XDR (eXtended Detection and Response)
ESET Inspect on-prem（V3.1）
導入手順書

第 1.0 版

2026 年 7 月 15 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	2026 年 7 月 15 日	初版発行

内容

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	8.4.0 以降 or 9.7.1 以降
Microsoft SQL Server	2017 以降

※EI Server のインストールには、64 ビット Microsoft Visual C++再頒布可能パッケージのインストールが必要となります。

※システム要件の詳細は以下をご確認ください。

https://help.eset.com/ei_deploy/3.1/en-US/?system_requirements.html

【ESET 環境】

製品名	バージョン
ESET Inspect on-prem	3.1
ESET PROTECT on-prem	11.1 以降

※本手順書は EP on-prem V13.0 を使用して作成しています。

○ 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

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 V11.1 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をご確認ください。

https://help.eset.com/ei_deploy/3.1/en-US/os_settings_windows.html?hardware_requirements.html

(3). インストール可能なサポート OS とデータベース以下をご確認ください。

・サポート OS

https://help.eset.com/ei_deploy/3.1/en-US/operating_systems.html

・データベース

https://help.eset.com/ei_deploy/3.1/en-US/database.html

2.2 EI Connector 要件

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

https://help.eset.com/ei_deploy/3.1/en-US/web_browsers.html

(2). オンプレミス型セキュリティ管理ツール V11.1 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 は以下をご確認ください。

※ESET Inspect on-prem の動作環境をご参照ください。

https://eset-support.canon-its.jp/faq/show/4926?site_domain=business

(4). 使用上の注意事項については以下をご確認ください。

https://eset-info.canon-its.jp/files/user/pdf/manual/ei_v31_readme.pdf

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 および EM 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】

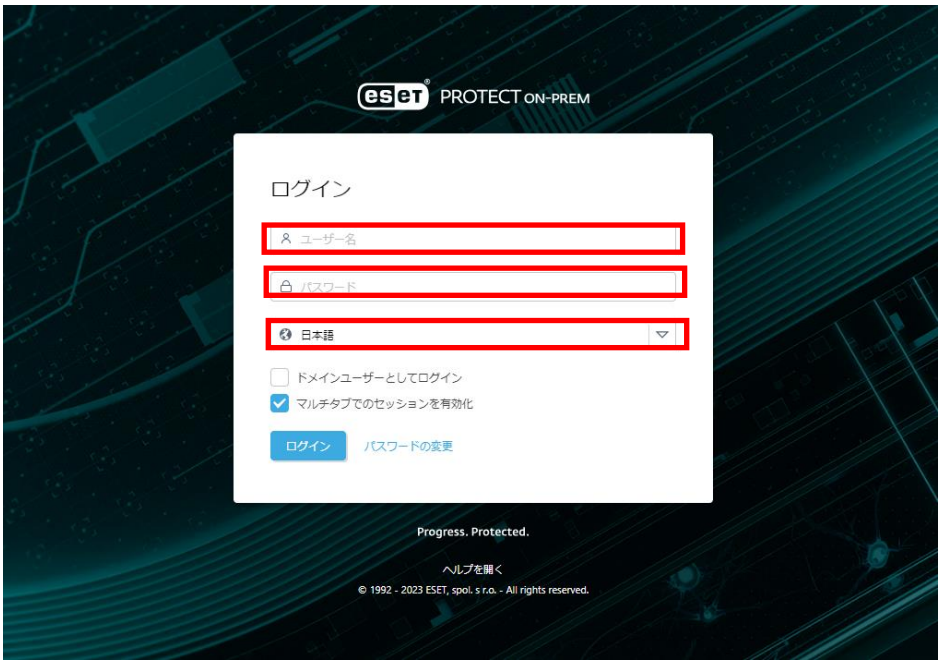
4-1 高度なセキュリティの有効化

(1). https://(EP on-prem Server を導入したサーバーの IP アドレス)/era 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。

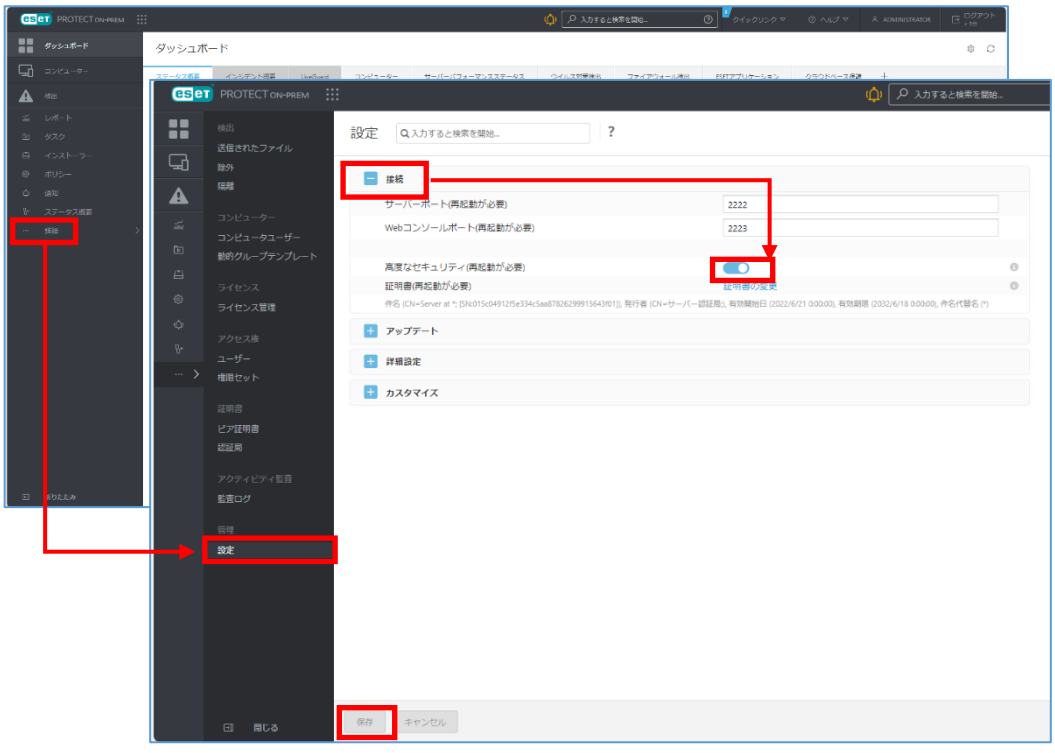
注意

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。

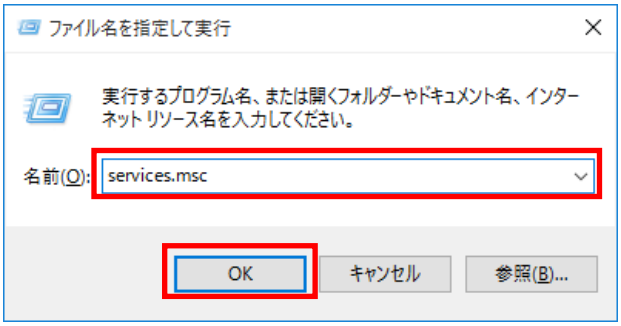
(2). EP Web Console に管理者権限のあるアカウントでログインします。
「日本語」選択して「EP ログインユーザー名」、「EP ログインパスワード」を入力し、「ログイン」をクリックします。



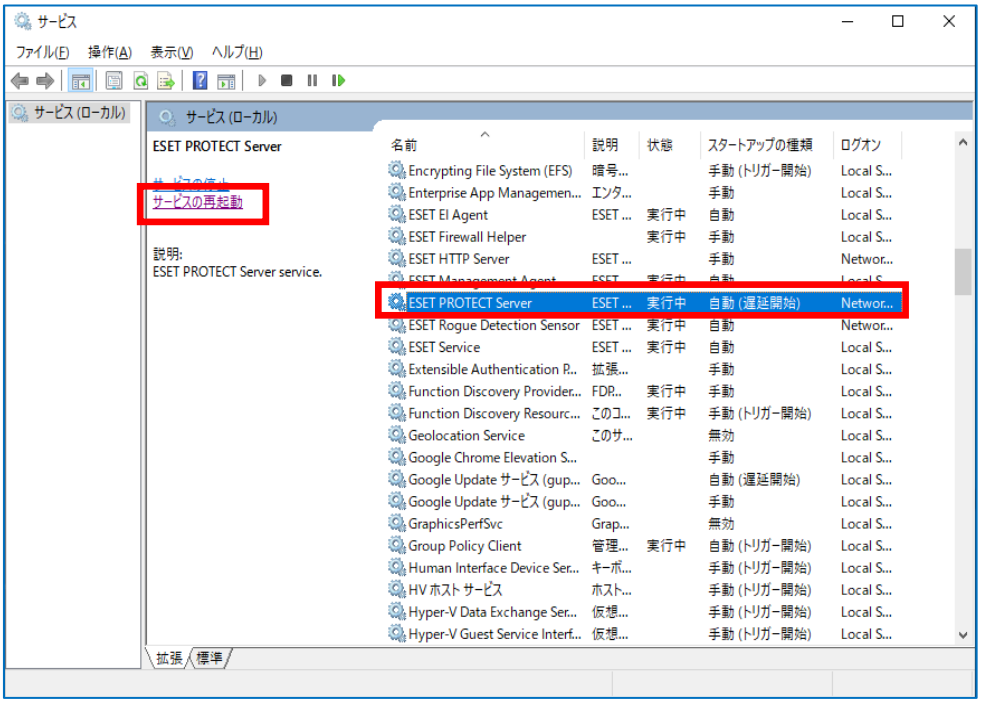
(3). [詳細]->[設定]->[接続]->[高度なセキュリティ(再起動が必要)]を有効化し、[保存]をクリックします。



(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。



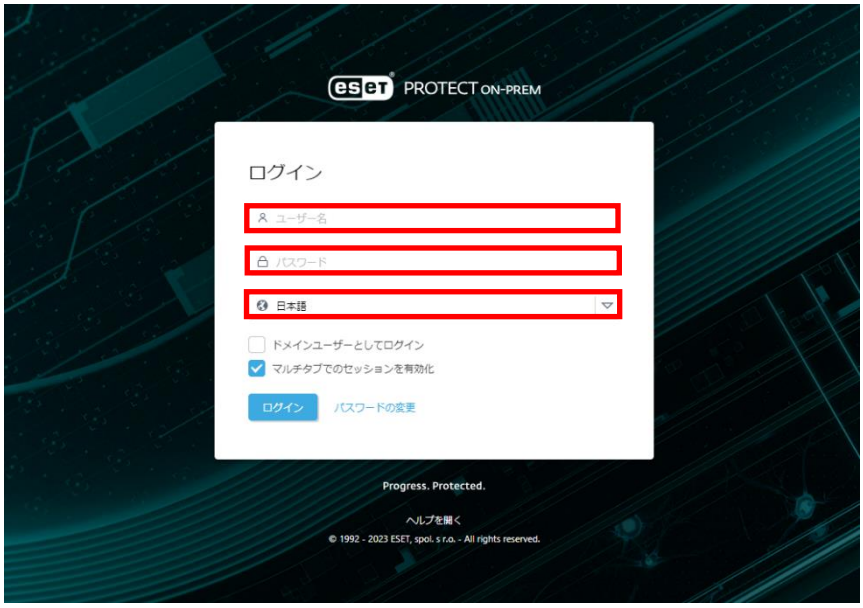
(5).「ESET PROTECT Server」を選択し、[サービスの再起動]をクリックします。「ESET PROTECT Server」サービスの状態が、実行中であることを確認します。



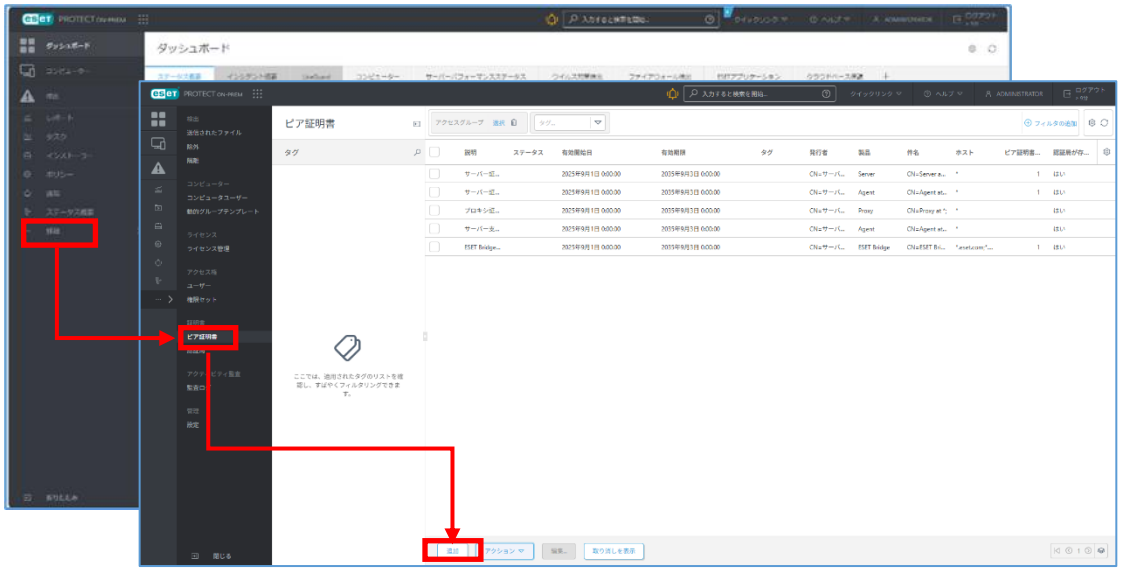
4.2 証明書作成

(1). EP Web Console に再ログインします。

「日本語」を選択して、「EP ログインユーザー名」、「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。

