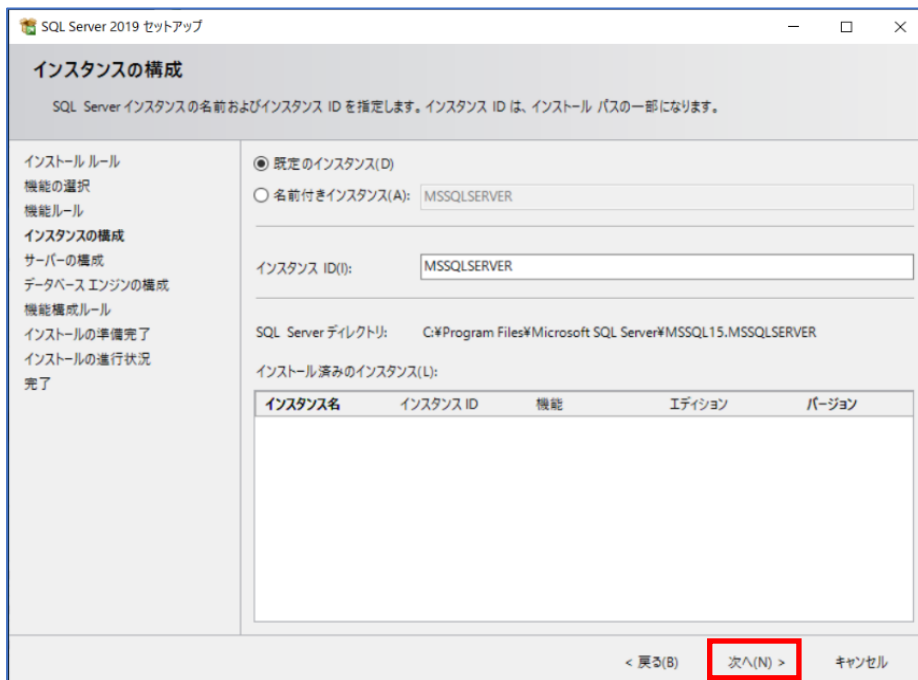
(9). 「Microsoft Update を利用して更新プログラムを確認する」にチェックを入れ、「次へ」をクリックします。



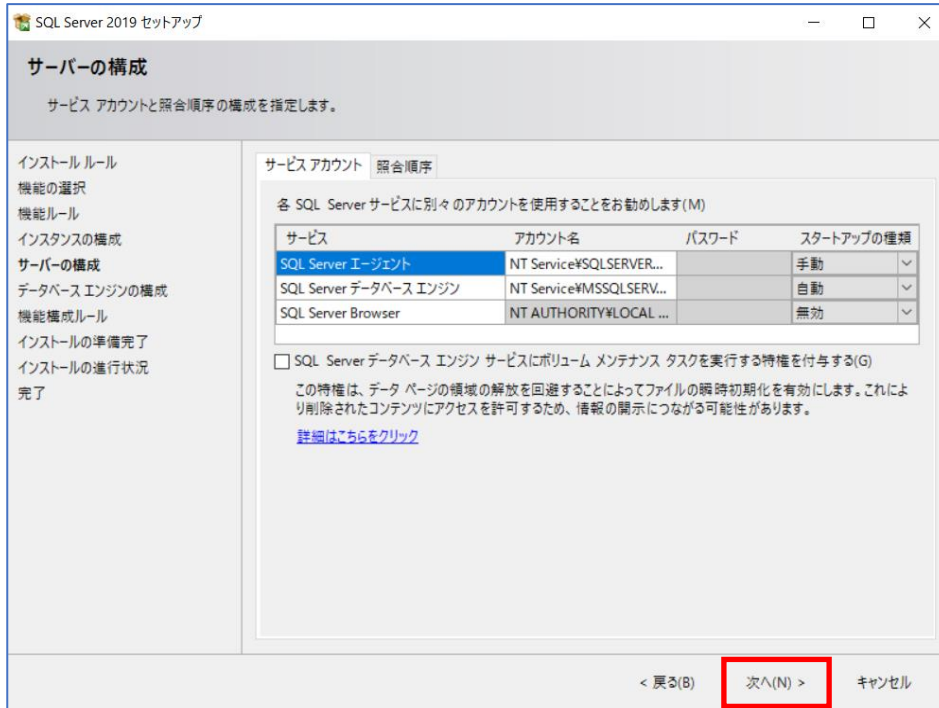
- (10). 「機能選択」画面にて、「データベースエンジンサービス」と「SQL クライアント接続 SDK」にチェックを入れ、「次へ」をクリックします。



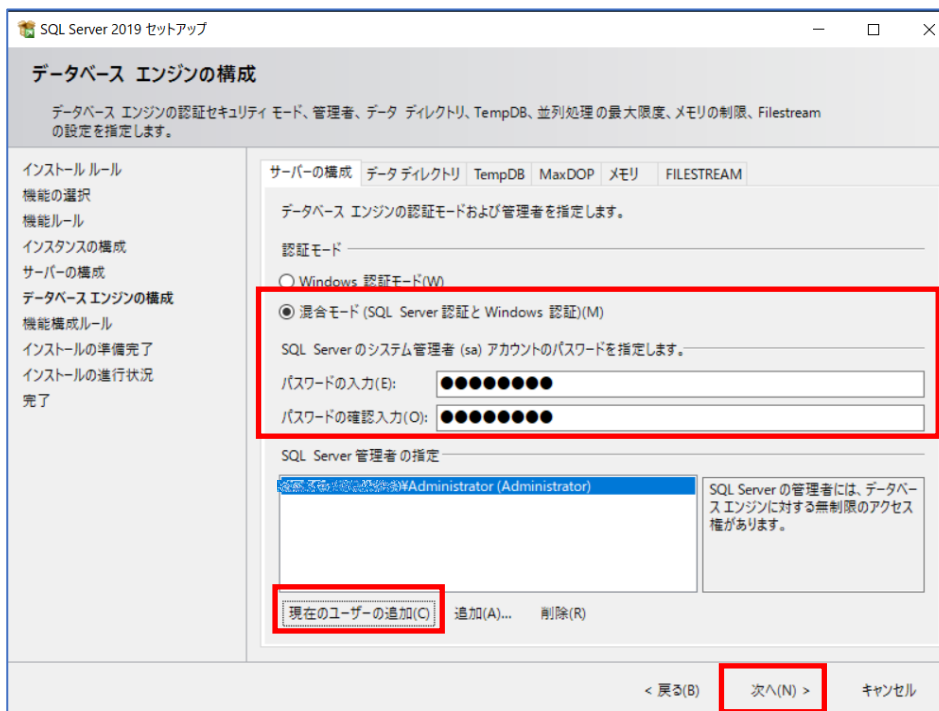
- (11). 「インスタンスの構成」画面にて既定値のまま「次へ」をクリックします。



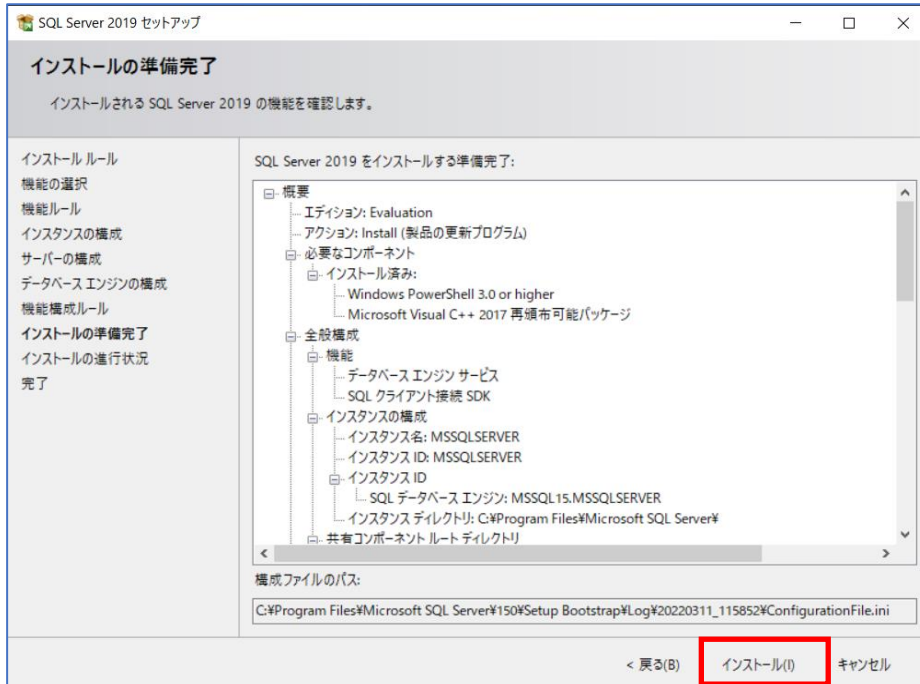
(12). 「サーバーの構成」画面にて既定値のまま「次へ」をクリックします。



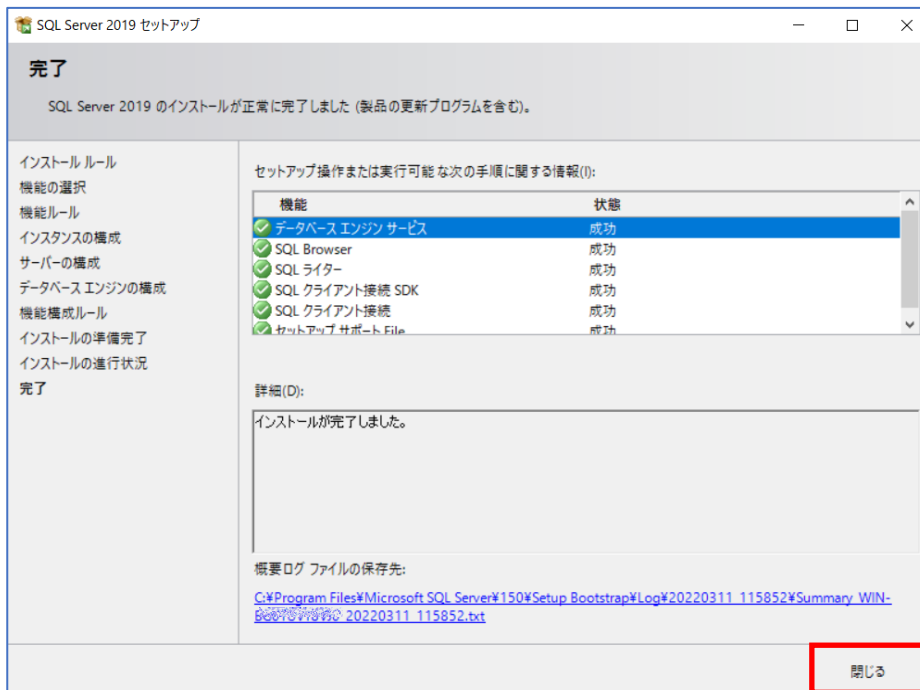
(13). 「データベースエンジンの構成」画面にて、「混合モード」を選択、sa パスワードを設定、「現在のユーザーを追加」をクリックし、「次へ」をクリックします。