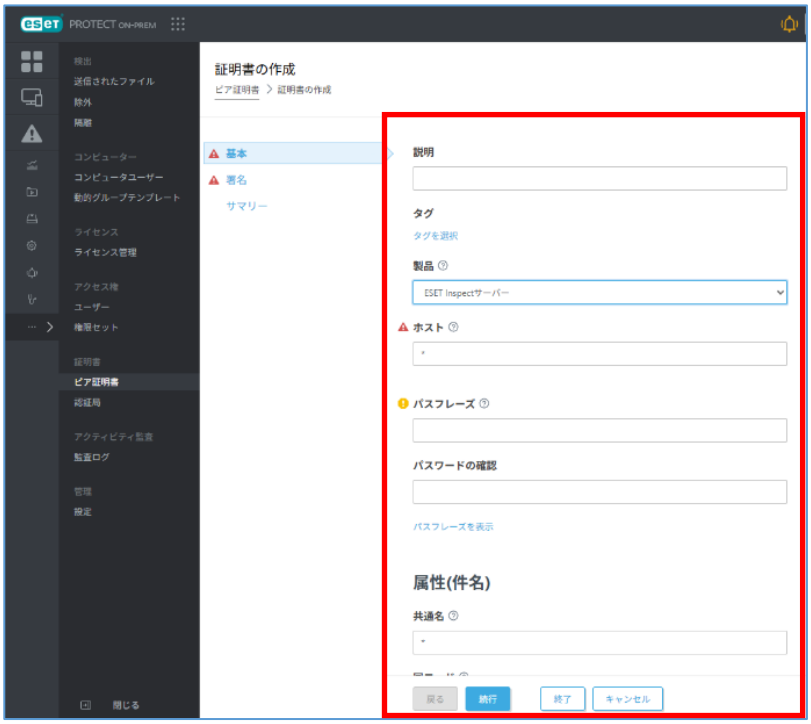


(2). [詳細]->[ピア証明書]->[追加]をクリックします。



(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。

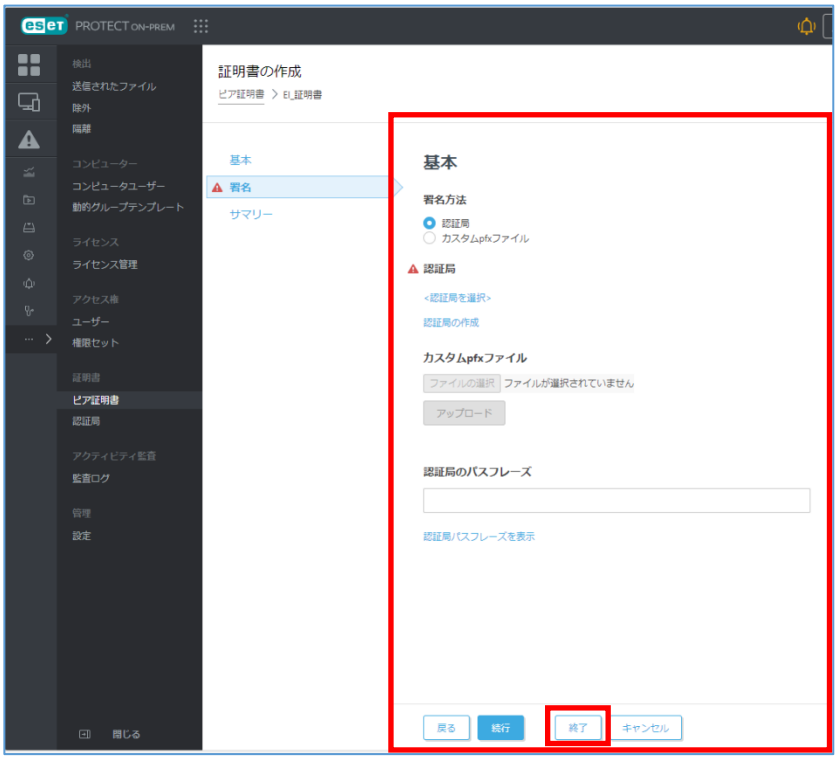
■[基本]セクション



■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

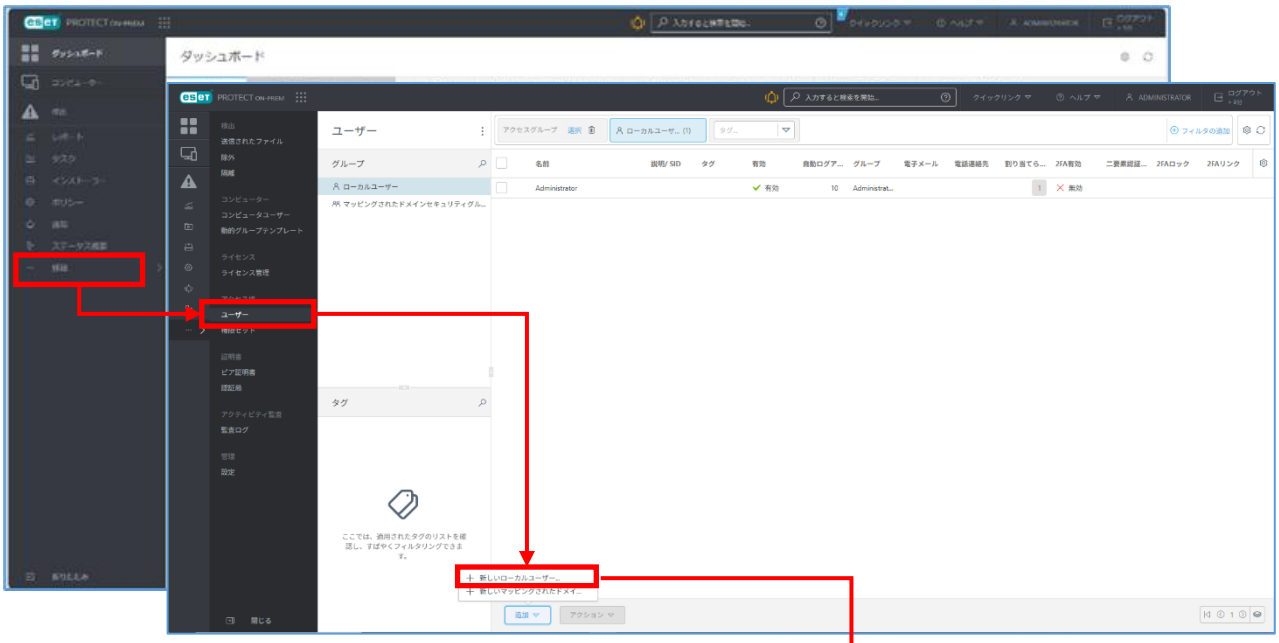


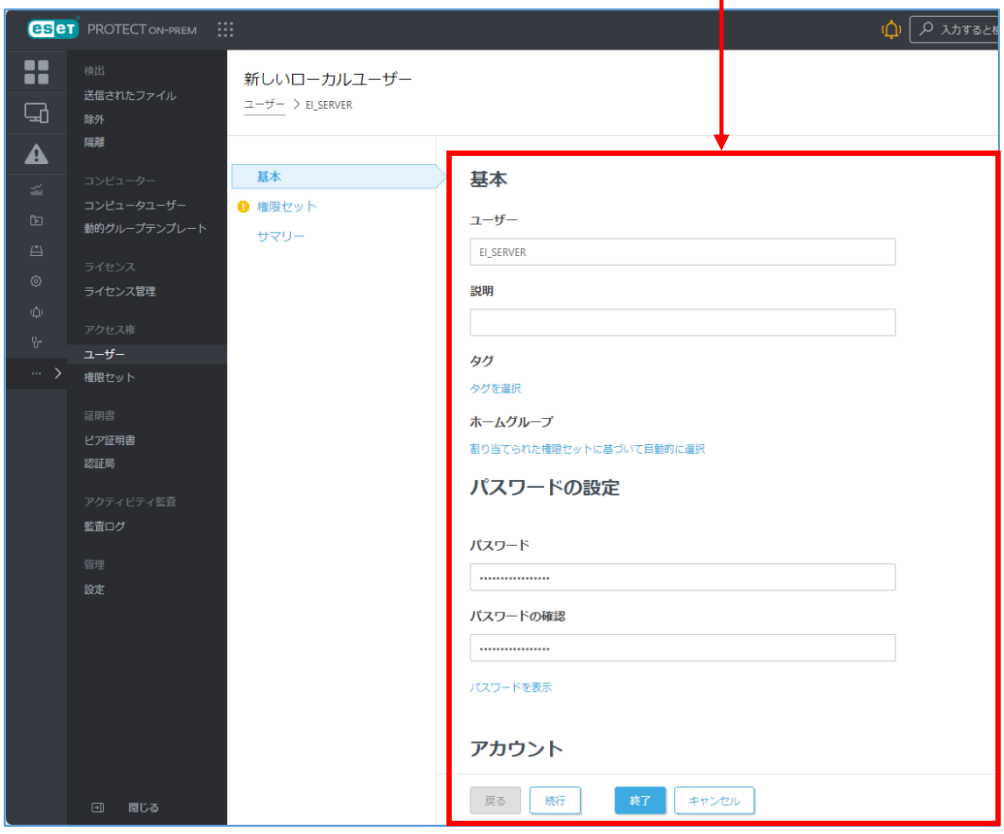
■設定値

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]->[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。

(3). [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 MySQL 8.4 or 9 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 MySQL 8.4 or 9 のインストール

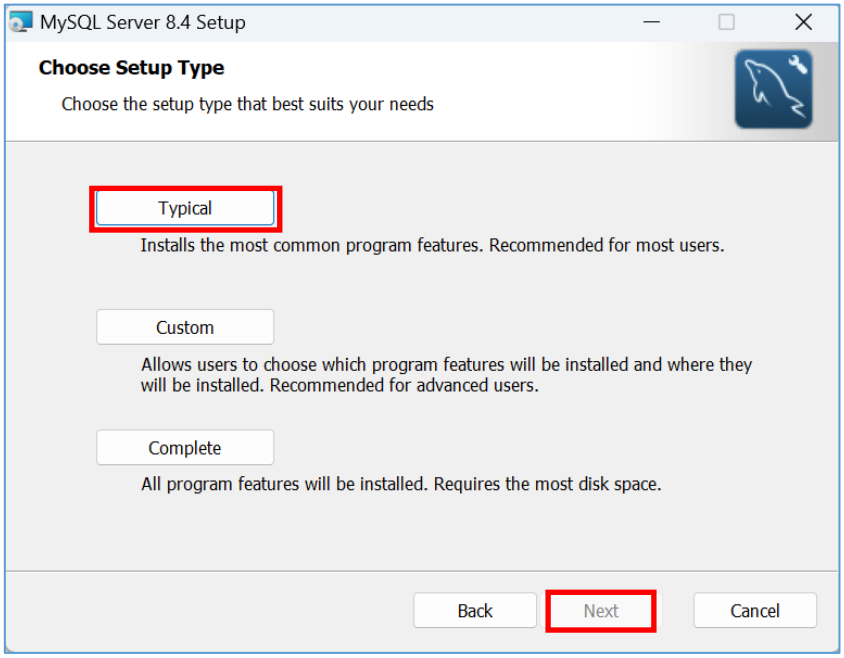
MySQL 8.4 or 9 を利用する場合は以下の手順を実施後、「6.EI サーバーのインストール」を行ってください。

※インストールするバージョンによっては画面が異なる場合がありますので、その場合は読み替えて実施ください。

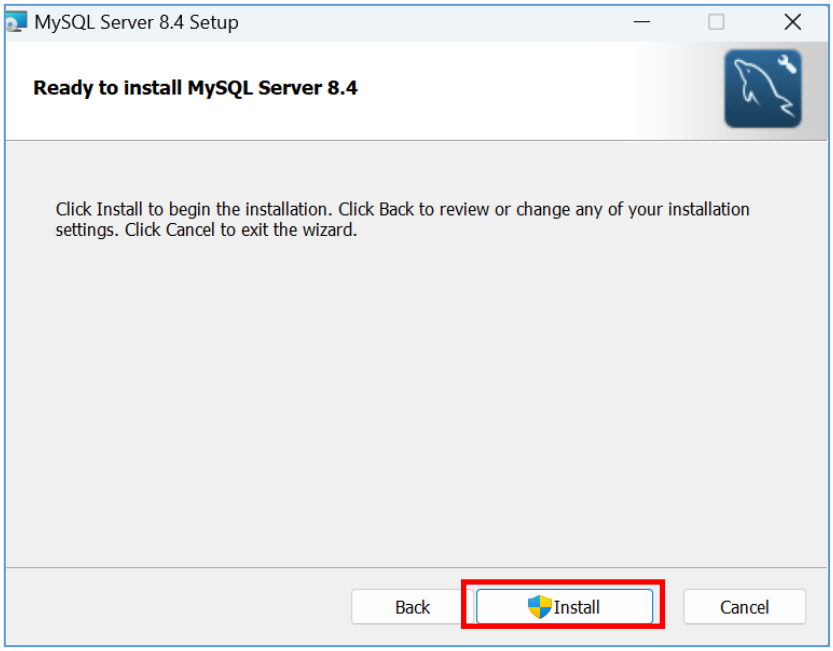
(1). MySQL を導入するサーバーに「Microsoft Visual C++ 2015-2022 redistributable Package(x64)」がインストールされていない場合は、以下 URL よりダウンロード、およびインストールを完了させます。
https://learn.microsoft.com/ja-jp/cpp/windows/latest-supported-vc-redist?view=msvc-170

(2). 以下 URL より、MySQL のインストーラー(mysql-8.4.x-winx64.msi あるいは mysql-9.x.x-winx64.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/mysql/

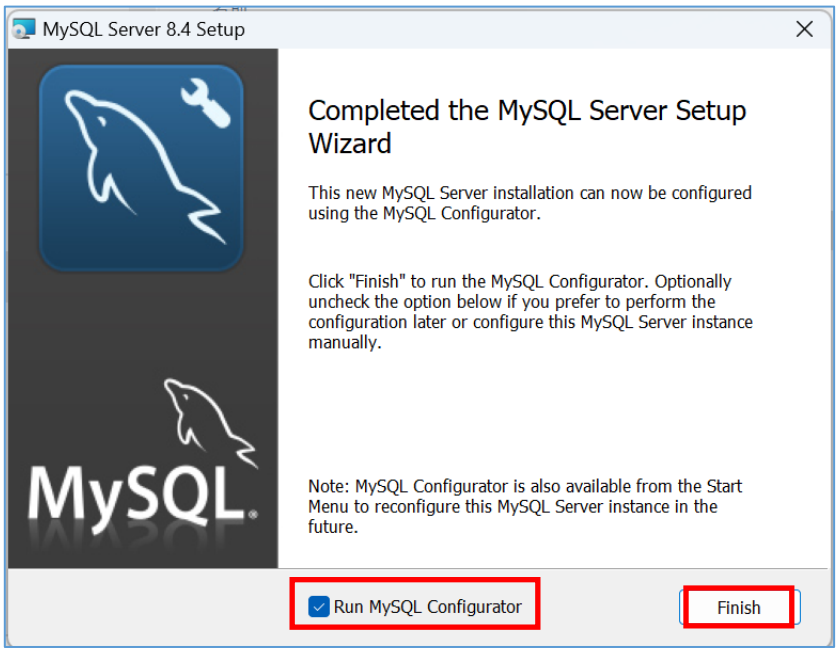
(3). Choosing a Setup Type 画面で[Typical]を選択し[Next]をクリックします。



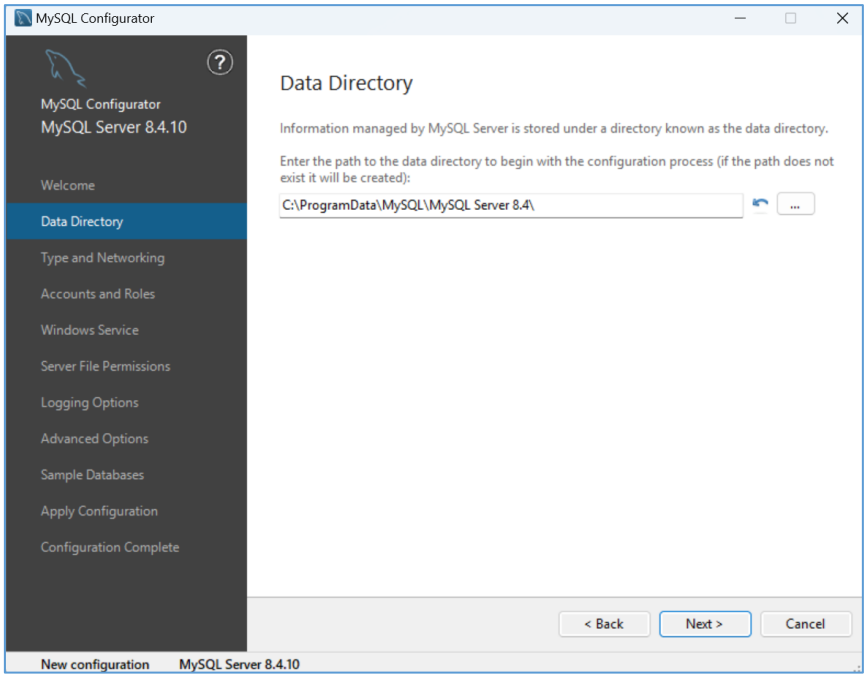
(4). Installation 画面で MySQL Sever が対応しているバージョンであることを確認し [Install]をクリックします。



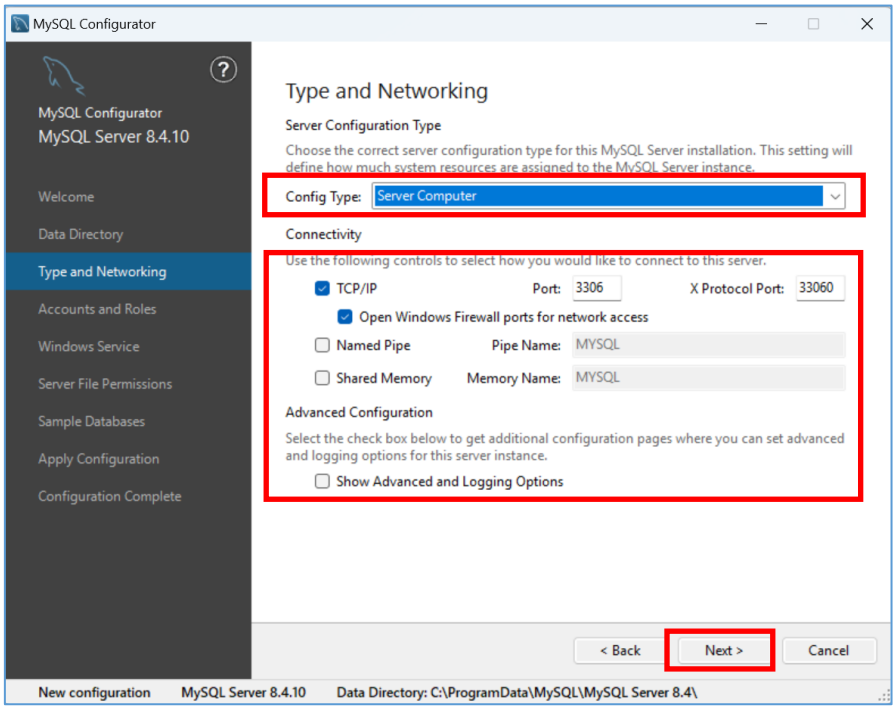
(5).「Run MySQL Configurator」 にチェックがついていることを確認し [Finish]をクリックします。



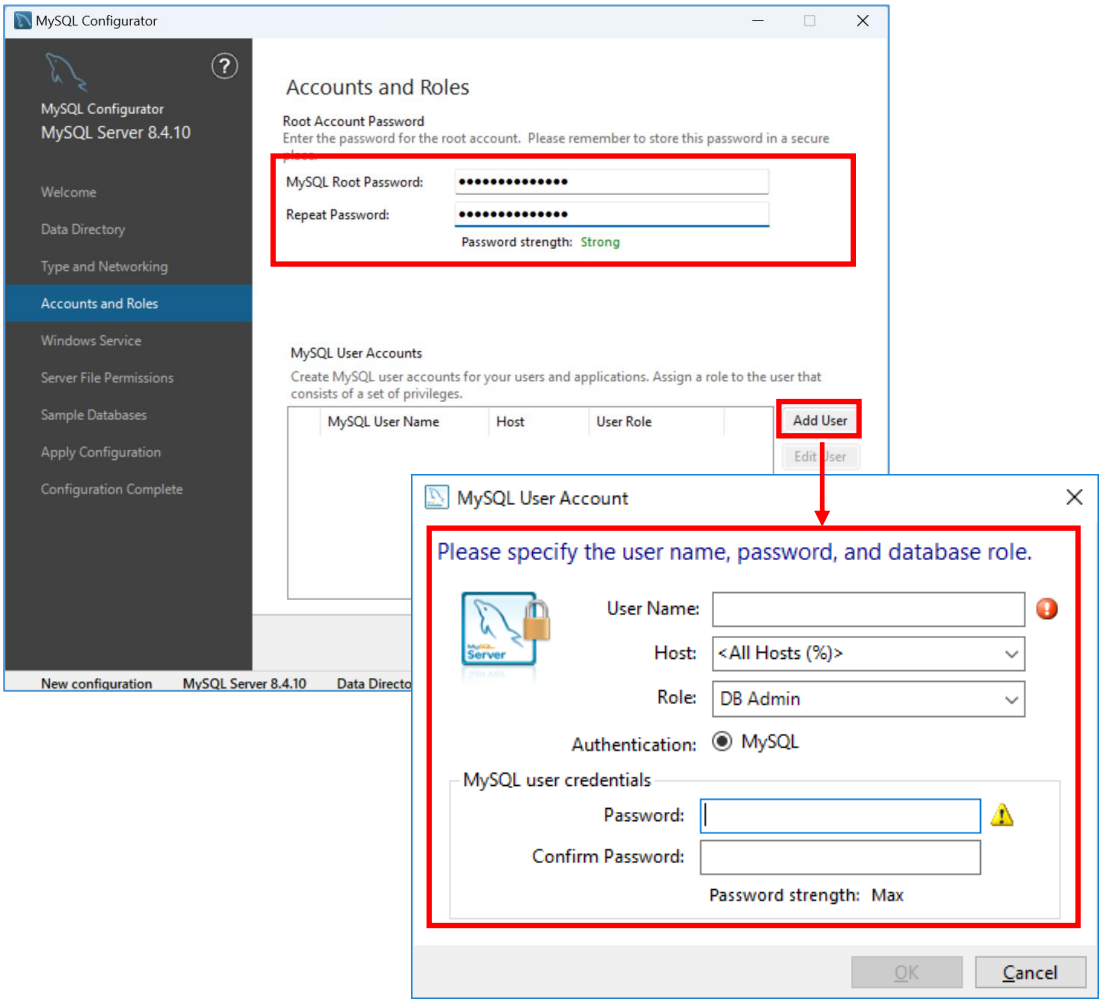
(6). 任意の保存場所を選択し、[Next]をクリックします。



(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). 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。



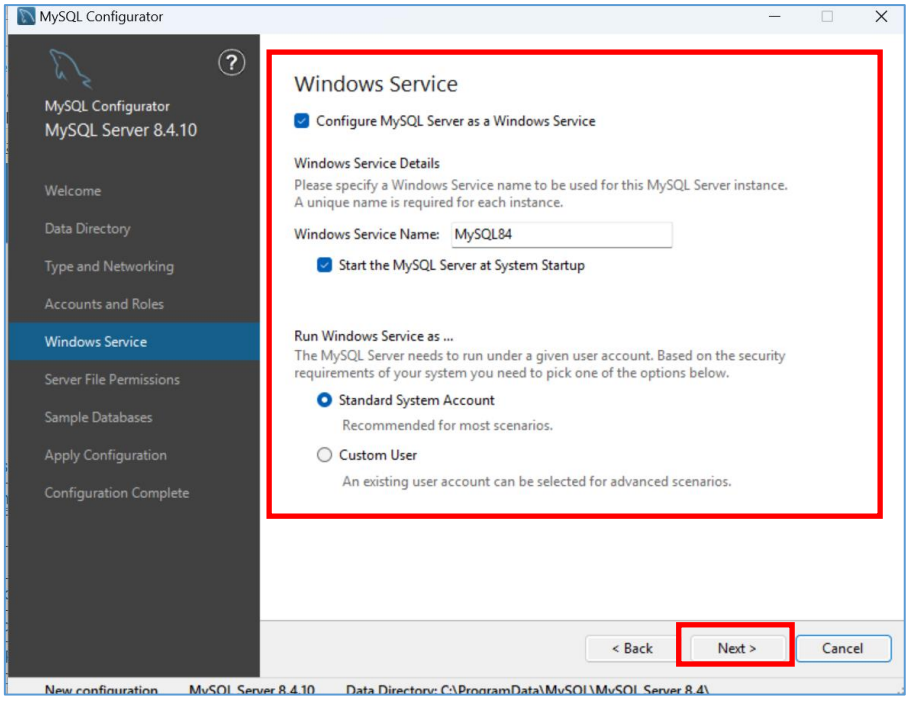
MySQL User Account ダイアログで、以下の通り入力します。

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)

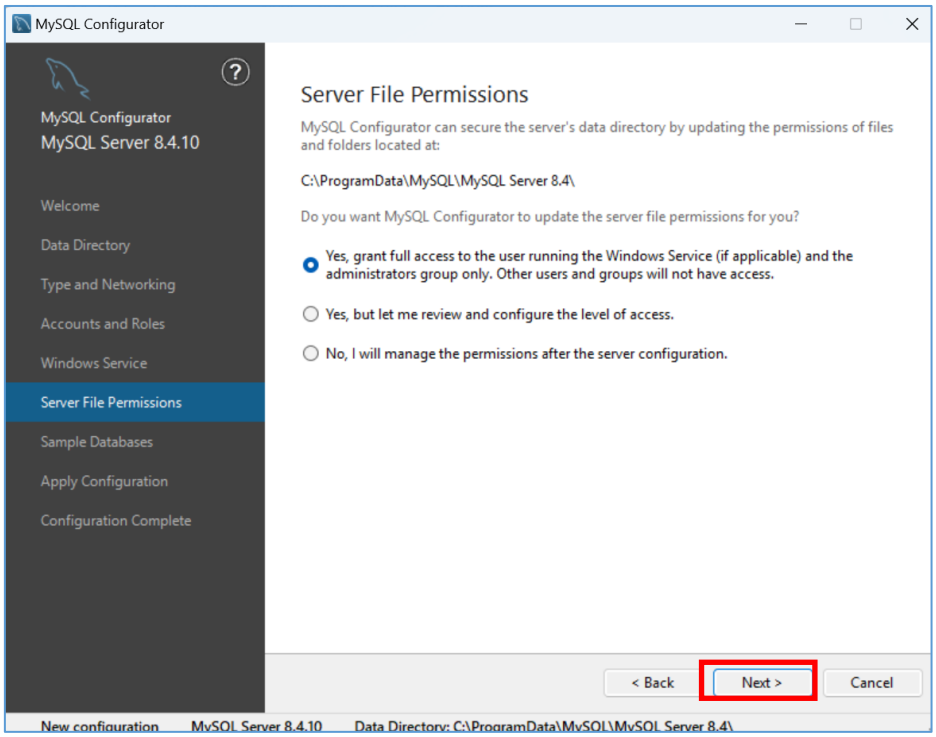
※本項番で入力した MySQL ユーザーアカウントとパスワードをメモしてください。
MySQL ユーザーアカウントとパスワードは項番 6-1 (7)で使用します。

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

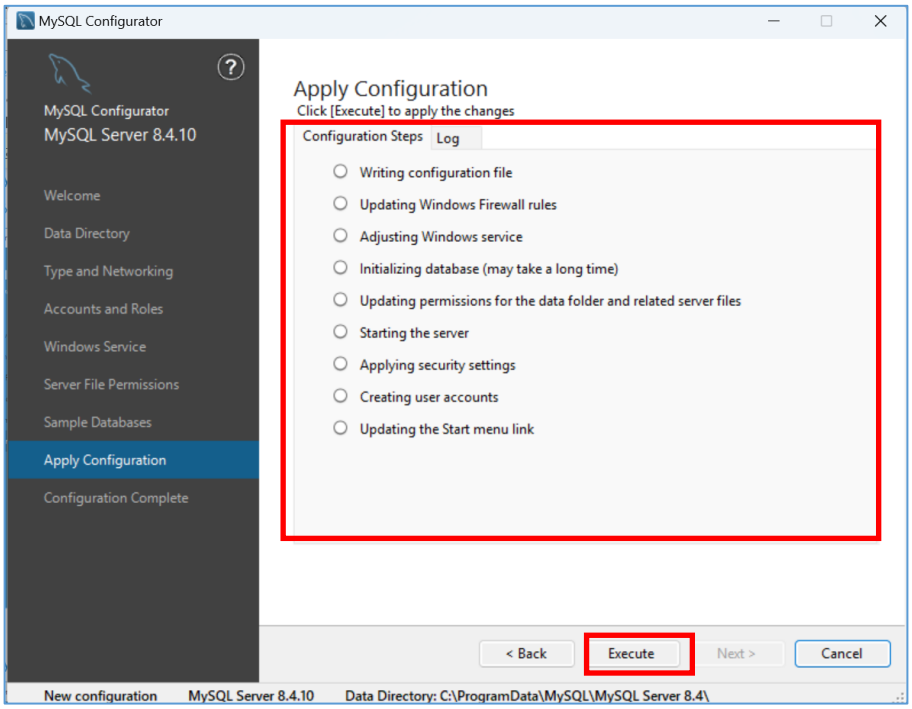
(11).Windows Service 画面は既定値のまま、[Next]をクリックします。



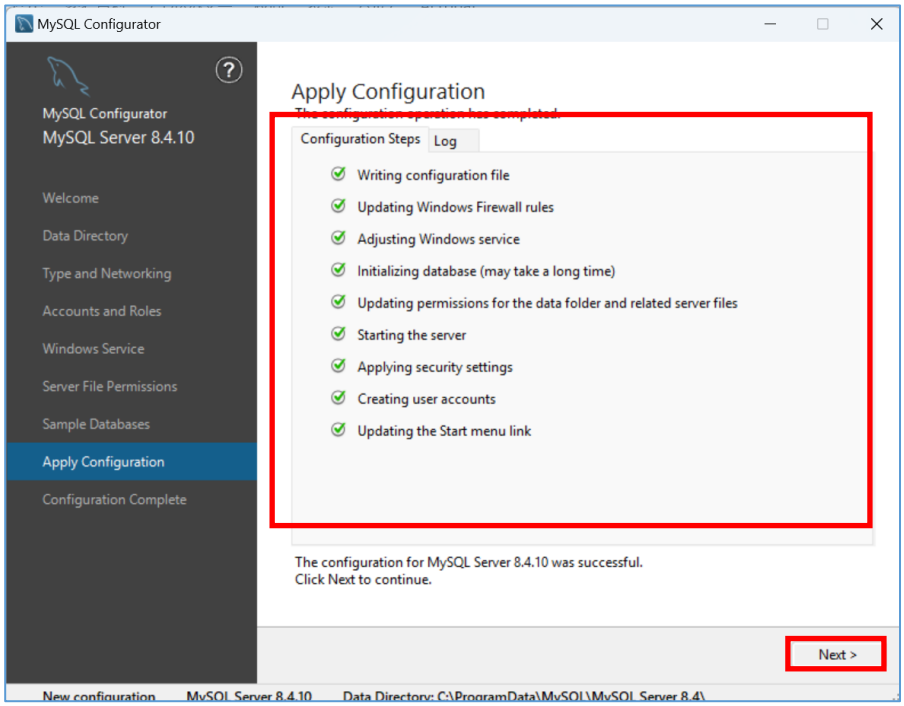
(12).Server File Permissions 画面で[Next]をクリックします。



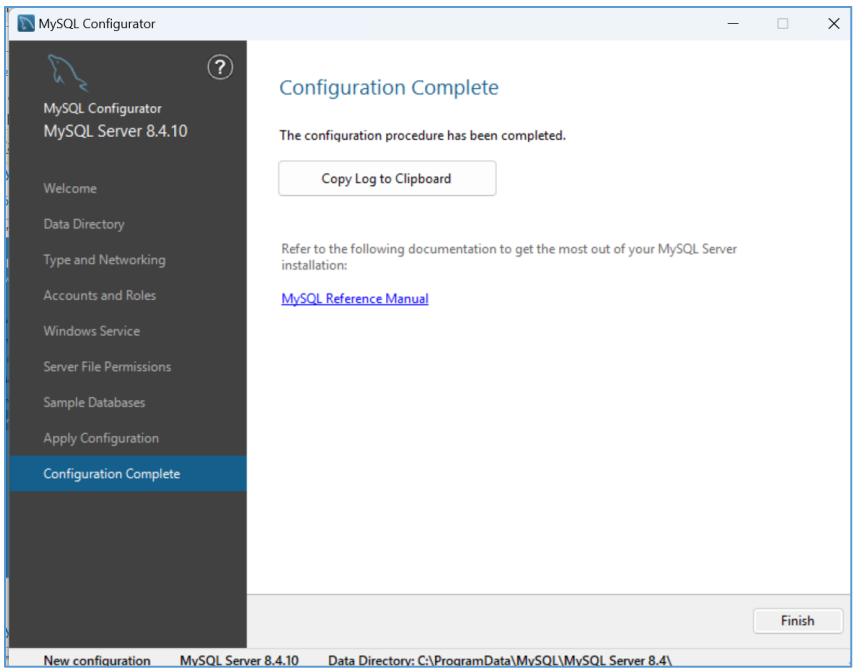
(13).Apply Configuration 画面で[Execute]をクリックします。 進捗が表示されるのでしばらく待ちます。



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

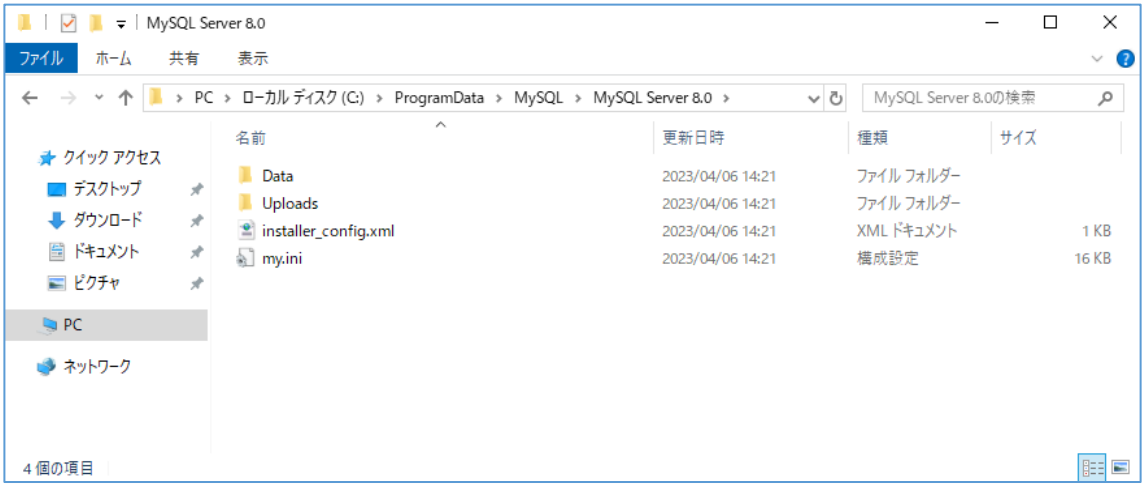


(15).Installation Complete 画面で[Finish]をクリックしインストーラーを終了します。



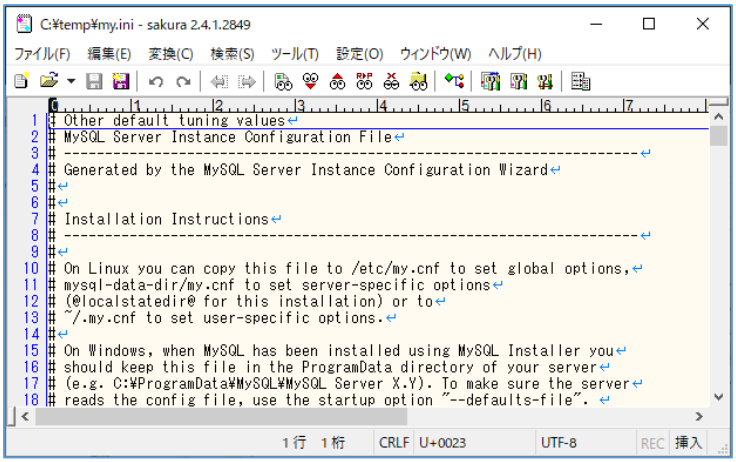
(16).C:¥ProgramData¥MySQL¥MySQL Server (バージョン番号)¥my.ini をテキストエディタで開きます。