(14). 「インストールの準備完了」画面にて、「インストール」をクリックします。

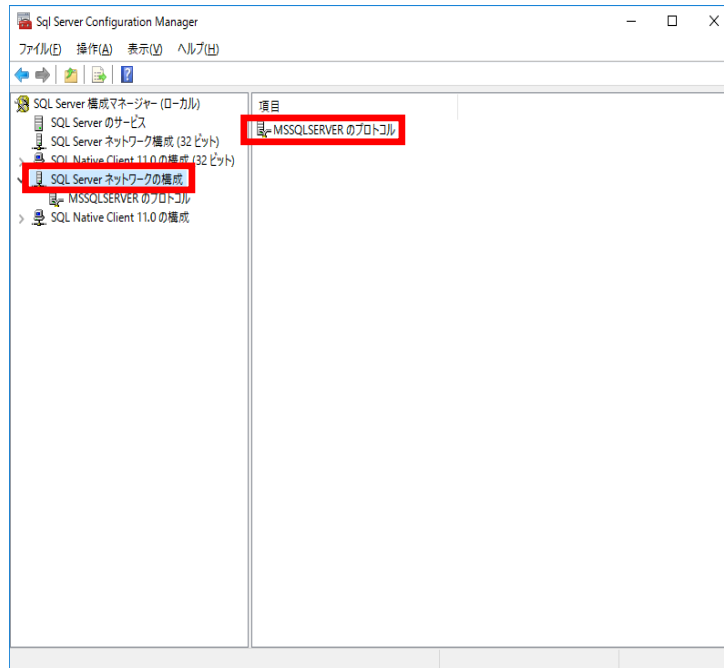


(15). 「完了」画面にて、状態が全て成功であることを確認して「閉じる」をクリックします。

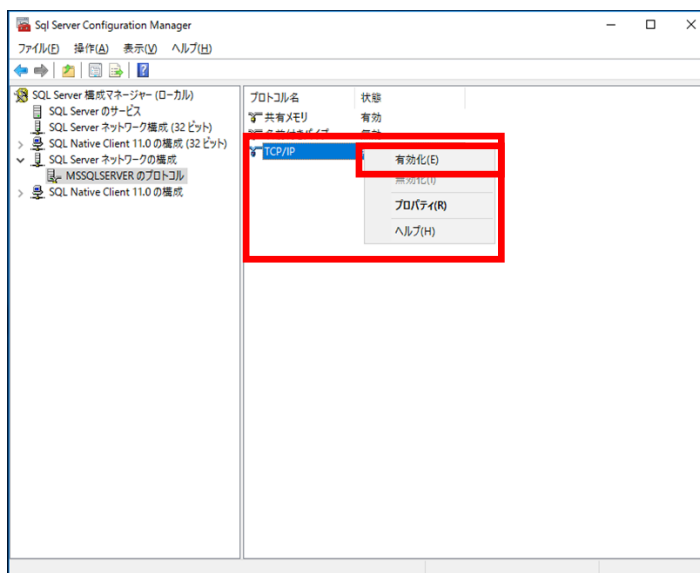


(16). スタートメニューより、「SQL Server 2019 構成マネージャー※」を開きます。
左メニューの「SQL Sever ネットワーク構成」->「MSSQLSERVER のプロトコル」を
クリックします。

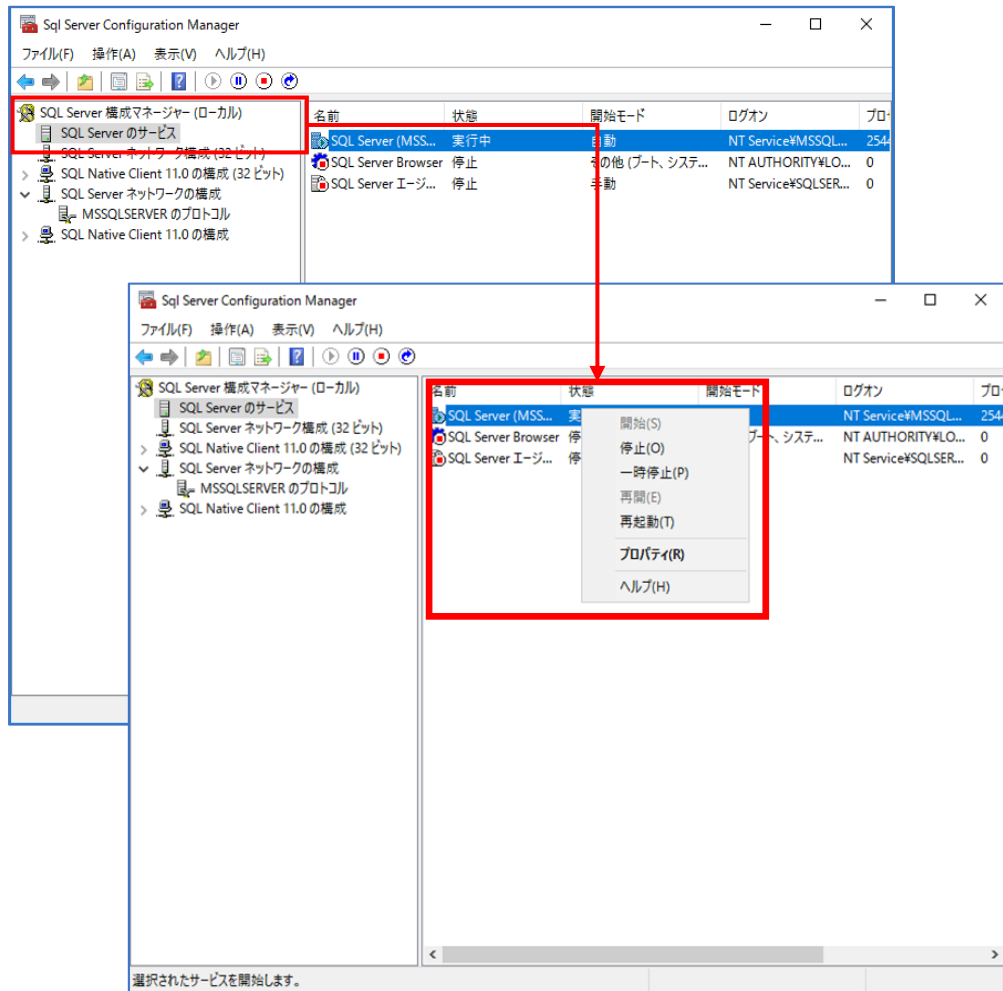
※アプリケーション名はインストールしたデータベースの情報に読み替えてください。



(17). 右メニューの「TCP/IP」を右クリックし、コンテキストメニューより「有効化」を
選択します。



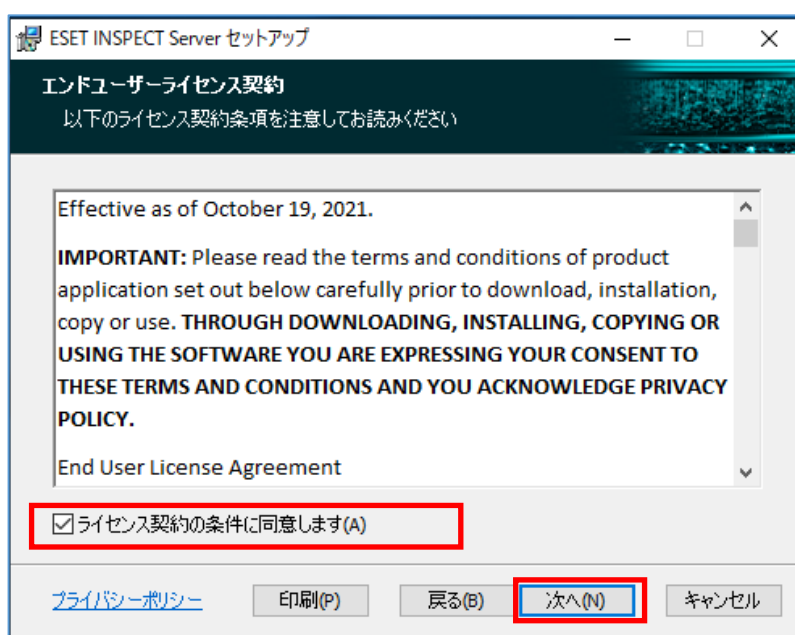
- (18). 左メニューの「SQL Server のサービス」をクリックし、右メニューの「SQL Server (MSSQLSERVER)」を右クリックし、「再起動」を実行します。



6. EI Server のインストール【EI on-prem 側作業】

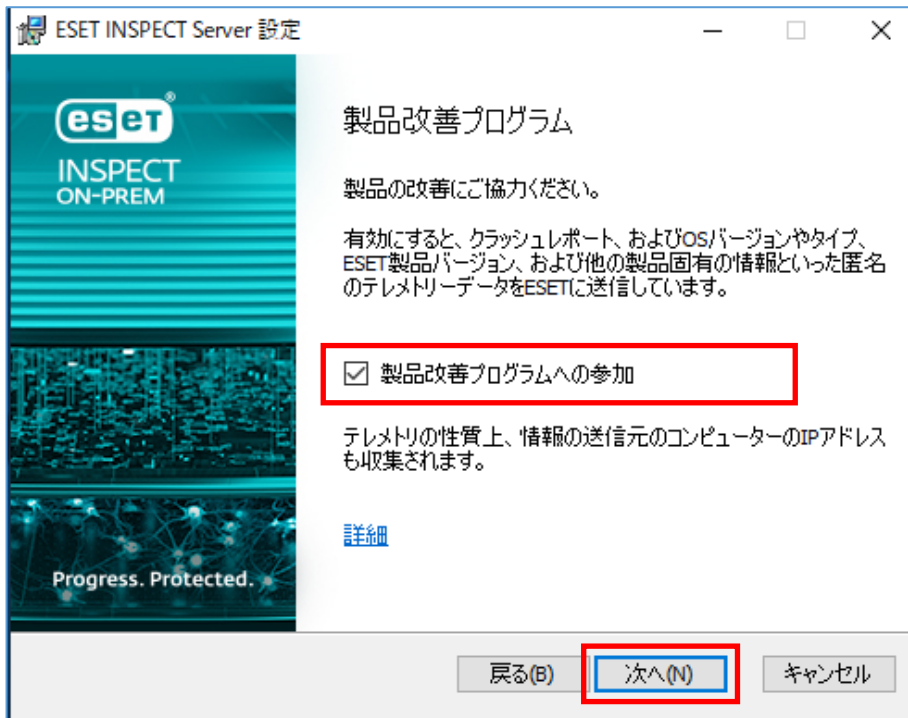
6.1 EI Server のインストール

- (1). EI Server の導入対象が Windows Server 2012 R2 の場合は、「April 2014 update rollup(KB2919355)」をインストールします。
- (2). EI Server のインストーラー(ei_server_nt64.msi)を使用し、インストールを開始します。
- (3). [次へ]をクリックしてインストールウィザードを進めます。エンドユーザーライセンス契約画面では、[ライセンス契約の条件に同意します (A)]にチェックを入れます。