※「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。



(17).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。



[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

open_files_limit=30000

innodb_redo_log_capacity=(※2)

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

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。

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。

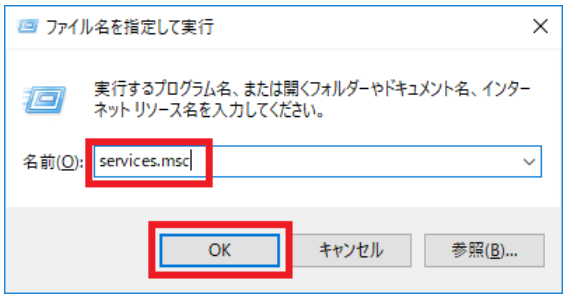
（※2）innodb_buffer_pool_size（※1）に指定した値を指定します。

設定値の詳細は以下をご確認ください。

https://support.eset.com/en/kb8597-how-to-create-dedicated-partition-on-mysql-server-for-eset-inspect-on-prem

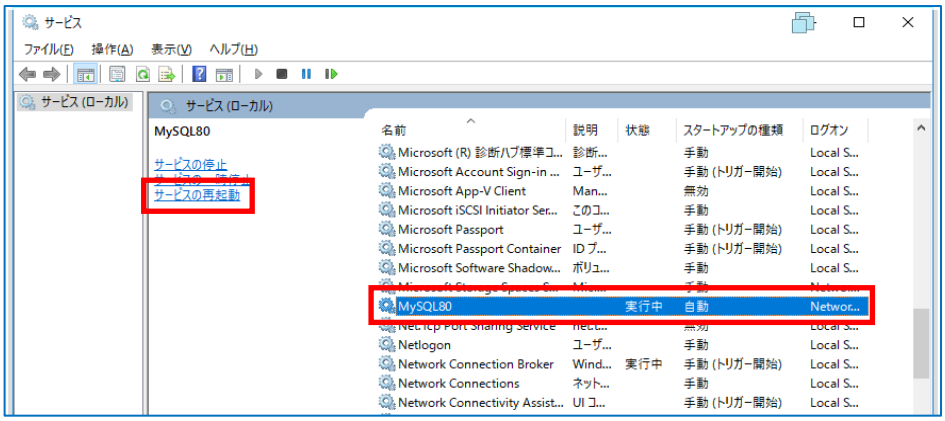
(18). my.ini を保存してテキストエディタを閉じます。

「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). MySQL84 or 9X を選択し、[サービスの再起動]をクリックします。

MySQL84 or 9X 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

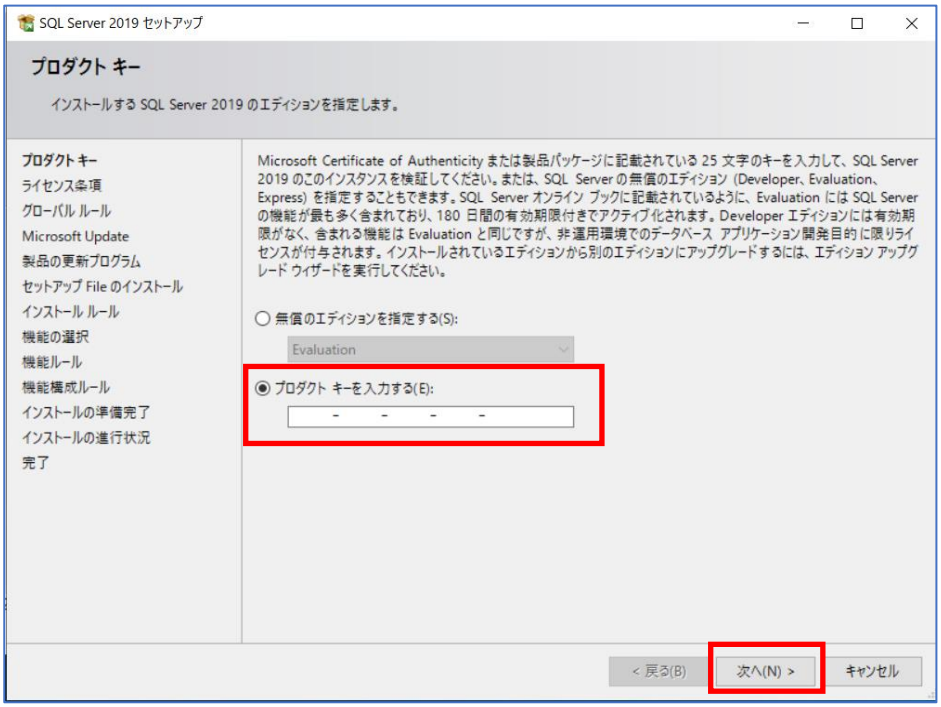
(2). 任意の場所に MSSQL Server のインストーラー”setup.exe”を配置し実行します。

(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。

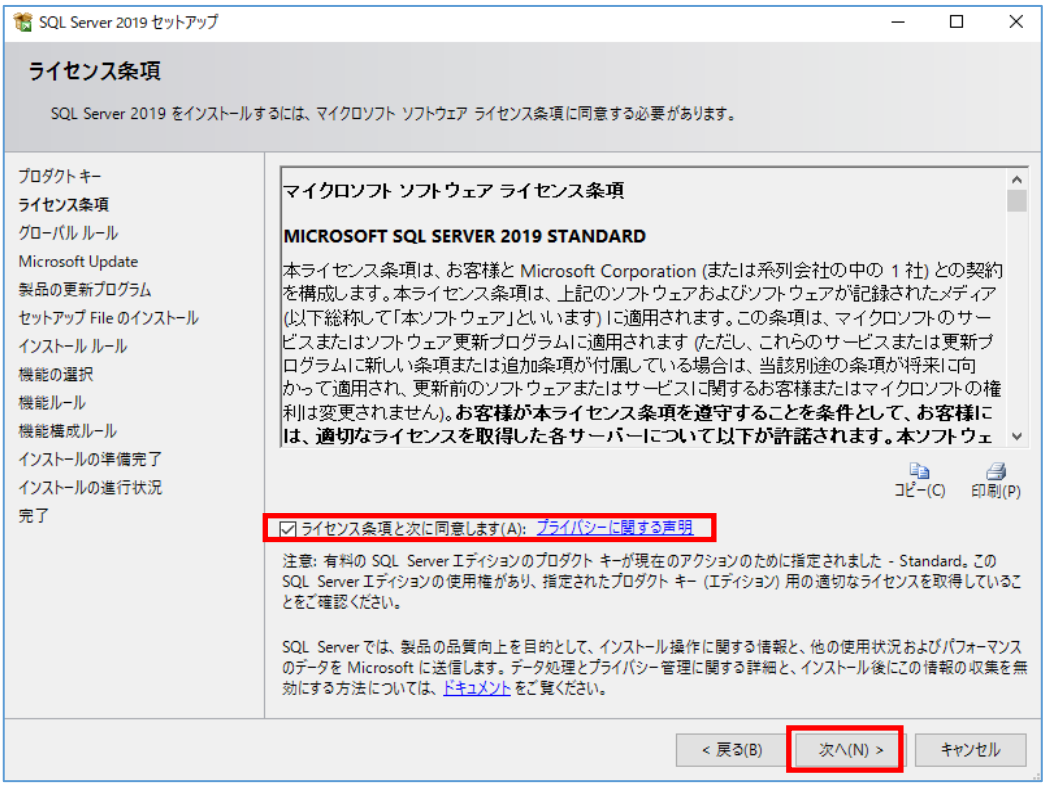
(4). 「SQL Server インストールセンター」画面が表示されたら、左メニューより「インストール」をクリックします。

(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。

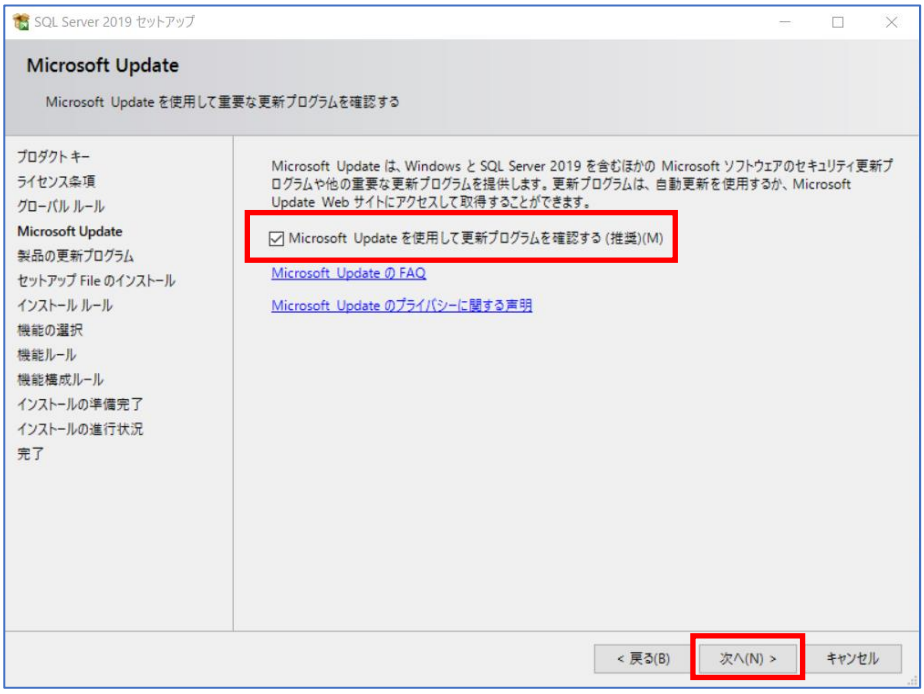
(7). 「プロダクトキーを入力する（E)」にチェックを入れ、プロダクトキーを入力して「次へ」クリックします。



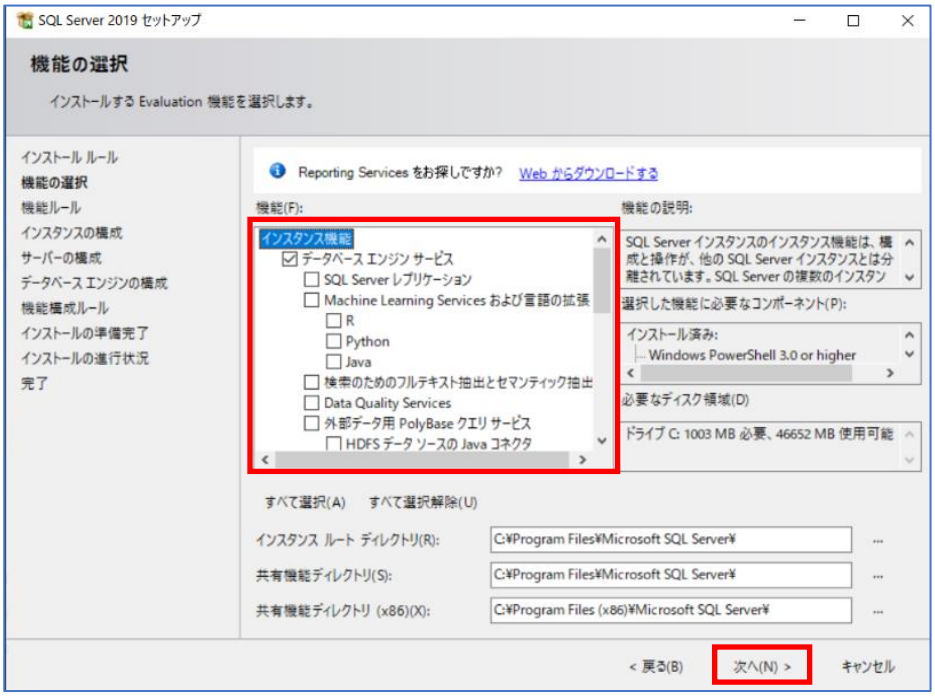
(8). ライセンス条項に同意します」にチェックを入れ、「次へ」をクリックします。



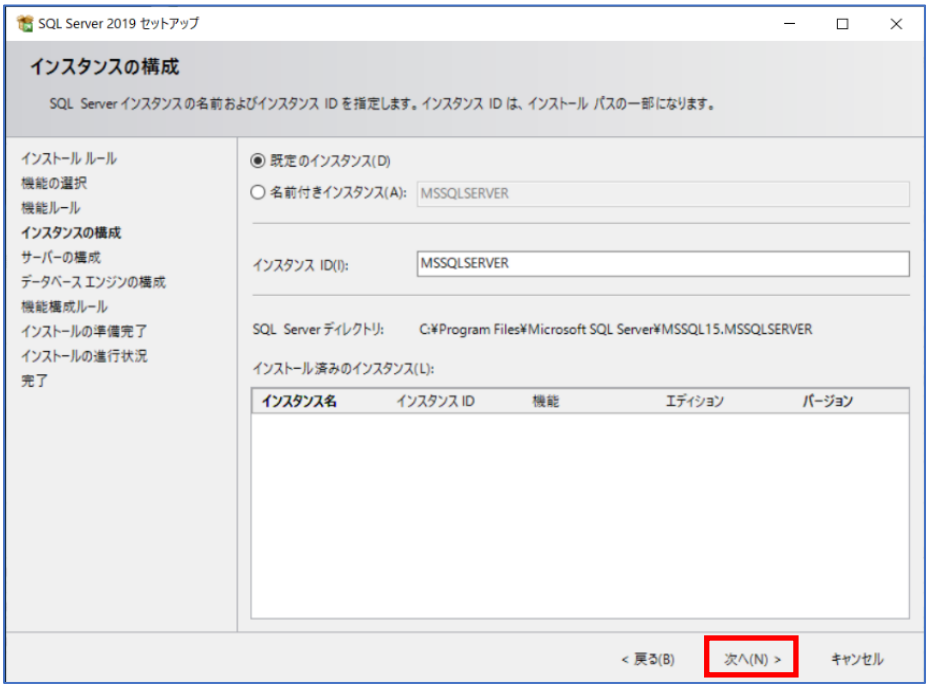
(9). 「Microsoft Update を利用して更新プログラムを確認する」にチェックを入れ、「次へ」をクリックします。



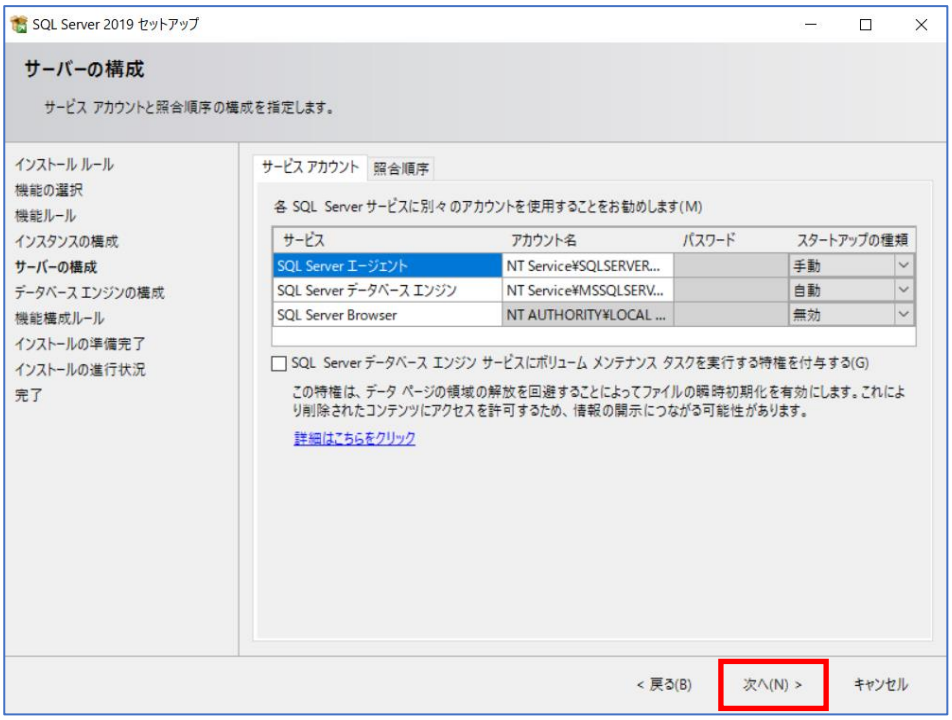
(10). 「機能選択」画面にて、「データベースエンジンサービス」と「SQL クライアント接続 SDK」にチェックを入れ、「次へ」をクリックします。



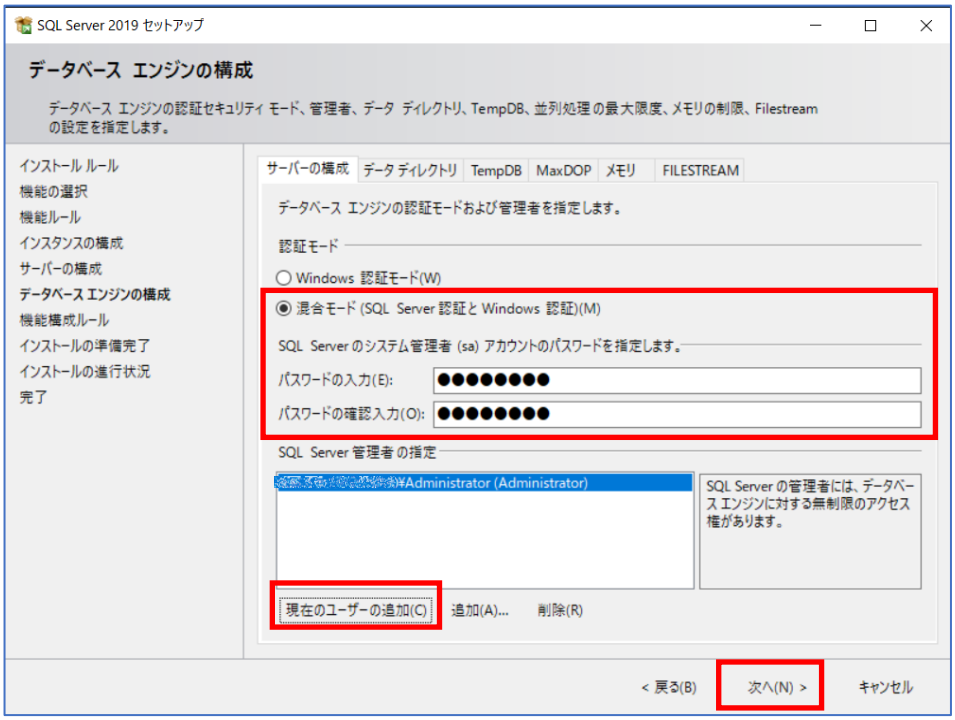
(11). 「インスタンスの構成」画面にて既定値のまま「次へ」をクリックします。



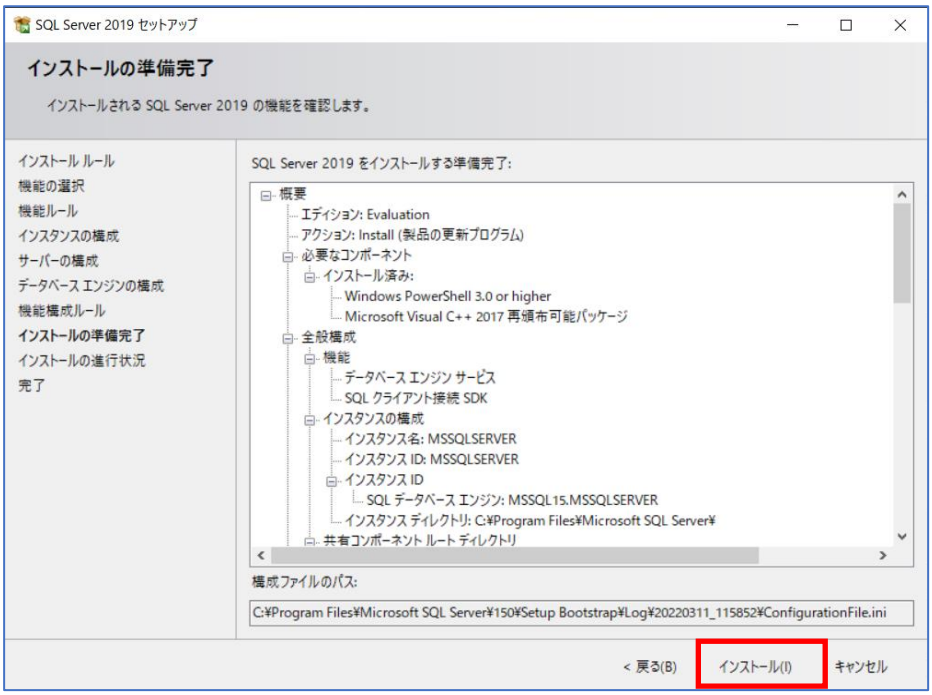
(12). 「サーバーの構成」画面にて既定値のまま「次へ」をクリックします。



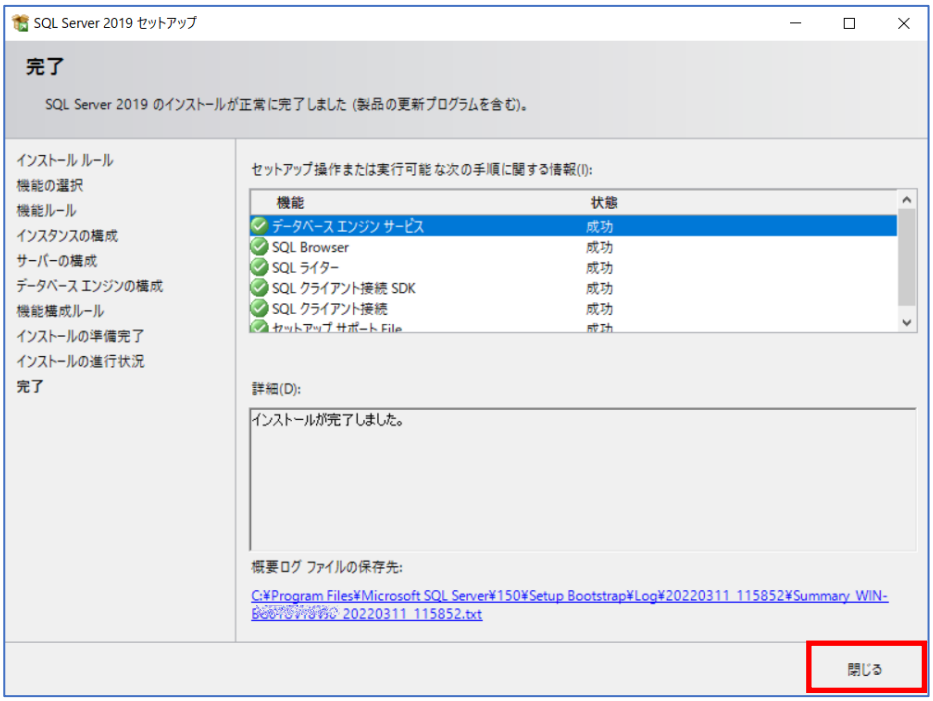
(13). 「データベースエンジンの構成」画面にて、「混合モード」を選択、sa パスワードを設定、「現在のユーザーを追加」をクリックし、「次へ」をクリックします。



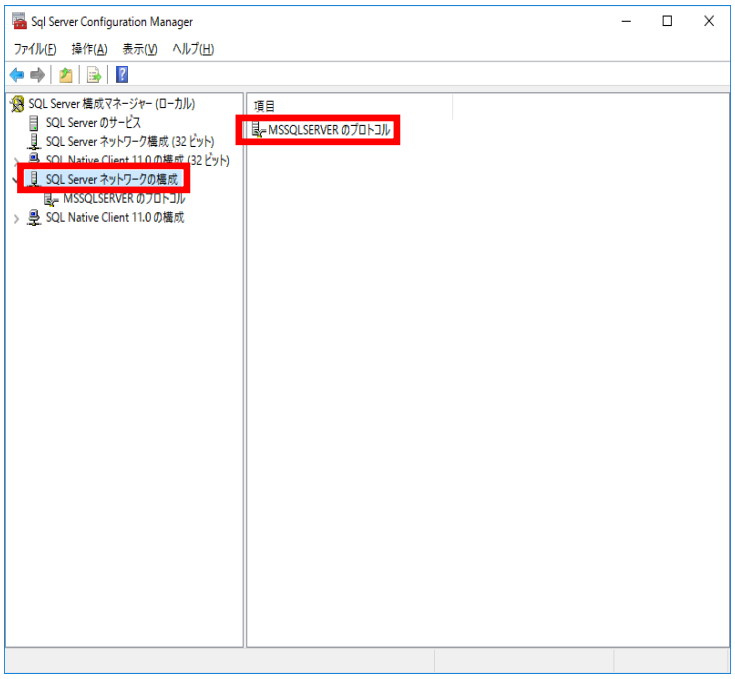
(14). 「インストールの準備完了」画面にて、「インストール」をクリックします。



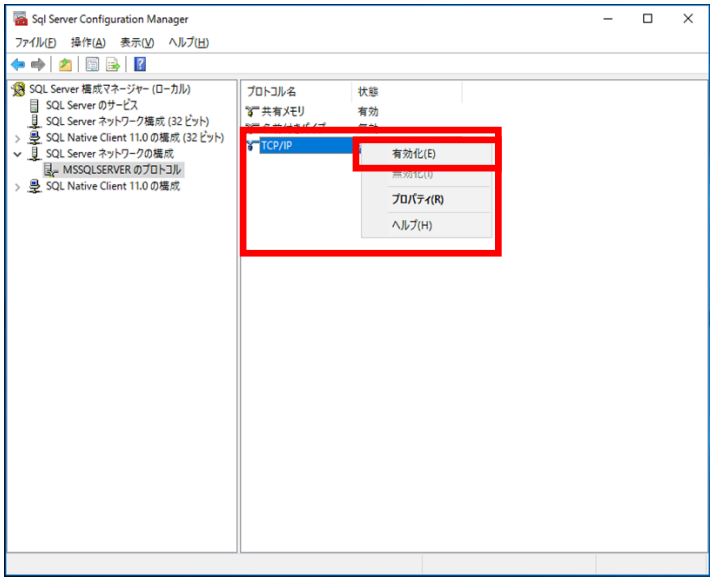
(15). 「完了」画面にて、状態が全て成功であることを確認して「閉じる」クリックします。



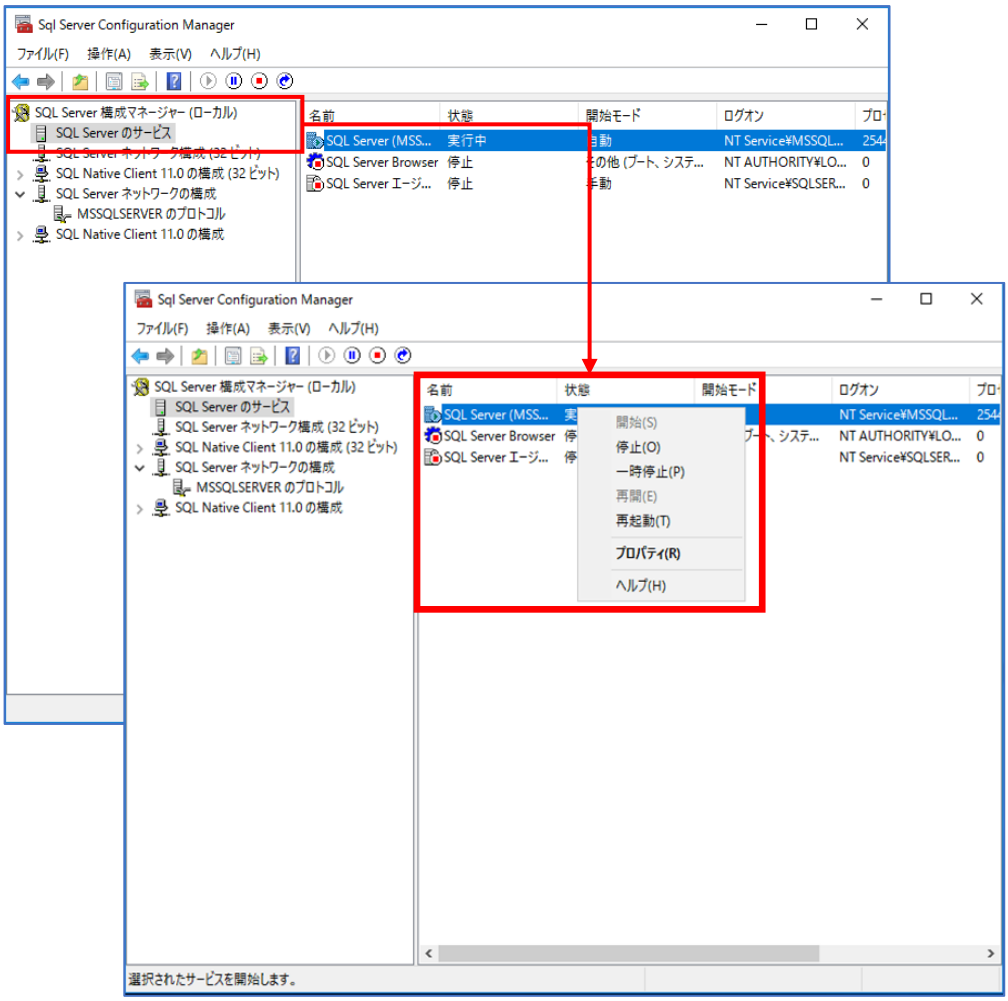
(16). スタートメニューより、「SQL Server 2019 構成マネージャー※」を開きます。
左メニューの「SQL Sever ネットワーク構成」->「MSSQLSERVER のプロトコル」を
クリックします。
※アプリケーション名はインストールしたデータベースの情報に読み替えてください。