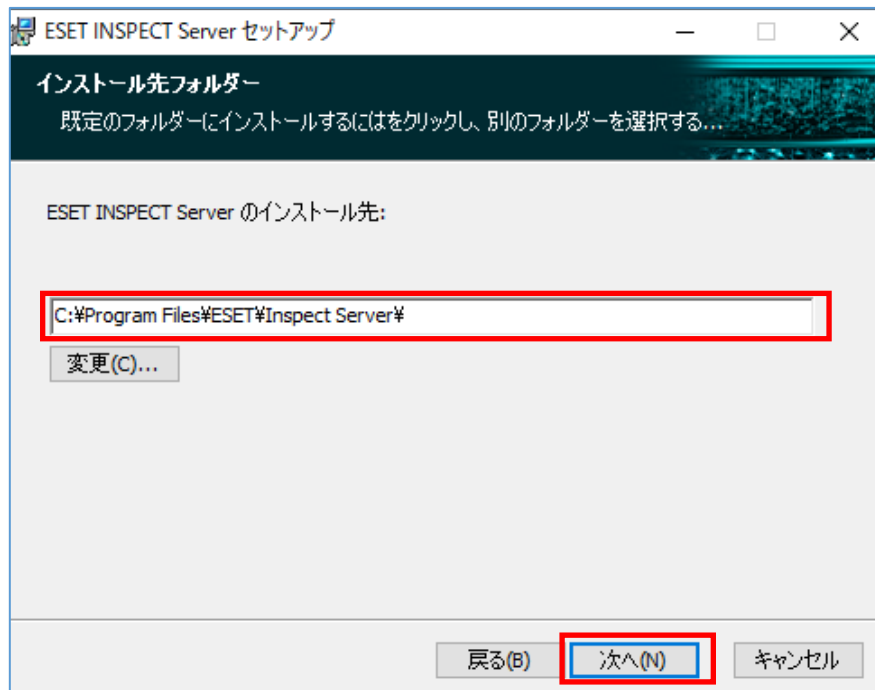


(4). 製品改善プログラム画面の[製品改善プログラムへの参加]のチェックは任意です。

※ EI on-prem の機能は、本項目にチェックを入れなくても利用できます。



(5). インストール先フォルダー画面で、任意のインストールフォルダを指定します。



(6). サーバー接続画面で、Web Console および Agent の接続ポート情報を入力します。

ESET INSPECT Server 設定

サーバー接続
Webコンソールとサーバーのポートを入力してください

WebコンソールHTTPSポート: 443
WebコンソールHTTPポート: 80
コネクターポート: 8093
公開ホスト名:

戻る(B) 次へ(N) キャンセル

(7). データベース接続画面で、データベースの接続情報を入力します。

- ① 以下は MySQL を利用した場合の設定値となります。データベースアカウントのユーザー名は項番 5-1(9)で作成したユーザー情報を入力します。

ESET INSPECT Server 設定

データベース接続
データベース設定を入力します

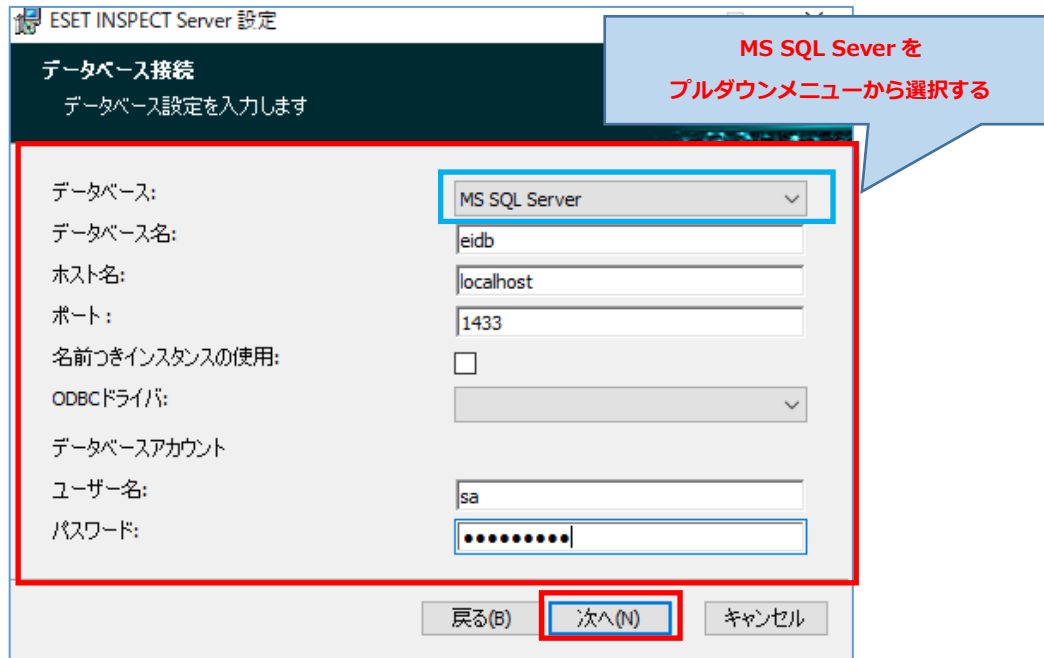
データベース: MySQL Server
データベース名: eidb
ホスト名: localhost
ポート: 3306

データベースアカウント
ユーザー名:
パスワード:

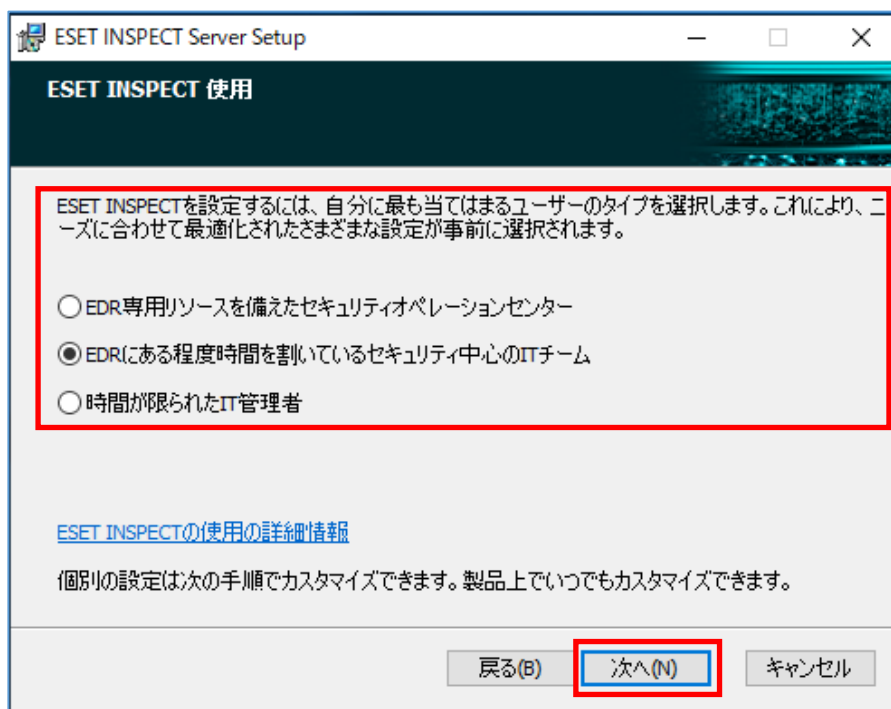
戻る(B) 次へ(N) キャンセル

MySQL Sever をプルダウンメニューから選択する

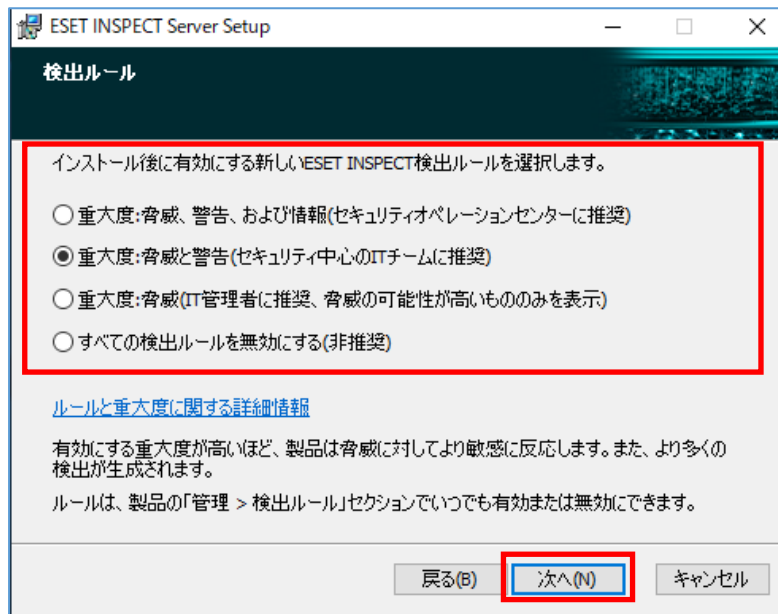
- ② 以下は MSSQL を利用した場合の設定値となります。データベースアカウントのユーザー名は項番 5-2(13)で作成したユーザー情報を入力します。



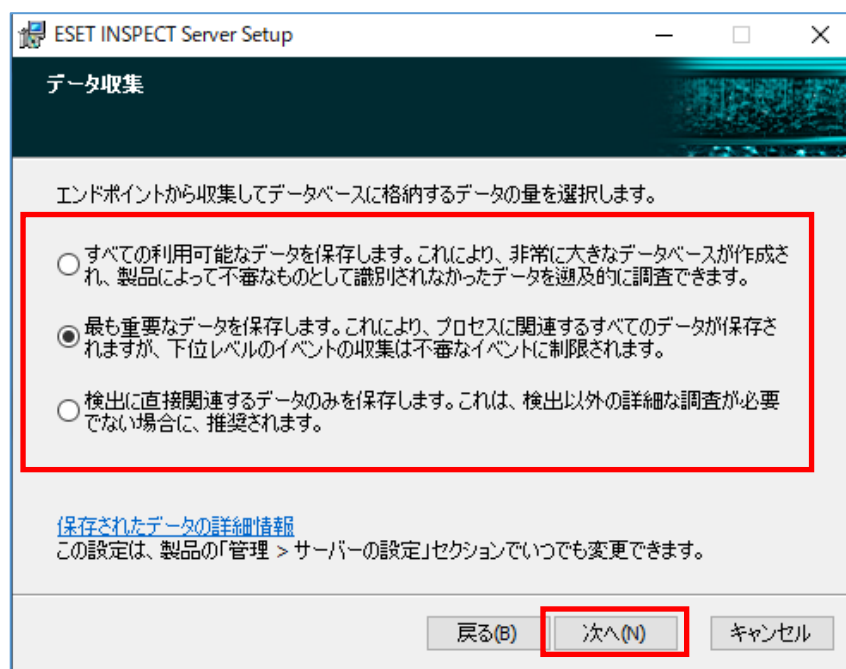
- (8). ESET Inspect 使用画面で、プロファイルベースの設定を行います。
本手順で選択した項目により、後続のデフォルトの選択値が変わります。



- (9). 検出ルール画面で、4つの重大度レベルに基づいて有効にするルールを選択します。本手順で選択した内容により、EI インストール後に既定で有効になるルールが変わります。



- (10). データ収集画面では、EI でのデータ収集オプションを設定します。本手順で選択した内容により、データがデータベースに保存される方法を設定します。EI on-prem で表示されるプロセスツリーの情報量に影響します。



- (11). データ保持画面では、EI on-prem でのデータの保持期間を選択します。
本手順では、検出データや下位レベルデータの保持期間を設定します。
※本設定は EI インストール後にも設定変更が可能です。

ESET INSPECT Server Setup

データ保持

データベースでデータを保存する期間を選択します。期間が長いほど、古いデータがパージされるまでのデータベースは大きくなります。

次の検出を保存します: 3ヶ月

次の下位レベルデータを保存します: 1週間

下位レベルのデータはデータベースサイズの大部分を占めるため、保存期間をできるだけ短くする必要があります。削除すると、製品によって不審なものとして識別されなかったデータの詳細な調査のみが制限されます。

[保存されたデータの詳細情報](#)

この設定は、製品の「管理 > サーバーの設定」セクションでいつでも変更できます。

戻る(B) 次へ(N) キャンセル

- (12). ESET Protect 設定画面で、EP on-prem の接続情報を入力します。

ESET INSPECT Server 設定

ESET PROTECT設定

ESET PROTECTとの接続に使用する設定を入力します

ESET PROTECTへのデータ接続

ESET PROTECTホストアドレス

ESET PROTECTデータ接続用ポート: 2223

ESET PROTECTユーザー: Administrator

ESET PROTECT/パスワード:

ESET PROTECTWebコンソールへの接続

使用したプロトコル: HTTP HTTPS

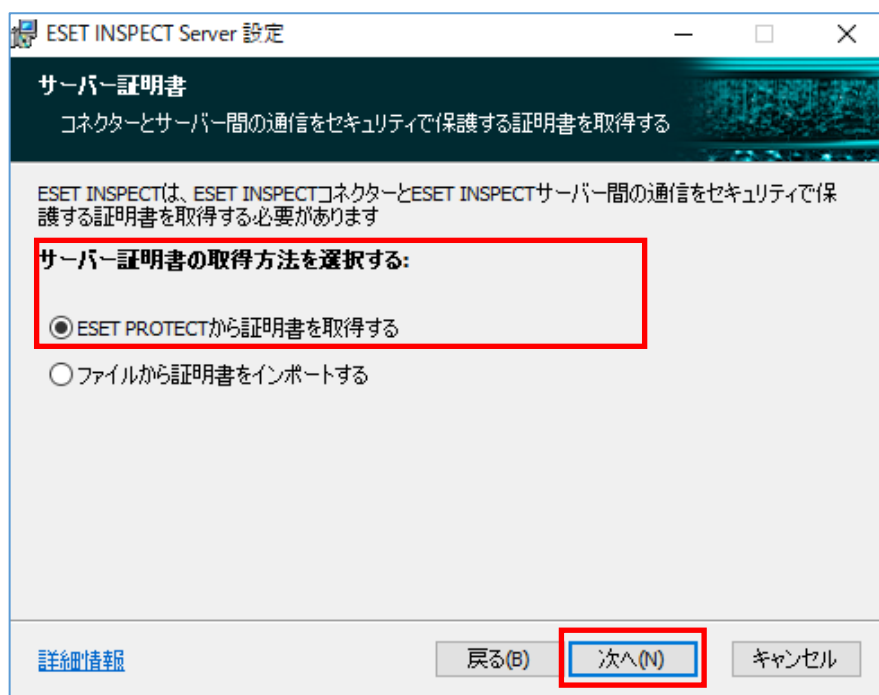
ESET PROTECTWebコンソールポート: 443

戻る(B) 次へ(N) キャンセル

(13). 接続先 ESET PROTECT ダイアログが表示されますので、[はい] を選択します。



(14). サーバー証明書画面で、EI Server と EI Connector 間の接続に使用する証明書の取得方法を選択します。ここでは既定の [ESET Protect から証明書を取得する] を選択し、[次へ]をクリックします。



- (15). サーバー証明書画面で、事前準備で作成した証明書(項番 4 4.2 で作成)を選択します。証明書パスワードは証明書作成時に設定したパスワードを入力します。
(空にした場合、入力不要)

ESET INSPECT Server 設定

サーバー証明書
コネクタとサーバー間の通信をセキュリティで保護する証明書を取得する

ESET INSPECTサーバー証明書を選択する 新しい証明書の作成

CN=xxx.xxx.xxx.xxx_Server証明書;C=JP;

証明書パスワード

詳細情報 戻る(B) 次へ(N) キャンセル

- (16). Web コンソール証明書画面で、EI Web Console で使用する証明書を選択します。ここでは既定の「コネクタ/サーバー通信と同じ証明書を使用する」を選択し、[次へ]をクリックします。

ESET INSPECT Server 設定

Webコンソール証明書
WebコンソールのHTTPS/SSLを有効にする証明書を取得する

ESET INSPECTは、ESET INSPECT WebコンソールとWebブラウザ間のHTTPS/SSL接続を有効にする証明書が必要です

HTTPS/SSL証明書の取得方法を選択する:

ESET PROTECTから証明書を取得する

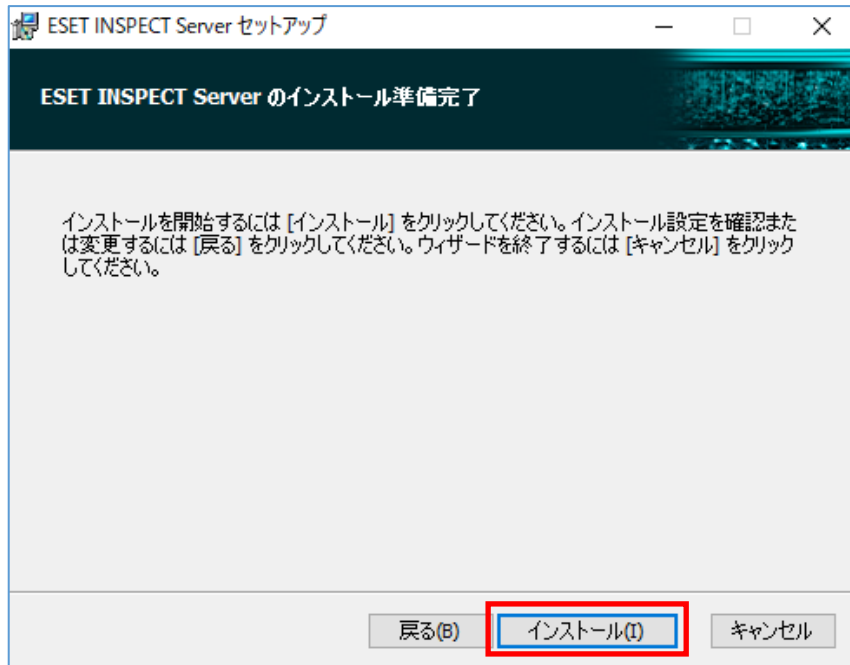
ファイルから証明書をインポートする

コネクタ/サーバー通信と同じ証明書を使用する

追加のHTTPS/SSL証明書要件:
- SHA-2アルゴリズムを使用してこの証明書に署名する必要があります(「ESET PROTECT > サーバー設定 > 接続」の「高度なセキュリティ」を有効にします) - 証明書の署名に使用される認証局がWebブラウザのHTTPS/SSL証明書リストに存在している必要があります。これらの要件が満たされていない場合、ESET INSPECT Webコンソールに接続すると、Webブラウザに警告が表示されます。

詳細情報 戻る(B) 次へ(N) キャンセル

- (17). ESET Inspect Server のインストール準備完了画面で [インストール] をクリックします。



- (18). インストール完了後に [完了] をクリックします。



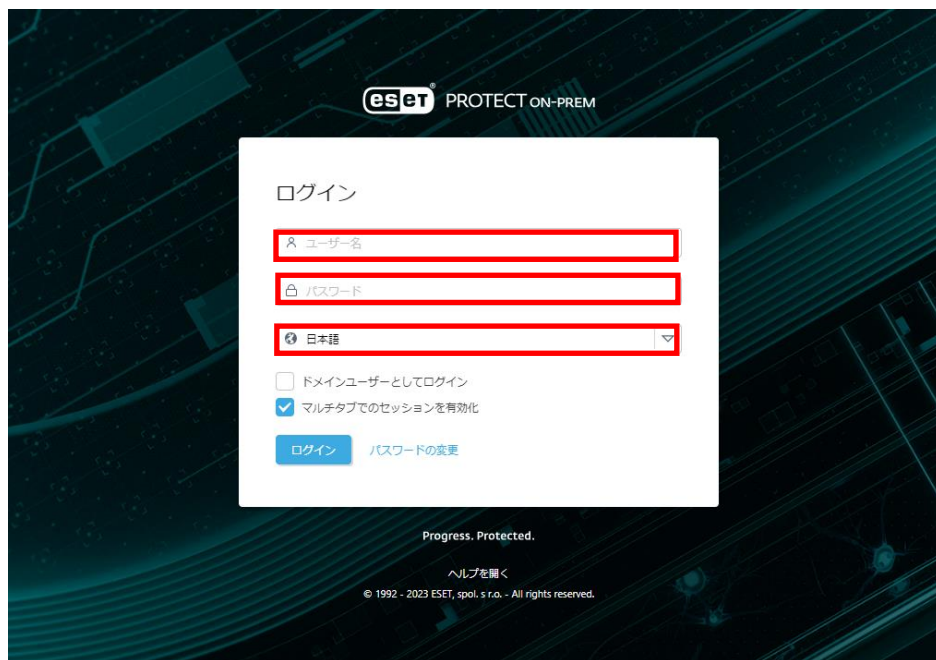
7. EI Connector の展開【EP on-prem 側作業】

7.1 EI on-prem ライセンスの登録

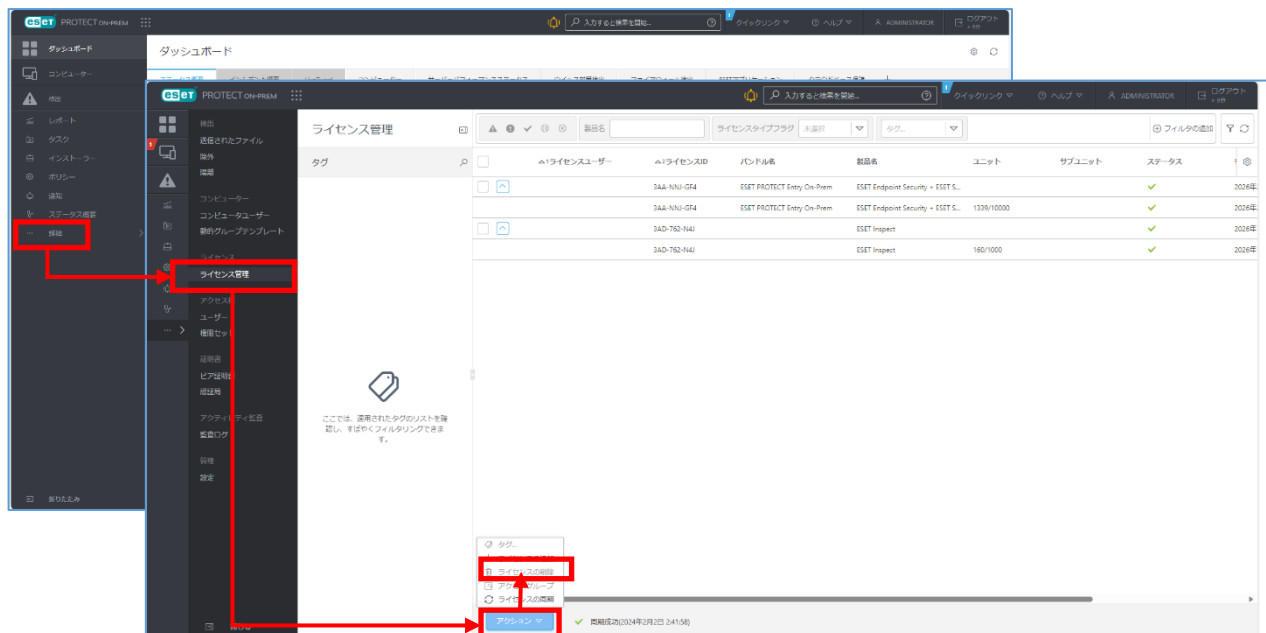
※本手順は既に EI on-prem が利用可能なライセンスを EP on-prem に登録している場合は実施不要です。

(1). EP Web Console に管理者権限のあるアカウントでログインします。

「日本語」を選択して、「EP ログイン名」・「EP ログインパスワード」を入力し、「ログイン」をクリックします。



(2). [詳細]->[ライセンス管理]->[アクション]->[ライセンスの追加]をクリックします。



- (3). ライセンス追加画面で[製品認証キー]を選択し、EI on-prem 用の製品認証キーを入力します。[ライセンスの追加]をクリックします。

ライセンスの追加

次のオプションのいずれかを使用して、ライセンスを追加できます。

- ESET Business AccountまたはESET MSP管理者
- 製品認証キー
- オフラインライセンスファイル

製品認証キー

XXXX-XXXX-XXXX-XXXX

ユーザー名とパスワードがある場合の手順

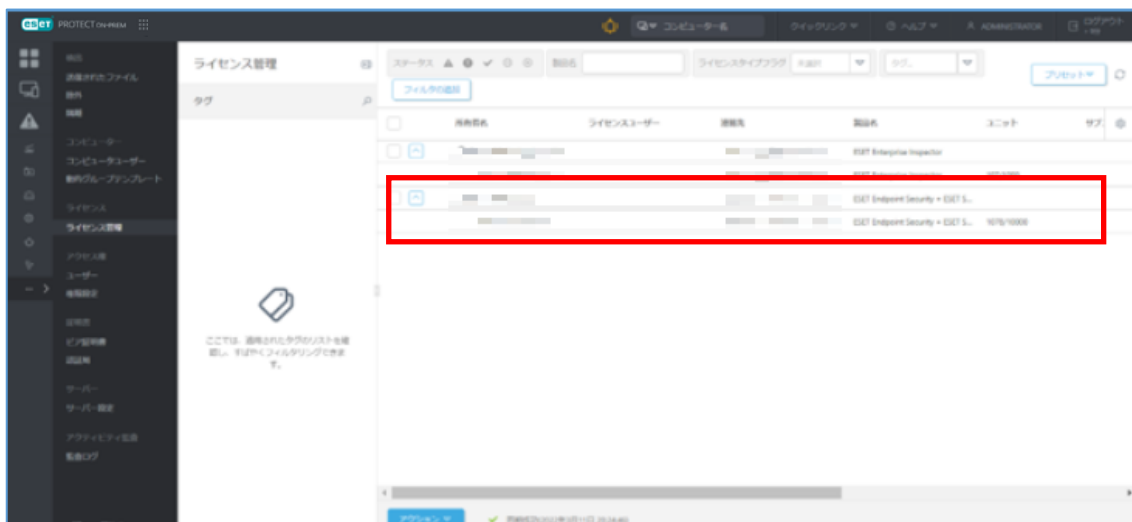
ライセンスの追加 キャンセル

- (4). ライセンスが追加された旨のダイアログが出ますので、[OK]をクリックします。

XXXX-XXXX-XXXX-XXXX によってライセンスが追加されました。
リストの更新は少し遅れる場合があります。

OK

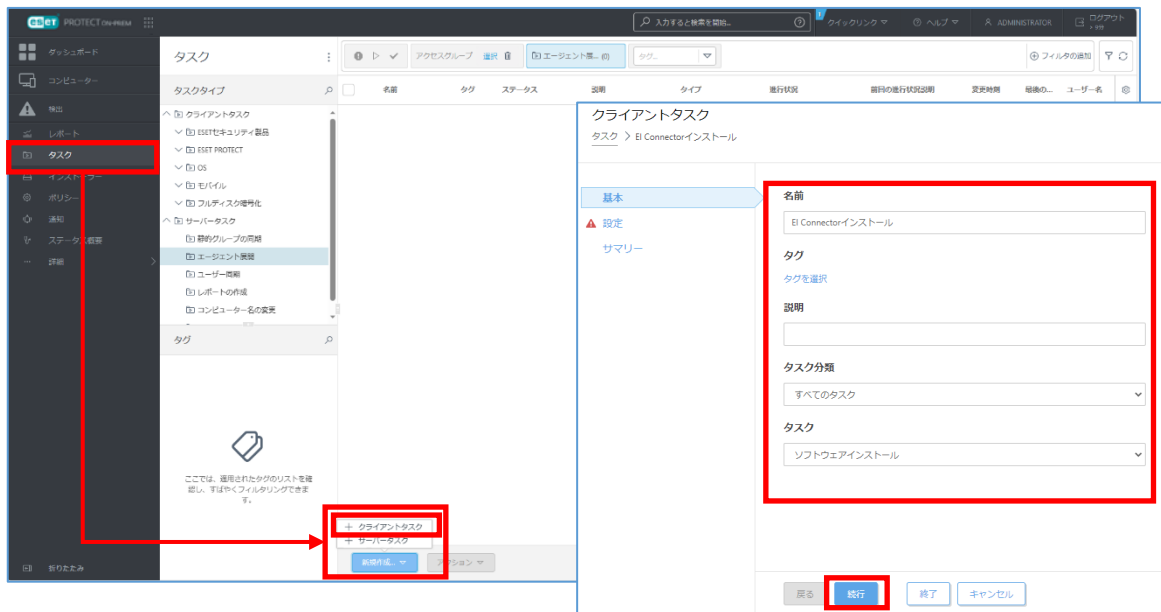
- (5). ライセンス管理画面に追加したライセンス情報が表示されることを確認します。



7.1 (i) クライアントタスクによる EI Connector の展開

すでに EP on-prem でクライアントを管理している場合は、クライアントタスクを使用して EI Connector をインストールが可能です。

(1). [タスク]->[新規作成]-> [クライアントタスク]にて次の通り設定し、[終了]をクリックします。



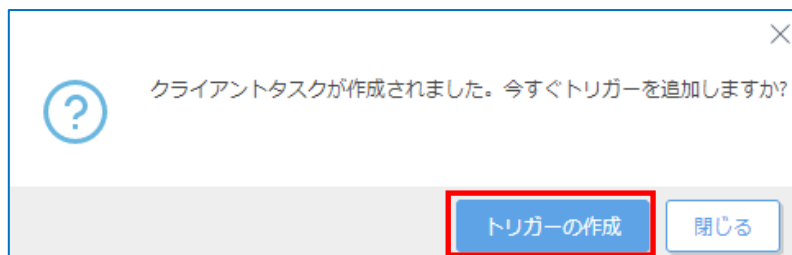
■ [基本]セクション

名前	任意の名前を設定します
説明	説明を記載します。
タスクの分類	すべてのタスク
タスク	「ソフトウェアインストール」を選択します

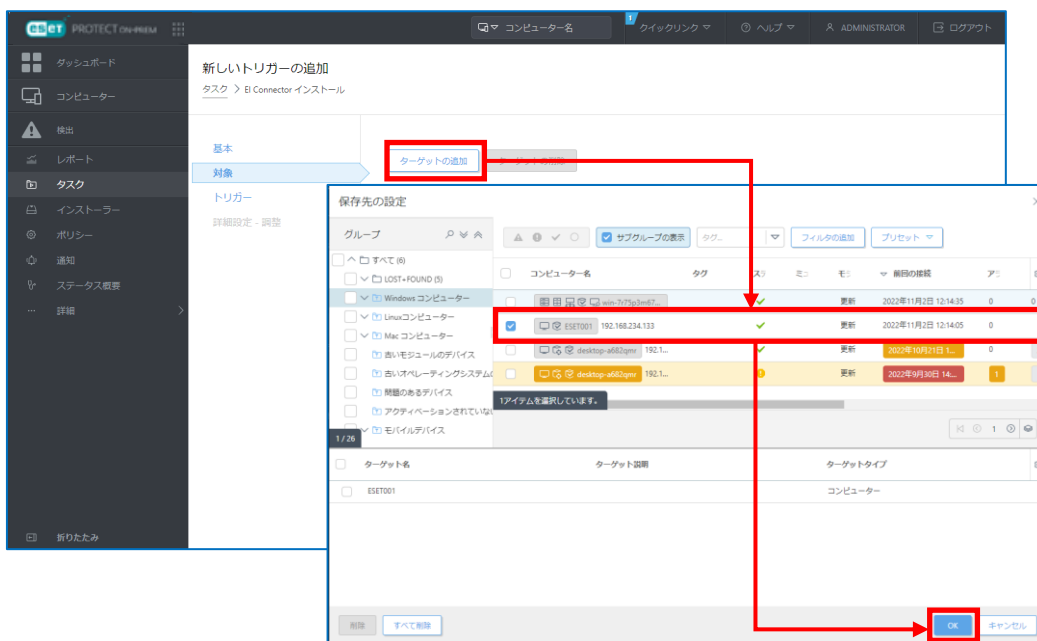
■ [設定]セクション

インストールするパッケージ	[リポジトリからパッケージをインストール]を選択 <パッケージの選択> : EI Connector を選択
ESET ライセンス	登録した EI on-prem ライセンスを選択
[アプリケーションエンドユーザー ー使用許諾書の...]	チェックを入れます
インストールパラメータ	P_HOSTNAME="EI Server の IP アドレス" P_IS_SERVER_ASSISTED=1
必要なときに自動的に再起動	チェックなし

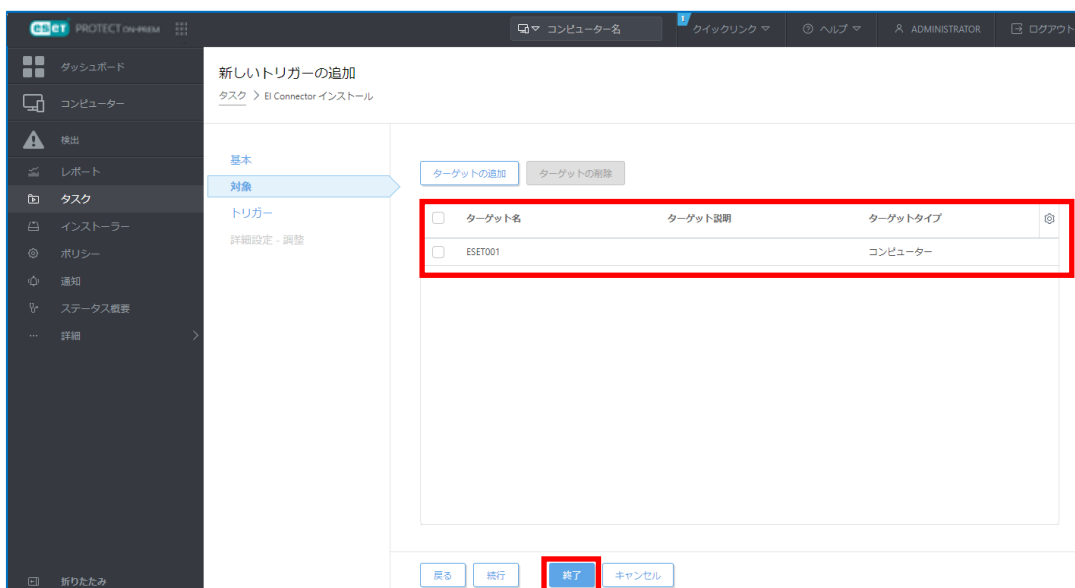
(2). [トリガーの作成]をクリックします。



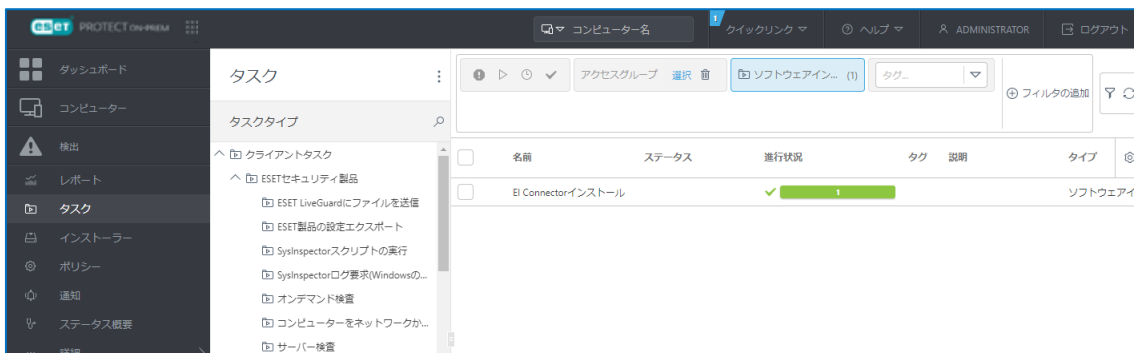
(3). [ターゲット]セクションで、[コンピュータの追加]または[グループの追加]をクリックし、EI Connectorの展開対象を選択後、[OK]をクリックします。