(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。



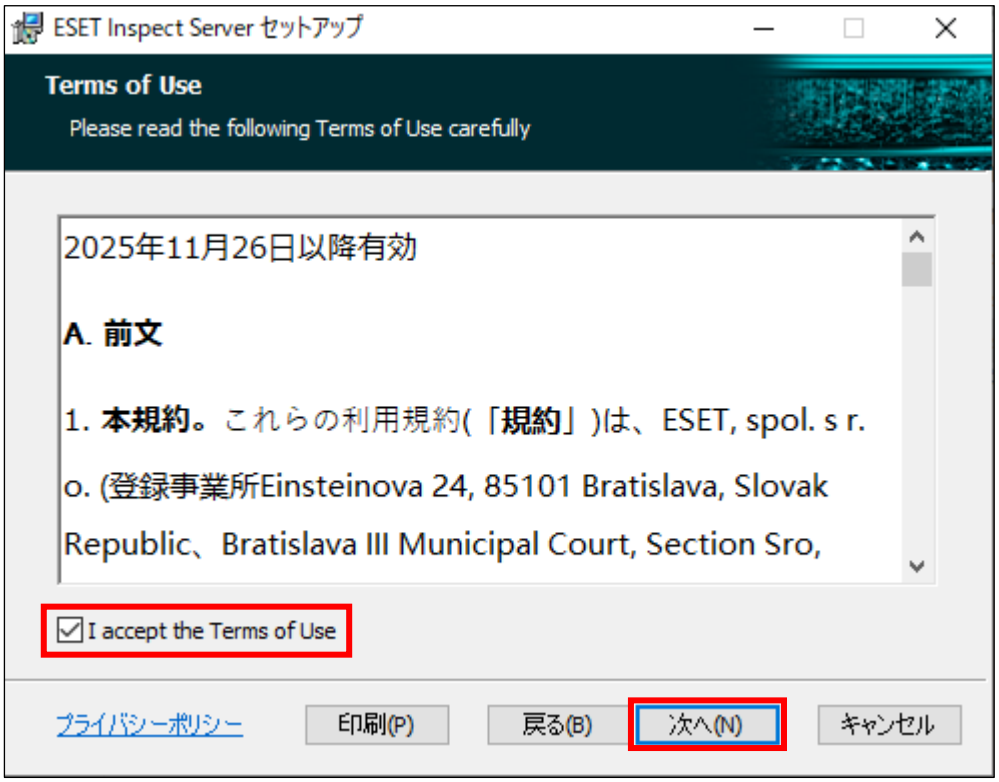
6. EI Server のインストール【EI on-prem 側作業】

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。

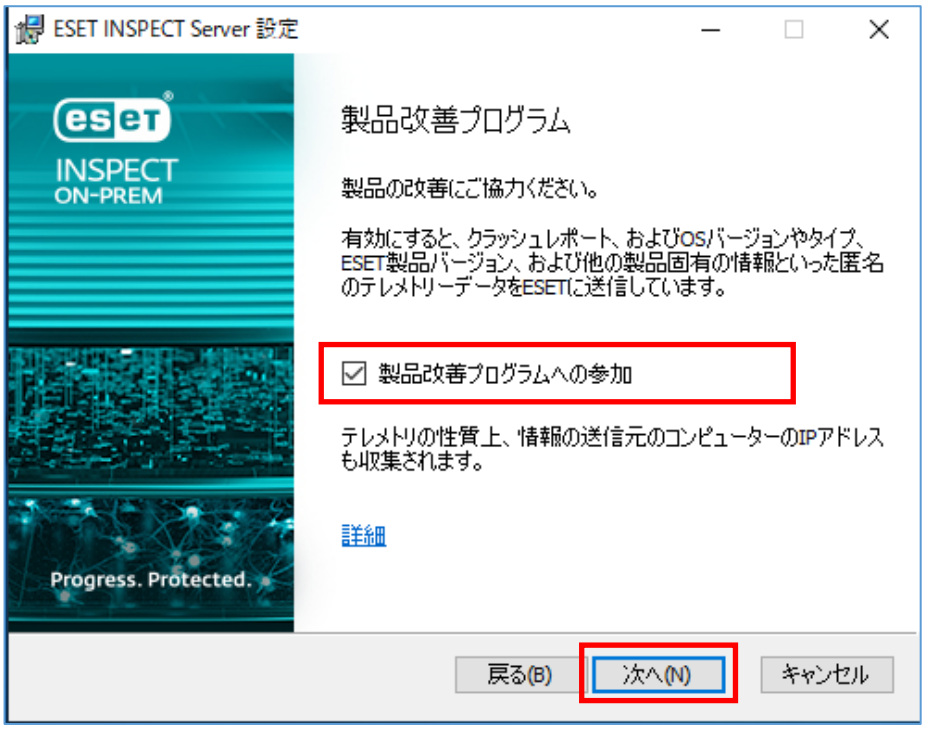
(2). EI Server のインストーラー(ei_server_nt64.msi)を使用し、インストールを開始します。

(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、[I accept the Terms of Use]にチェックを入れます。

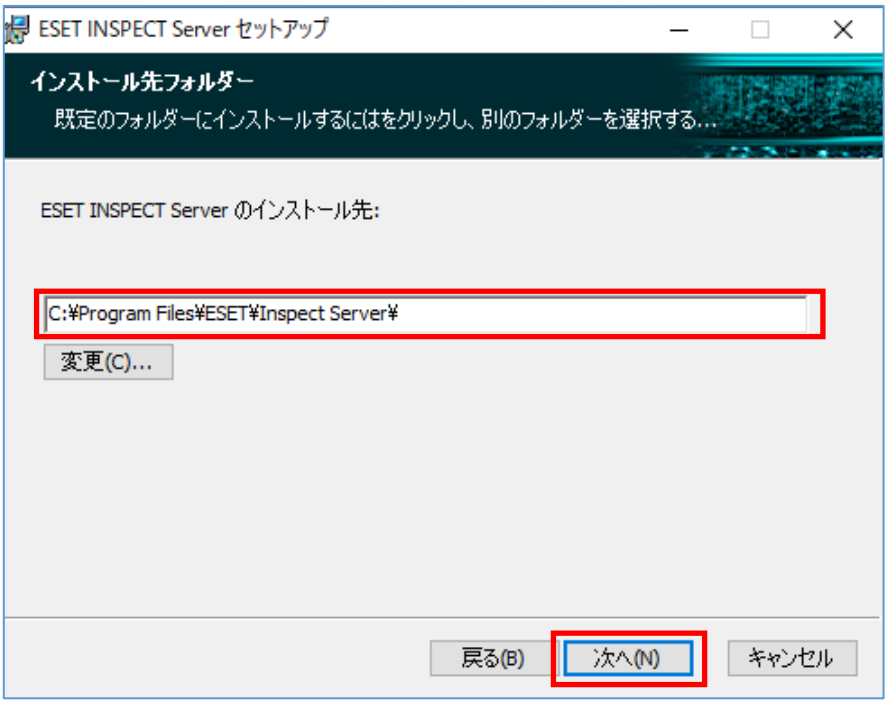


(4). 製品改善プログラム画面の[製品改善プログラムへの参加]のチェックは任意です。

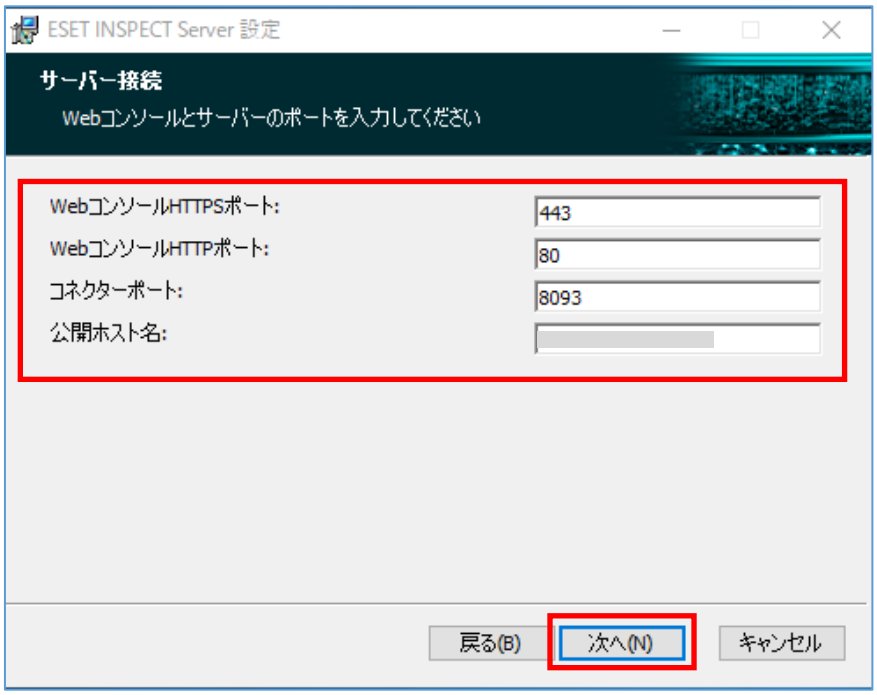
※ EI on-prem の機能は、本項目にチェックを入れなくても利用できます。



(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先を指定します。

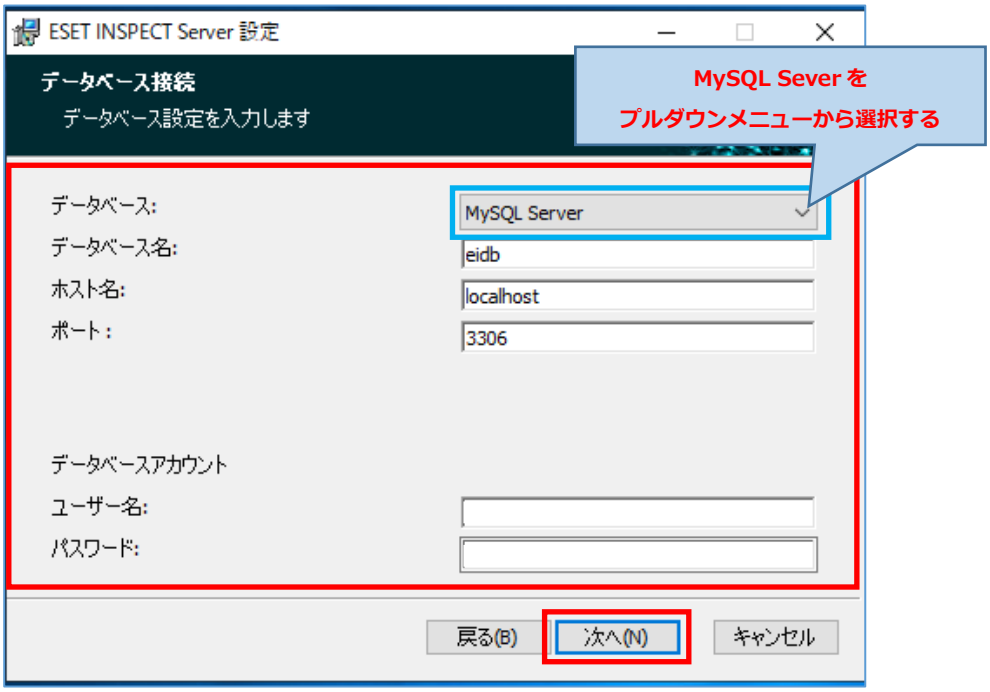


(6). サーバー接続画面で、Web Console および Agent の接続ポート情報を入力します。



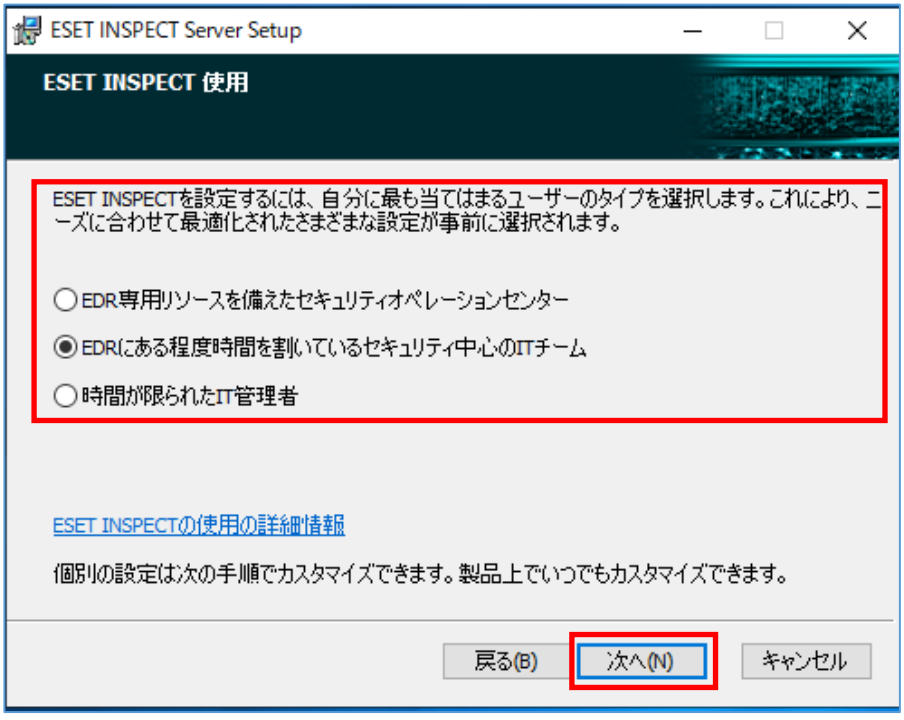
(7). データベース接続画面で、データベースの接続情報を入力します。

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。

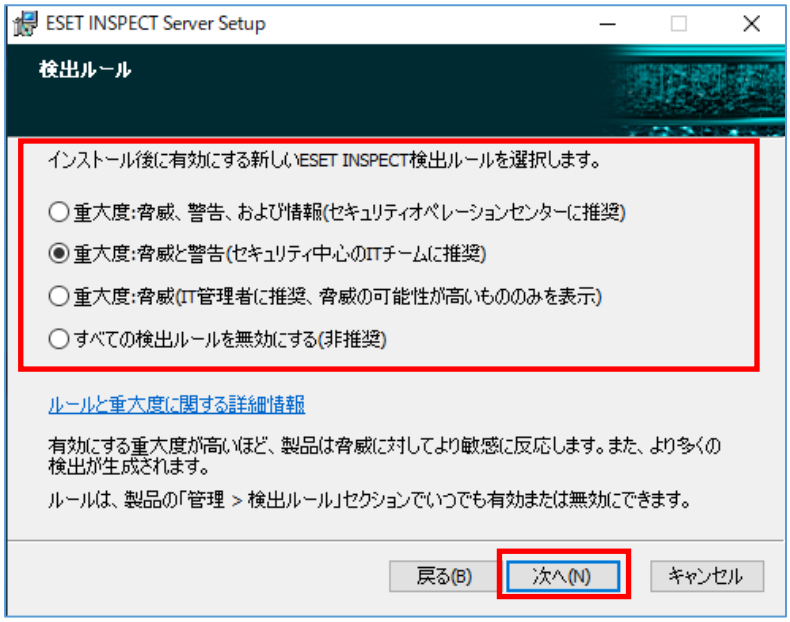


② 以下は MSSQL を利用した場合の設定値となります。データベースアカウントのユーザー名は項番 5-2(13)で作成したユーザー情報を入力します。

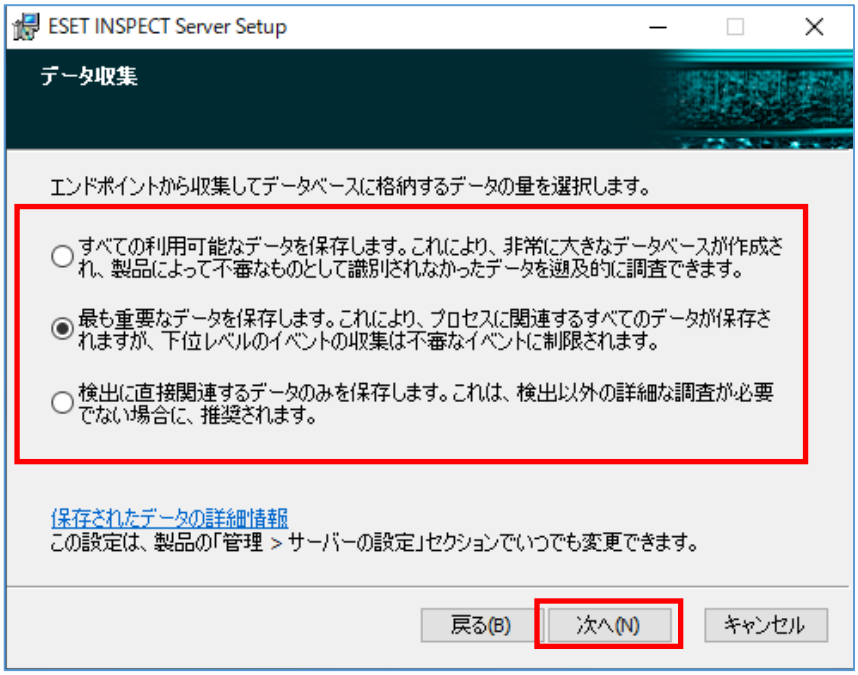
(8). ESET Inspect 使用画面で、プロファイルベースの設定を行います。
本手順で選択した項目により、後続のデフォルトの選択値が変わります。



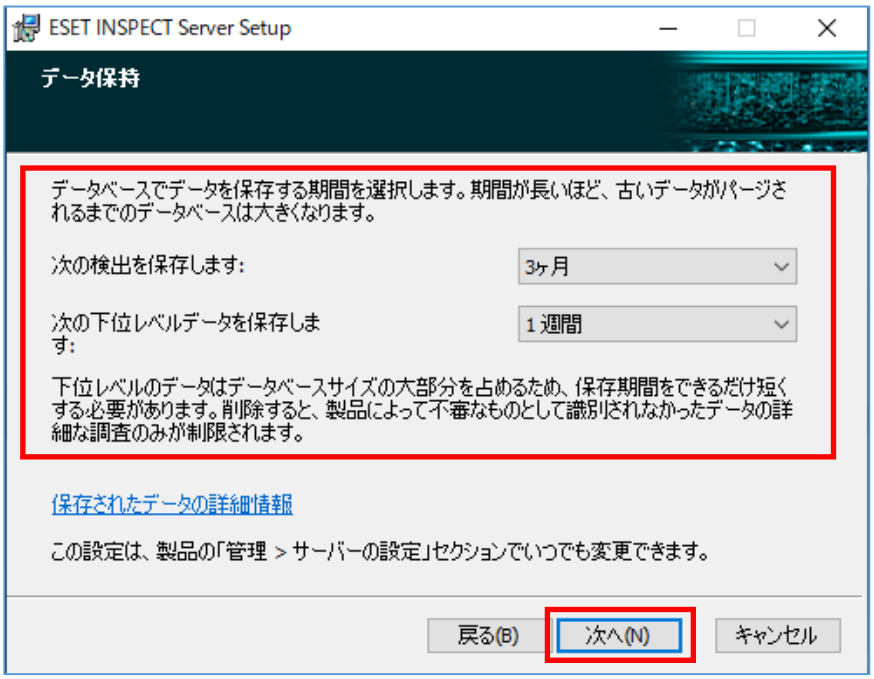
(9). 検出ルール画面で、４つの重大度レベルに基づいて有効にするルールを選択します。
本手順で選択した内容により、EI インストール後に既定で有効になるルールが変わります。



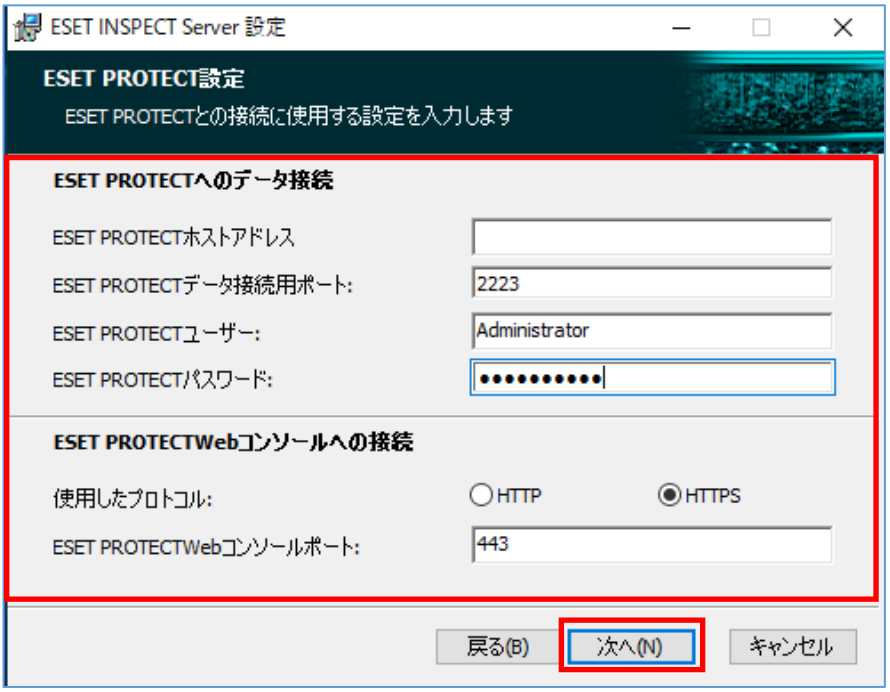
(10). データ収集画面では、EI でのデータ収集オプションを設定します。
本手順で選択した内容により、データがデータベースに保存される方法を設定します。
EI on-prem で表示されるプロセスツリーの情報量に影響します。



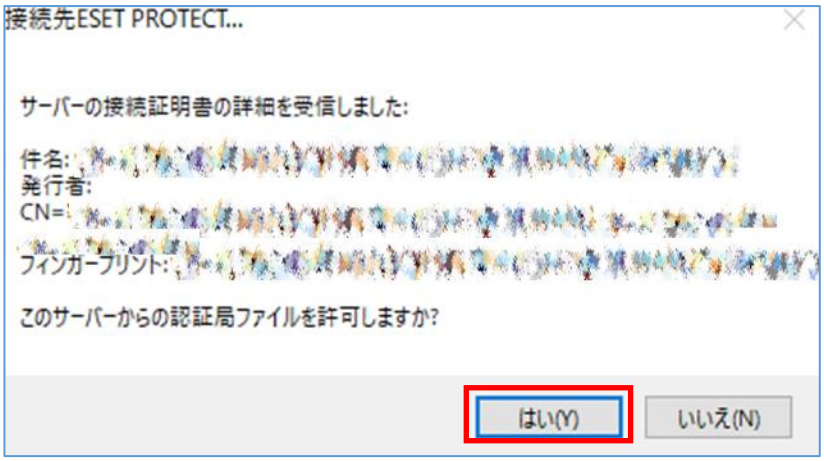
(11). データ保持画面では、EI on-prem でのデータの保持期間を選択します。
本手順では、検出データや下位レベルデータの保持期間を設定します。
※本設定は EI インストール後にも設定変更が可能です。



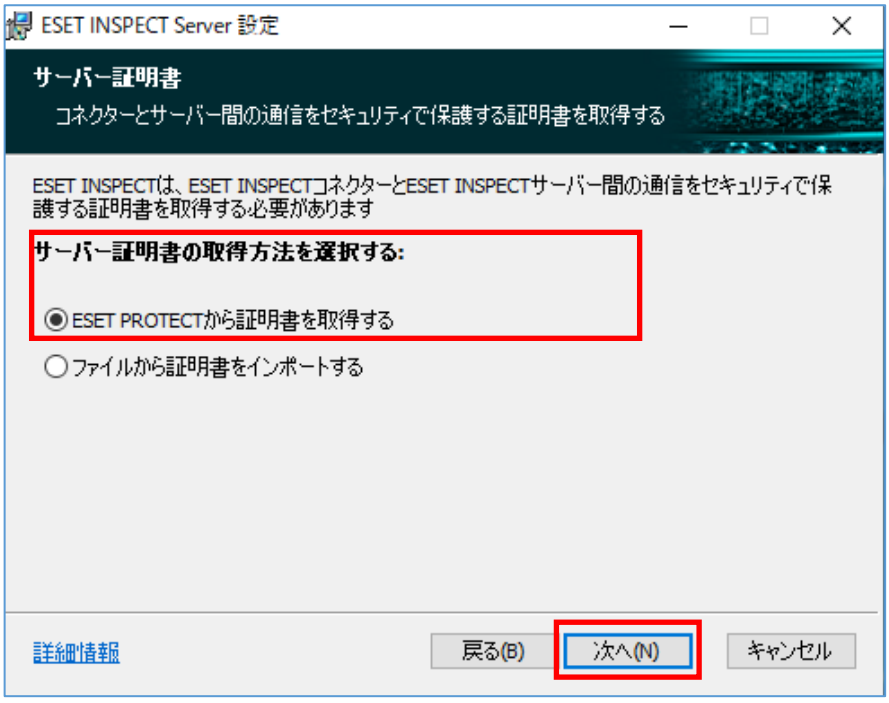
(12). ESET PROTECT 設定画面で、EP on-prem の接続情報を入力します。



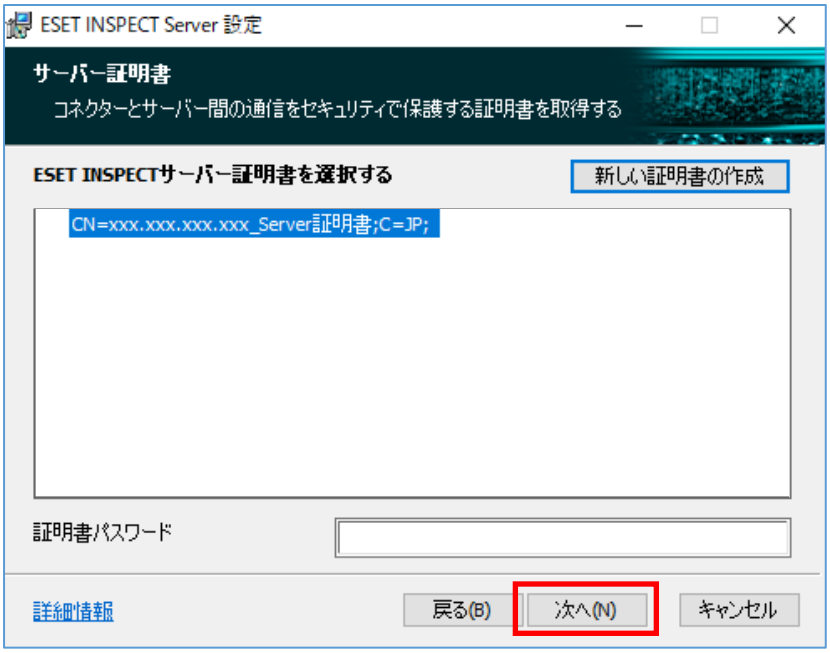
(13). 接続先 ESET PROTECT ダイアログが表示されますので、［はい］を選択します。



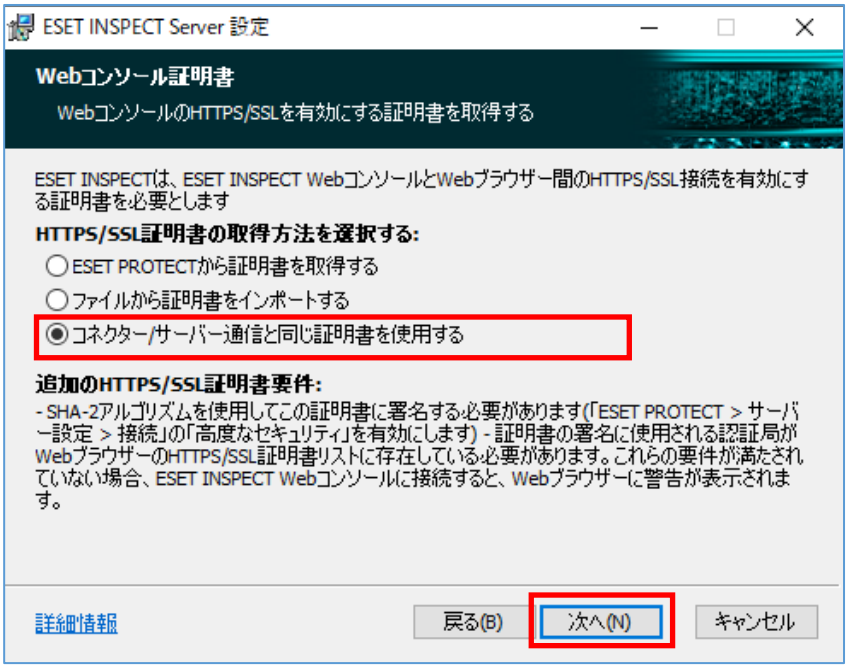
(14). サーバー証明書画面で、EI Server と EI Connector 間の接続に使用する証明書の取得方法を選択します。ここでは既定の［ESET PROTECT から証明書を取得する］を選択し、[次へ]をクリックします。



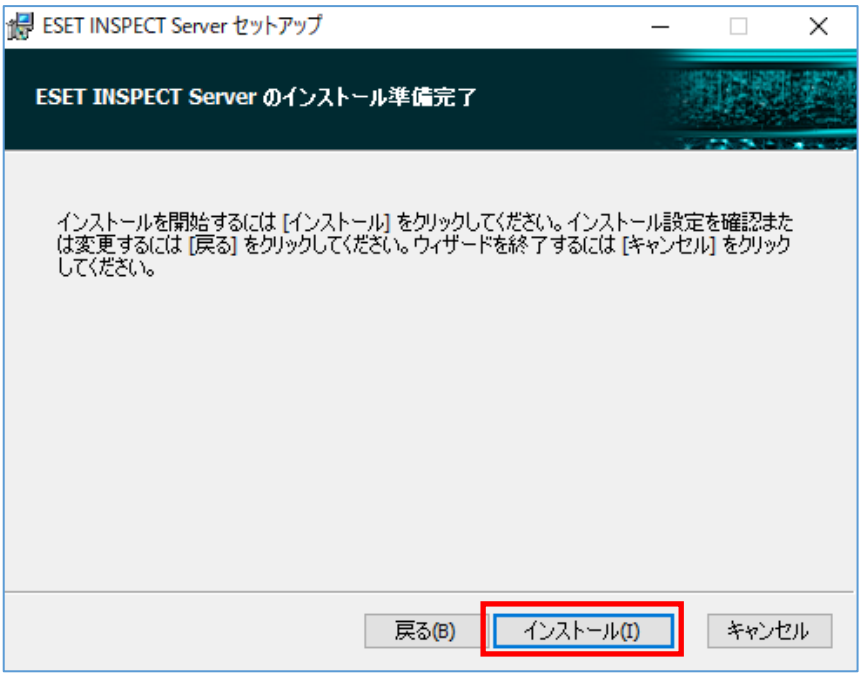
(15). サーバー証明書画面で、事前準備で作成した証明書(項番 4 4.2 で作成)を選択します。証明書パスワードは証明書作成時に設定したパスワードを入力します。（空にした場合、入力不要）



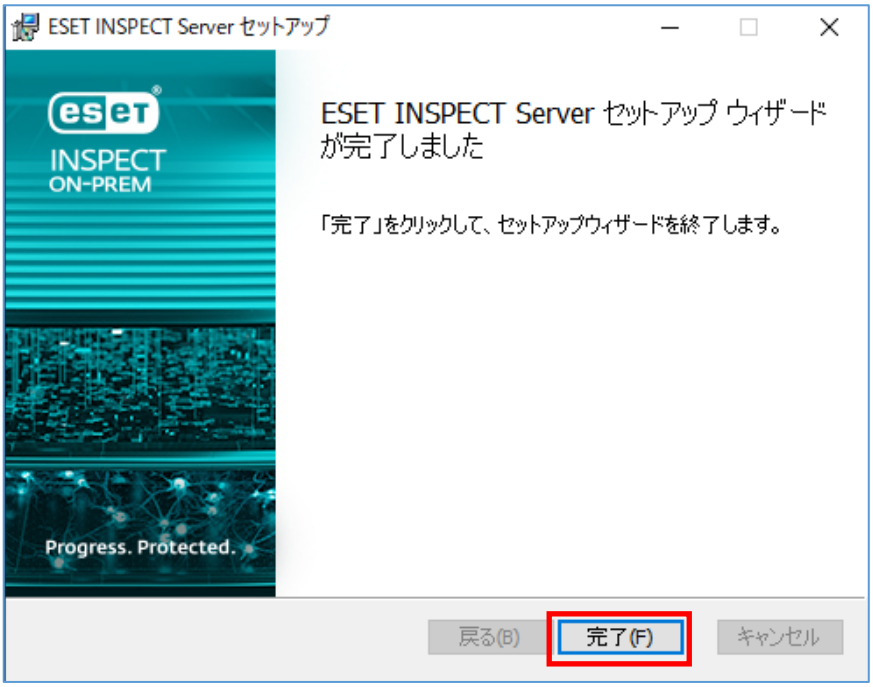
(16). Web コンソール証明書画面で、EI Web Console で使用する証明書を選択します。ここでは既定の「コネクター/サーバー通信と同じ証明書を使用する」を選択し、[次へ]をクリックします。