(4). [終了]をクリックします。



- (5). 該当タスクの進捗状況が緑色に遷移したらタスクが成功です。展開対象の PC に「EI Connector」がインストールされていることをご確認ください。

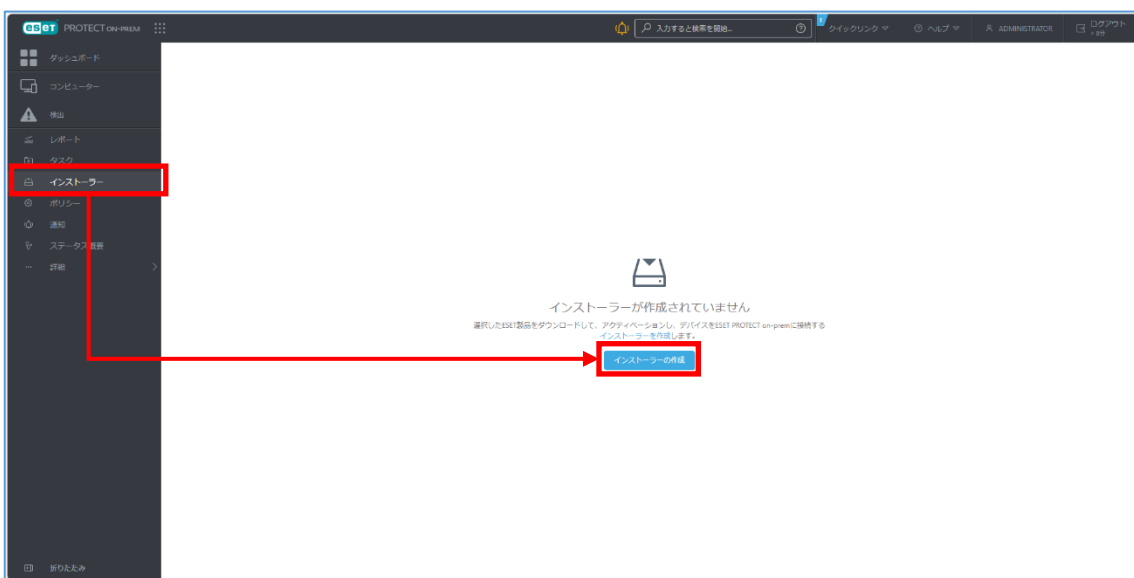


7.2(ii) オールインワンインストーラーによる EI I Connector の展開

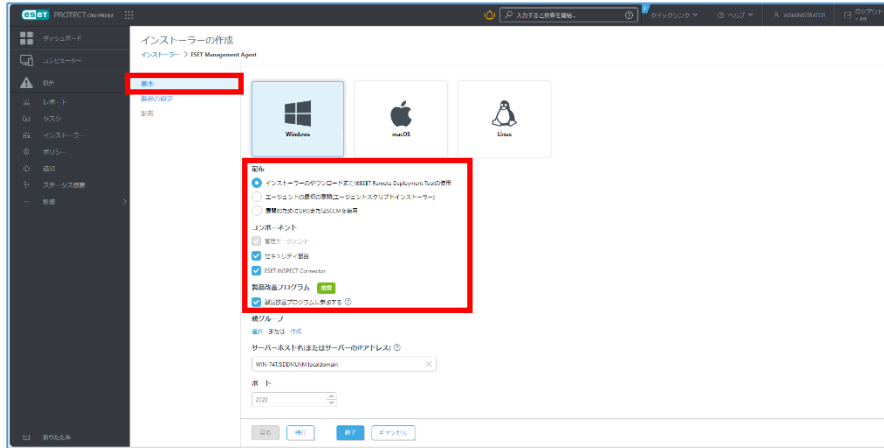
EP on-prem でクライアントを管理していない場合は、EP on-prem で作成したオールインワンインストーラーを使用して、EM Agent とクライアント用プログラムと同時に EI Connector のインストールが可能です。

※ オールインワンインストーラーの作成には、インターネット接続環境が必須です。

- (1). [インストーラー]->[インストーラーの作成]をクリックします。



(2). 「Windows」アイコン→ [インストーラーのダウンロードまたは ESET Remote Deployment Tool の使用] にチェックを入れ、コンポーネントを選択します。

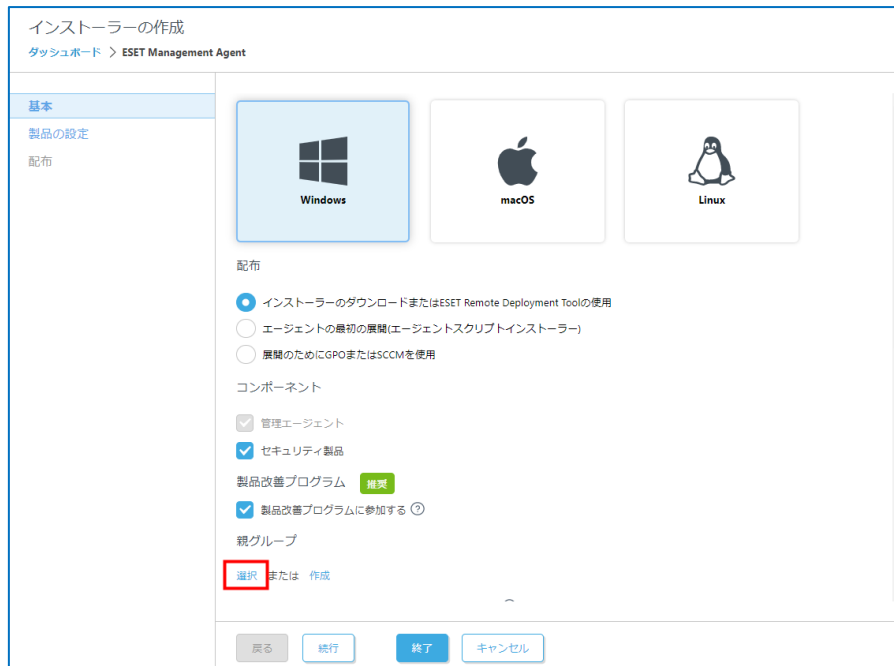


セキュリティ製品	チェックを入れます
ESET Inspect Connector	チェックを入れます

(3). インストールするクライアント端末をすでに作成されたグループに登録する場合は、[親グループ] の [選択] をクリックしてグループを指定します。

※ 特に登録するグループを指定しない場合は「LOST+FOUND」に登録されます。

※ 新しくグループを作成したい場合は、[作成] をクリックして作成します。



- (4). [サーバーホスト名 (またはサーバーの IP アドレス)] に、セキュリティ管理ツールのホスト名、または、IP アドレスを入力します。

インストーラーの作成
ダッシュボード > ESET Management Agent

基本
製品の設定
配布

サーバーホスト名(またはサーバーのIPアドレス) ②

ポート

- (5). ポート番号「2222」が入力されていることを確認します。

インストーラーの作成
ダッシュボード > ESET Management Agent

基本
製品の設定
配布

サーバーホスト名(またはサーバーのIPアドレス) ②

ポート

2222

ピア証明書

- (6). [ピア証明書] の [ESET PROTECT 証明書] を選択し、証明書が正しいことを確認します。

パスフレーズを設定している場合は、設定したパスフレーズを入力します。

インストーラーの作成
ダッシュボード > ESET Management Agent

基本
製品の設定
配布

サーバーホスト名(またはサーバーのIPアドレス) ②

ポート

2222

ピア証明書

ESET PROTECT 証明書
 カスタム証明書

ESET PROTECT 証明書

説明 サーバー証明書、

証明書パスフレーズ ②

(7). [その他の設定をカスタマイズ] をクリックし、各項目を設定します。

インストーラーの作成
インストーラー > ESET Endpoint Security + ESET Inspect Connector

基本

製品の設定

配布

証明書ハッシュのレスポンス

[その他の設定をカスタマイズ](#) >

● インストーラー名

説明 (任意)

コンポーネントインストール

常に利用可能な新バージョンの製品とコンポーネントをインストール ②

タグ

[タグを選択](#)

初期構成 (任意) ②

この構成は初期構成としてのみ使用されます。ポリシーが適用されたグループ内にデバイスが設置される場合、構成は置き換えられます。コンピューターの「運用済みポリシー」で初期構成は見えません。

エージェント設定

[選択](#) または [作成](#)

HTTPプロキシ設定

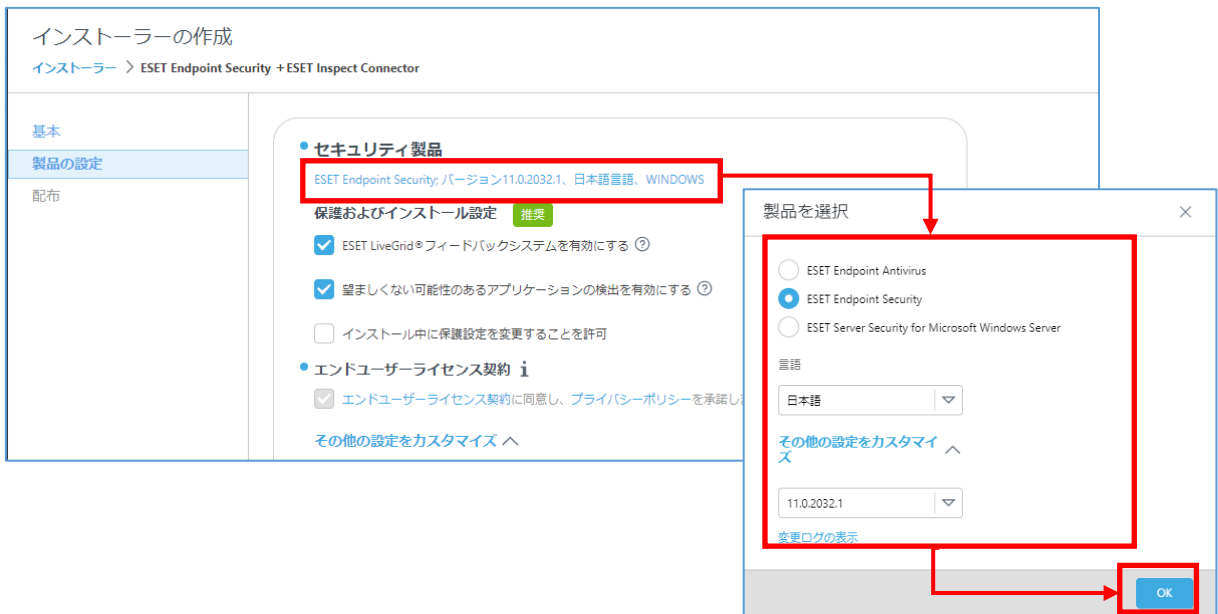
HTTPプロキシ設定を有効にする

戻る
続行
終了
キャンセル

インストーラー名	任意の名前を入力します。
コンポーネントインストール	チェックを入れるとリポジトリに公開されている最新バージョンがインストールされます。
エージェント設定	ESET Management エージェントにポリシーを適用する場合、[選択] をクリックします。

(8). [製品の設定] → [セキュリティ製品] を選択し、以下の設定をして [OK] ボタンをクリックします。

- ・製品を変更する場合、インストールしたいクライアント用プログラムを選択
- ・[言語] を [日本語] に設定
- ・プログラムのバージョンを変更する場合、[詳細] にチェックを入れてバージョンを選択



(9). [エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。] にチェックを確認します。



(10). [その他の設定をカスタマイズ] をクリックし、[ライセンス] にオールインワンインストーラーの作成に利用するライセンスが登録されているか確認します。



(11).クライアント用プログラムにポリシーを適用する場合、[設定] の [選択] をクリックします。



(12). [ESET AV リムーバーを実行] に**チェックが入っていない**ことを確認します。

インストーラーの作成
インストーラー > ESET Endpoint Security + ESET Inspect Connector

基本
製品の設定
配布

● セキュリティ製品
ESET Endpoint Security バージョン11.0.2032.1, 日本語言語, WINDOWS
保護およびインストール設定 [推奨](#)

- ESET LiveGrid®フィードバックシステムを有効にする ②
- 望ましくない可能性のあるアプリケーションの検出を有効にする ②
- インストール中に保護設定を変更することを許可

● エンドユーザーライセンス契約 ⓘ
 エンドユーザーライセンス契約に同意し、プライバシーポリシーを承認します。

その他の設定をカスタマイズへ

ライセンス
[Redacted] ×

設定
選択 または 作成

ESET AV Removerを実行
 ESET AV Removerを有効にすると、該当するエンドユーザーライセンス契約に同意したものとします

モジュールインストール
 すべてのESETモジュールが含まれるセキュリティ製品インストーラーを使用 ②

(13). [モジュールインストール] に以下の通り設定します。

ESET AV リムーバーを実行
 ESET AV REMOVERを有効にすると、該当するエンドユーザーライセンス契約に同意したものとします

モジュールインストール
 すべてのESETモジュールが含まれるセキュリティ製品インストーラーを使用 ②

すべての必須フィールドを入力してください

戻る 続行 終了 キャンセル

フルモジュールインストーラーを使用する場合	チェックを入れる
最小モジュールインストーラーを使用する場合	チェックを外す

- (14). [製品の設定] → [ESET Inspect Connector] 内にあるプログラム名をクリックし、必要に応じて[詳細]にチェックを入れてバージョンを選択します。

※言語は英語のみとなります。



- (15). [エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。]にチェックを確認します。



(16). [その他の設定をカスタマイズ] をクリックし、以下の設定をします。

- ・サーバーホスト名に EI Server のホスト名または IP アドレスを入力
- ・ポートに 8093(既定)を入力

インストーラーの作成
インストーラー > ESET Endpoint Security + ESET Inspect Connector

基本
製品の設定
配布

● エンドユーザーライセンス契約
 エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。
その他の設定をカスタマイズ >

● ライセンス
設定
選択 または 作成

ESET Inspectサーバー設定

サーバーホスト名
ポート

認証局
 ESET PROTECT認証局
 カスタム認証局
ESET PROTECT認証局
選択

(17). 認証局では[ESET PROTECT 認証局]を選択し、[選択]をクリックして認証局を選択します。

インストーラーの作成
インストーラー > ESET Endpoint Security + ESET Inspect Connector

基本
製品の設定
配布

● エンドユーザーライセンス契約
 エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。
その他の設定をカスタマイズ >

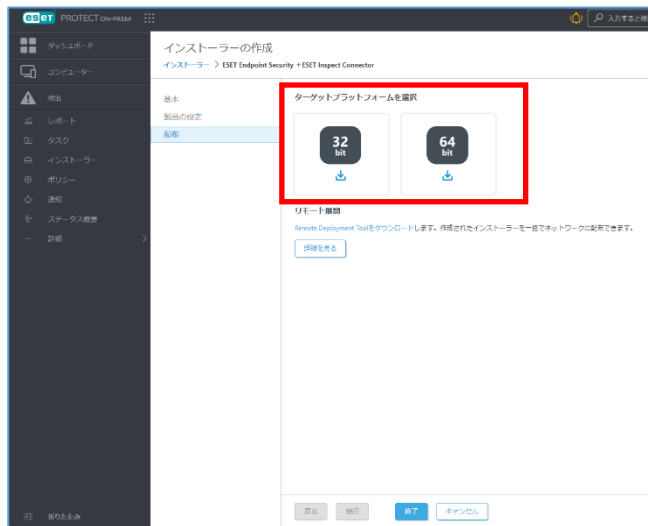
● ライセンス
設定
選択 または 作成

ESET Inspectサーバー設定

サーバーホスト名
ポート

認証局
 ESET PROTECT認証局
 カスタム認証局
ESET PROTECT認証局
選択

(18).[終了]をクリックし、インストールするクライアント端末の環境にあわせて、[32bit版をダウンロード]、[64bit版をダウンロード]、のいずれかをクリックします。



(19).ダウンロードしたオールインワンインストーラーを各クライアントに展開して実行します。

8. EI Web Console の確認【EI 側作業】

(1). [https://\(EI Server を導入したサーバーの IP アドレス\)](https://(EI Server を導入したサーバーの IP アドレス)) にアクセスします。

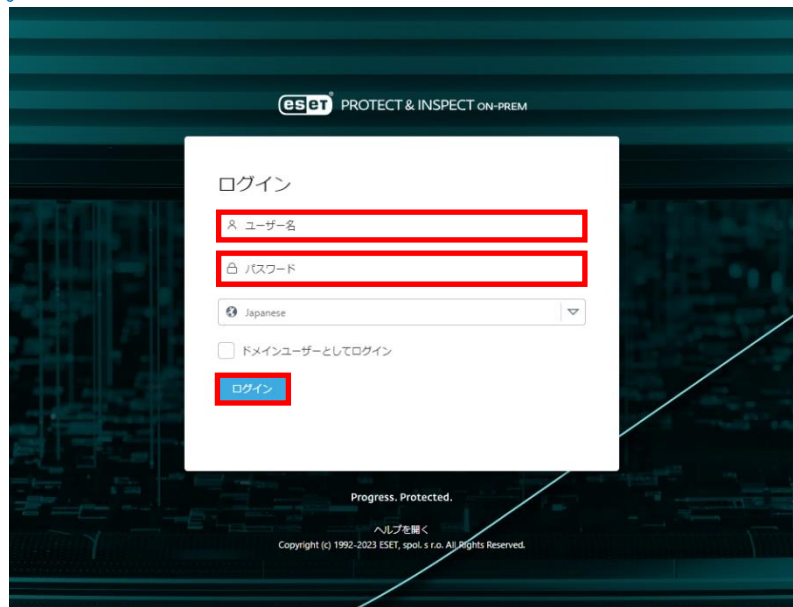
以下の画面が表示されますので、「xxx.xxx.xxx.xxx にアクセスする（安全ではありません）」をクリックします。



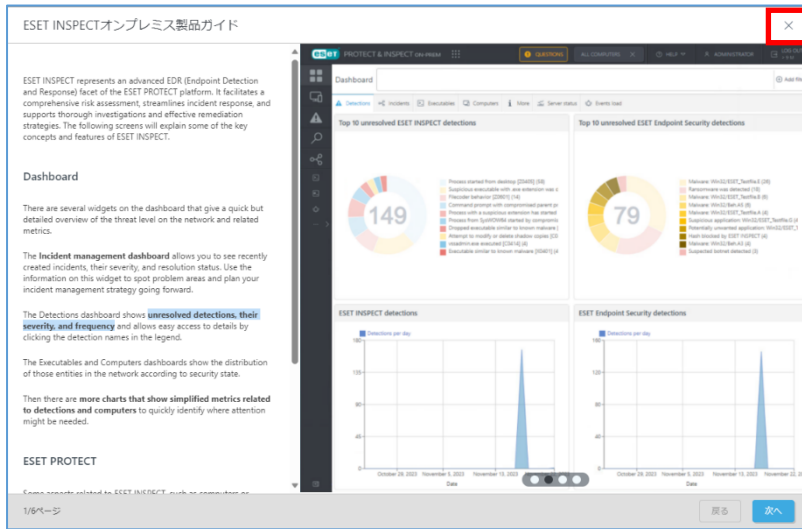
注意

ここでは、ESET PROTECT インストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。お使いのブラウザにより、表示内容が異なります。

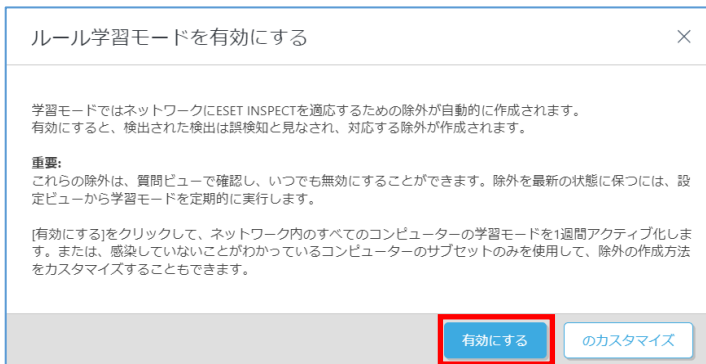
(2). 言語を「Japanese」に選択して「項番 4.3 ユーザーアカウント作成（例:本手順書では EI_SERVER）」で作成した、ユーザー名、パスワードを入力し [ログイン] をクリックします。



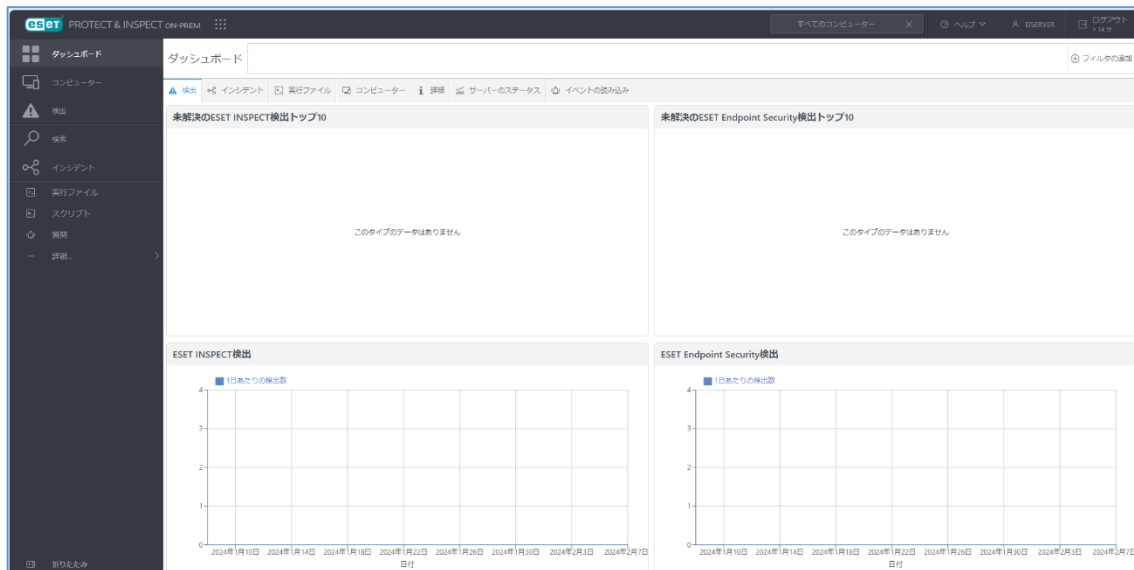
(3). 初回ログイン時、以下の画面が表示されたら、「×」で閉じます。



(4). 以下の画面では期間と対象グループを指定し自動で除外ルールを作成可能です。(任意)



(5). EI on-prem にログインできることを確認します。



以上で ESET Inspect on-prem の導入は完了です。

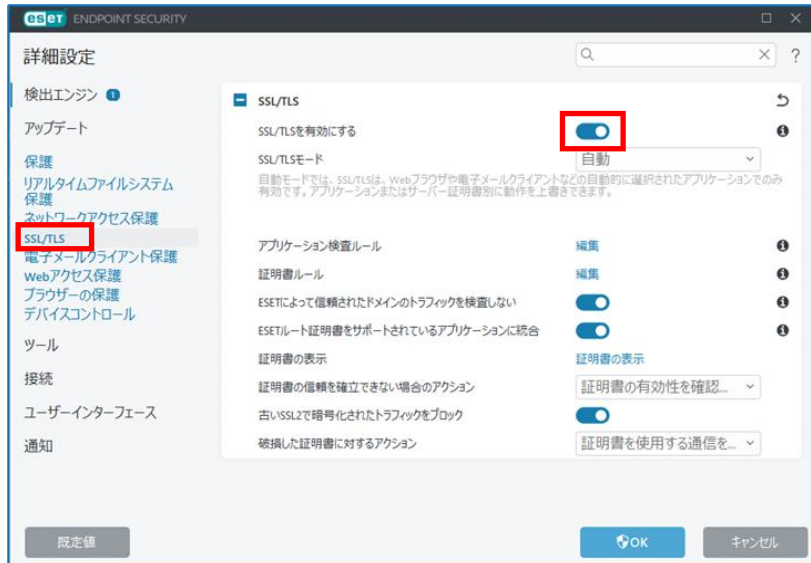
※以降は EI on-prem 導入時の ESET Endpoint 製品の推奨設定をご案内しております。

9. EI on-prem 導入時の ESET Endpoint 製品の推奨設定

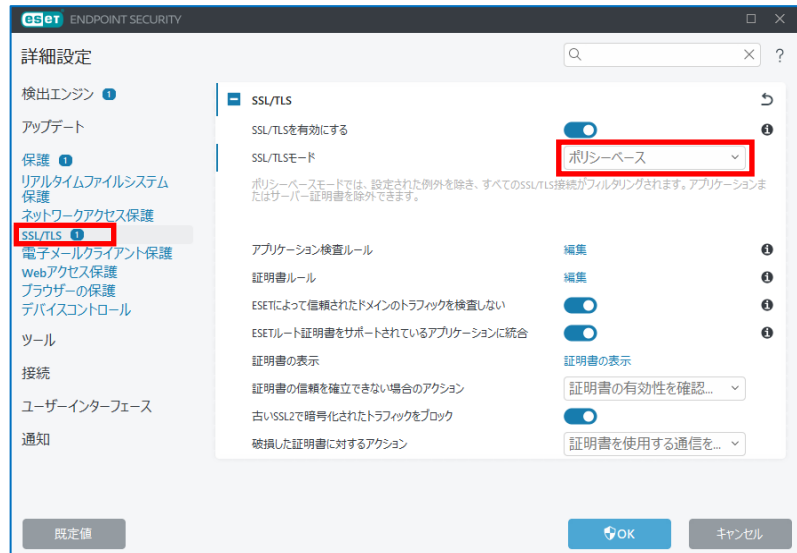
高度なセキュリティを保ちつつ、EI on-prem をより効果的に活用いただくために以下の設定を推奨いたします。

9.1 推奨設定の実施（ESET Endpoint 製品の詳細設定）

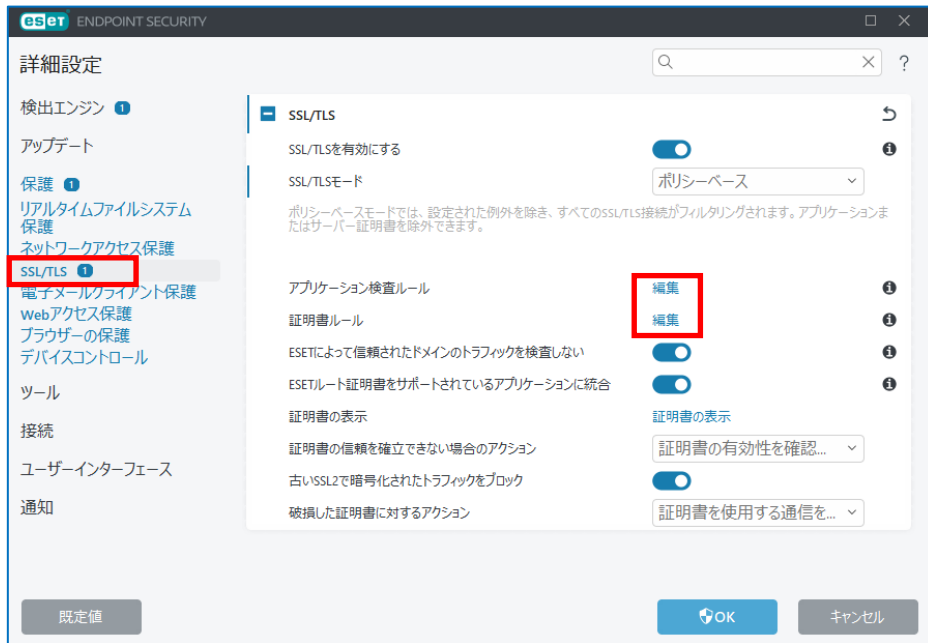
(1). 【SSL/TLS を有効にする】を有効にします。



(2). 【SSL/TLS モード】をポリシーベースモードにします。

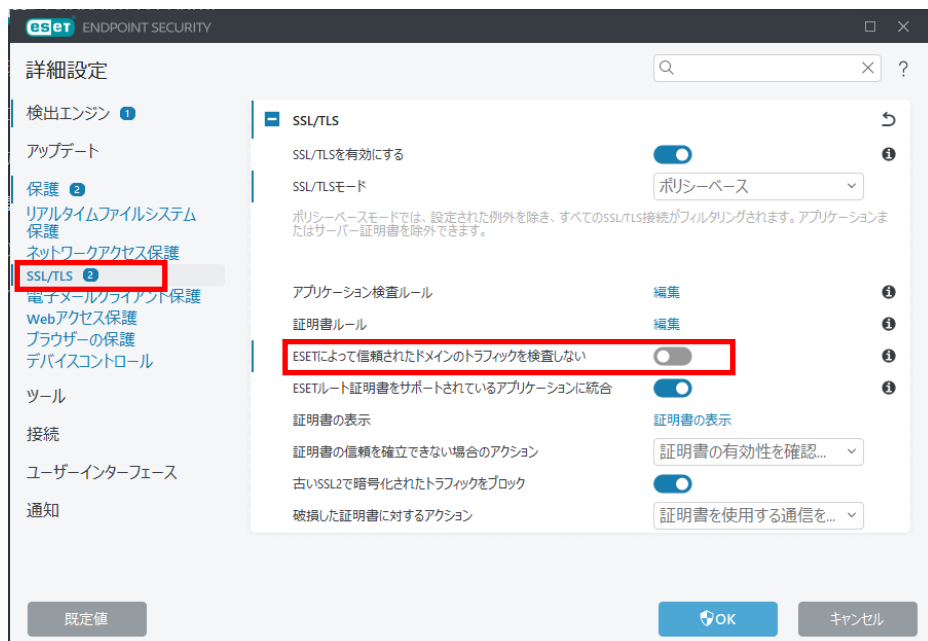


※ポリシーベースモードはデフォルトで全てのSSL/TLS接続がフィルタリングされてしまうため、必要に応じて【アプリケーション検査ルール】と【証明書ルール】の編集を行い、検査アクション“無視”を設定してください。



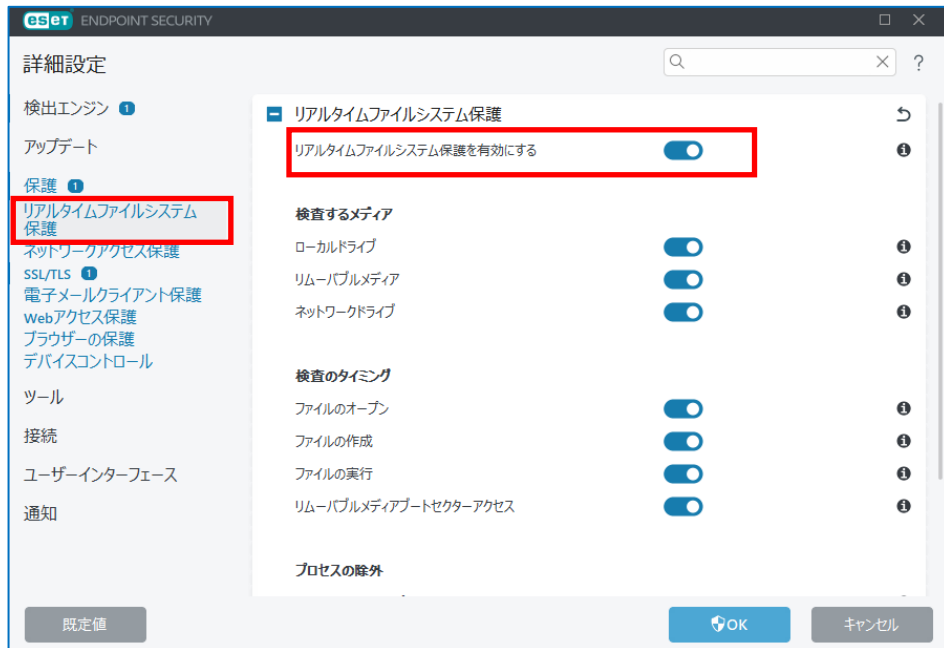
(3). 【ESET によって信頼されたドメインのトラフィックを検査しない】を無効にします。

※ドメインフロンティング攻撃に対応する為の設定です。



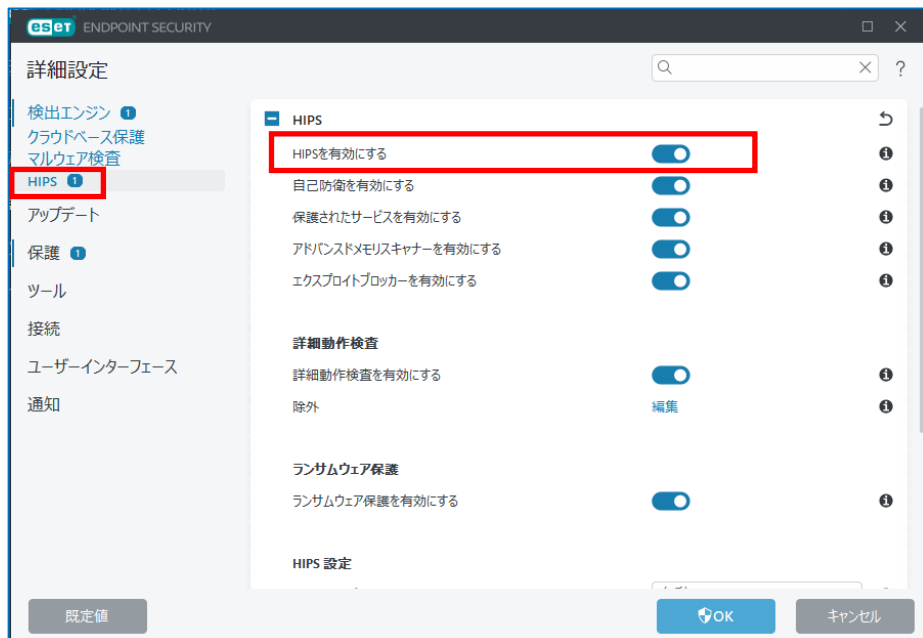
(4). 【リアルタイムファイルシステム保護を有効にする】を有効にします。

※無効の場合、EI on-prem の機能を正常に利用できません。



(5). 【HIPS を有効にする】を有効にします。

※無効の場合、EI on-prem の機能を正常に利用できません。



本手順書は以上で終了です。