(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。



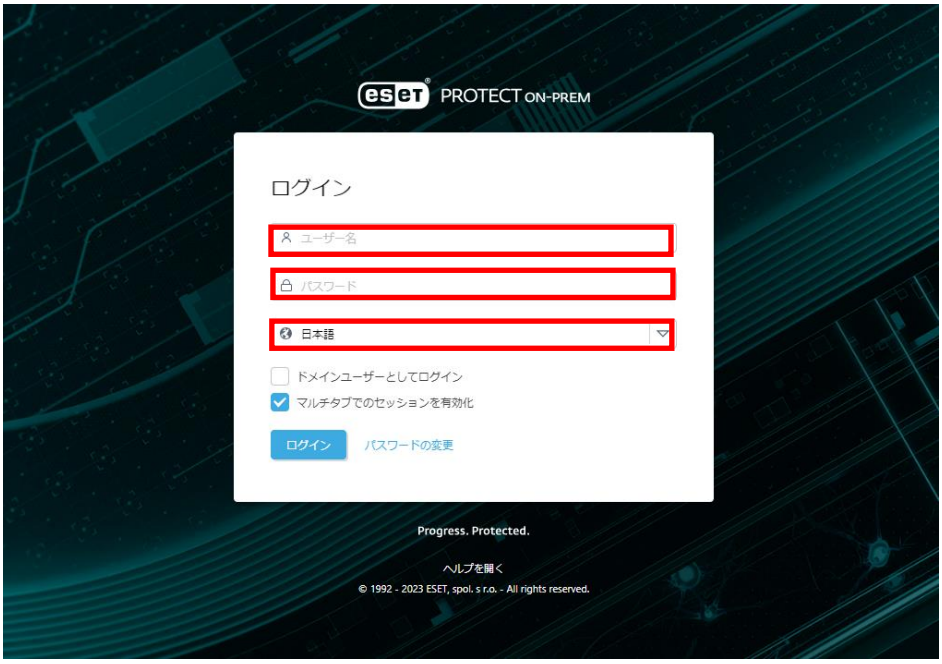
7. EI Connector の展開【EP on-prem 側作業】

7.1 EI on-prem ライセンスの登録

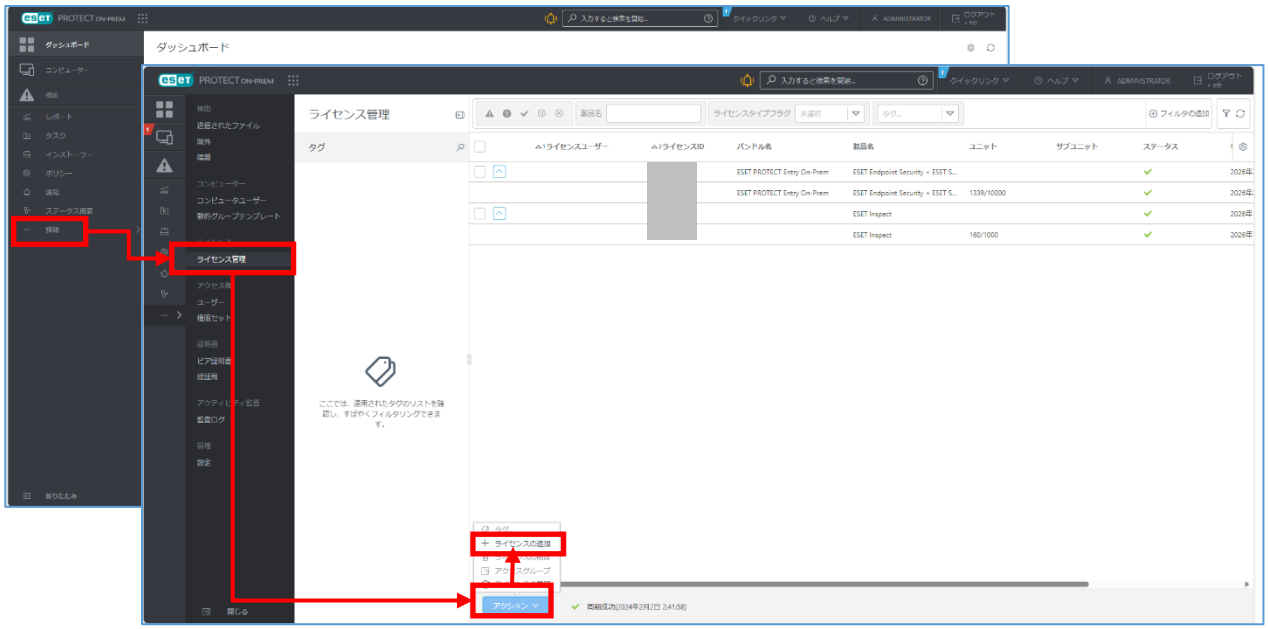
※本手順は既に EI on-prem が利用可能なライセンスを EP on-prem に登録している場合は実施不要です。

(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。

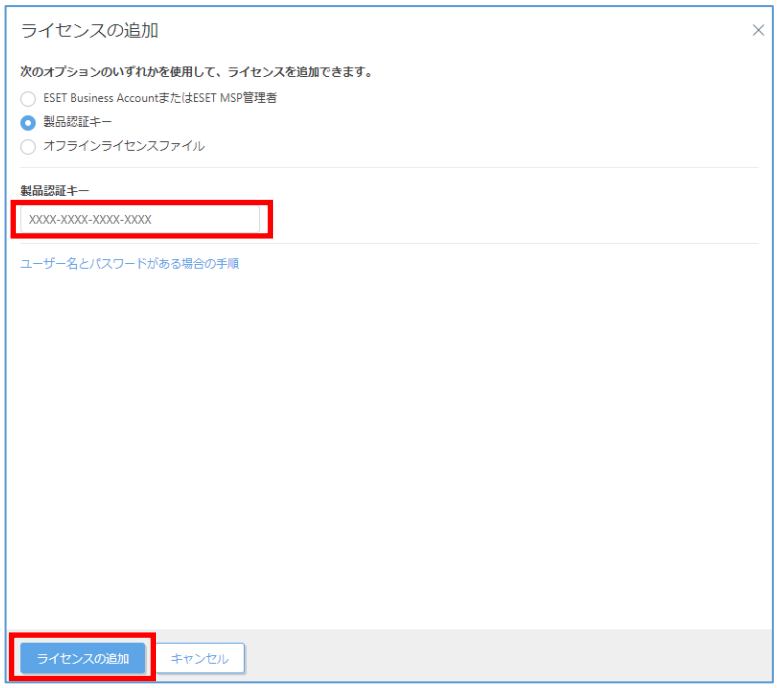
「日本語」を選択して、「EP ログインユーザー名」・「EP ログインパスワード」を入力し、「ログイン」をクリックします。



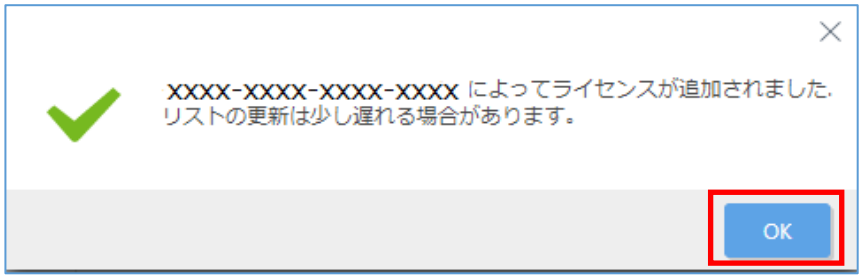
(2). [詳細]->[ライセンス管理]->[アクション]->[ライセンスの追加]をクリックします。



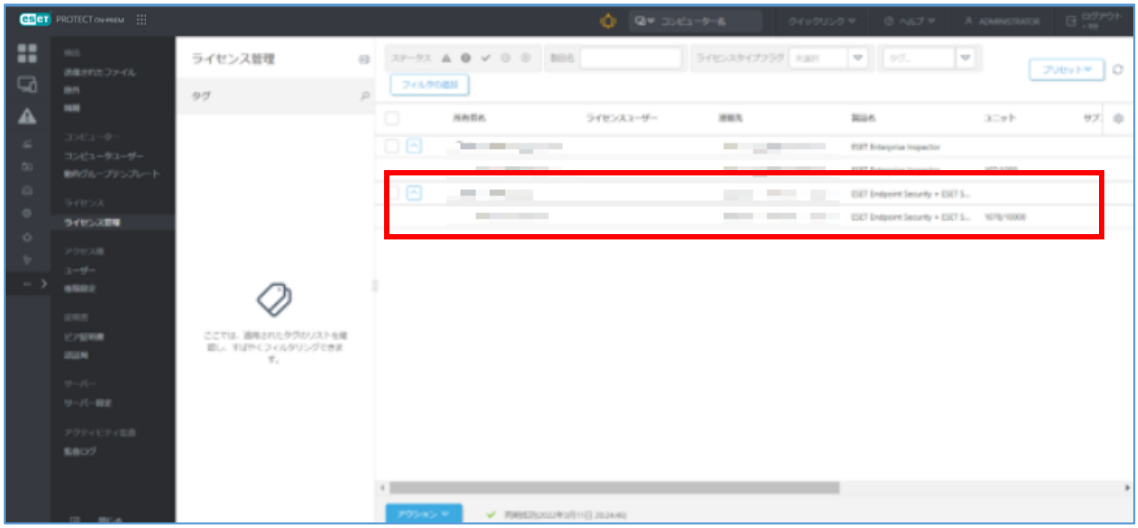
(3). ライセンス追加画面で[製品認証キー]を選択し、EI on-prem 用の製品認証キーを入力します。[ライセンスの追加]をクリックします。



(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。



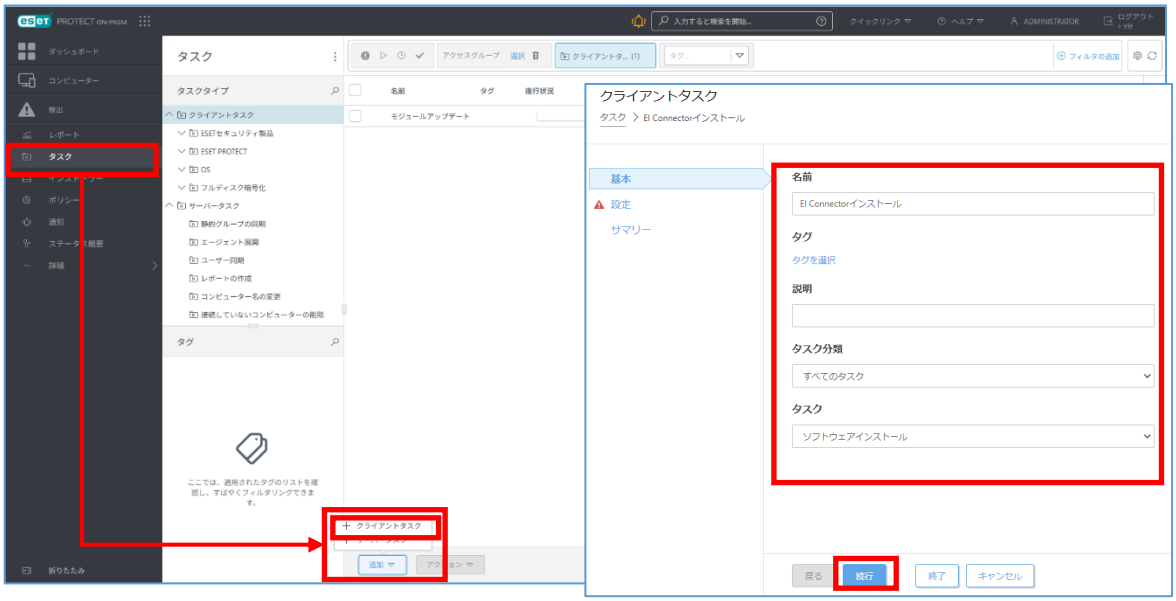
(5). ライセンス管理画面に追加したライセンス情報が表示されることを確認します。



7.2 (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]->[追加]-> [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

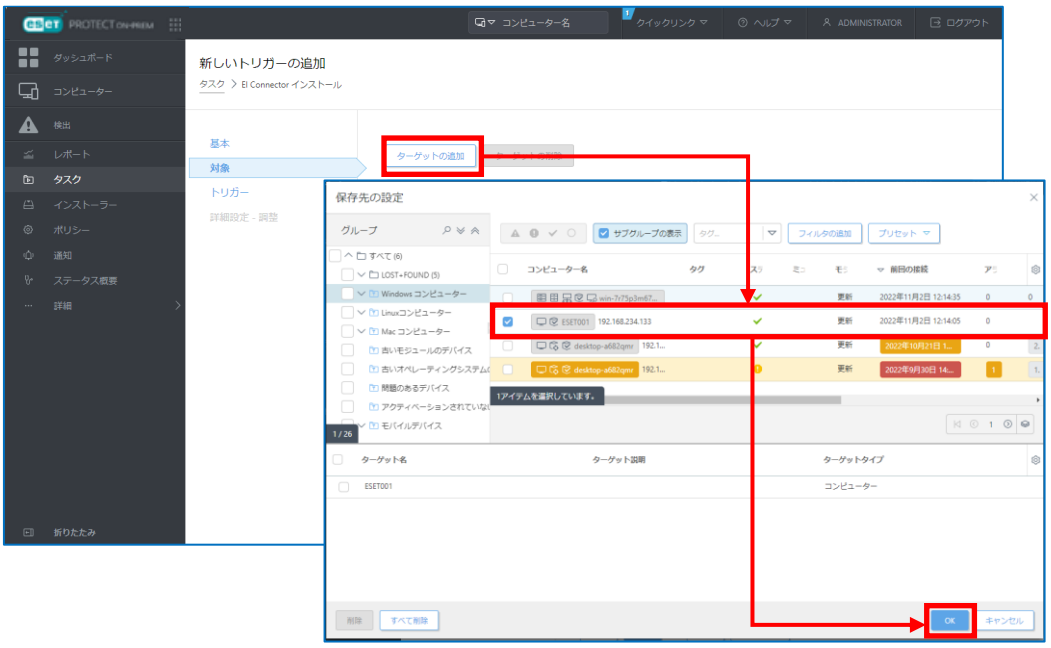
■[設定]セクション

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]を選択します
オペレーティングシステムを選択	利用 OS を選択します
リポジトリからパッケージを選択	<製品を選択>：ESET Inspector Connector ※最新バージョンが選択されます
ESET ライセンス	登録した EI on-prem ライセンスを選択します
エンドユーザーライセンス契約への同意	チェックを入れます

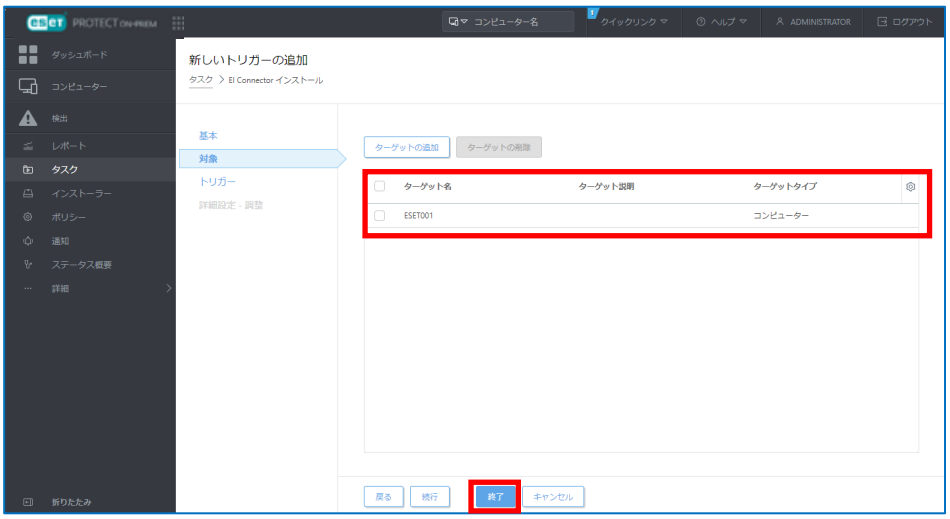
インストールパラメータ	P_HOSTNAME="EI Server の IP アドレス" P_IS_SERVER_ASSISTED=1
必要なときに自動的に再起動	チェックなし

(2). [トリガーの作成]をクリックします。

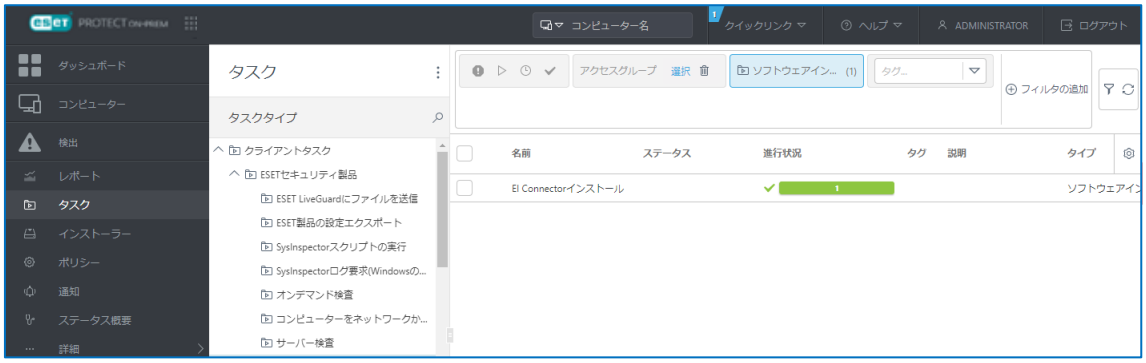
(3). [ターゲット]セクションで、[コンピュータの追加]または[グループの追加]をクリックし、EI Connector の展開対象を選択後、[OK]をクリックします。



(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。

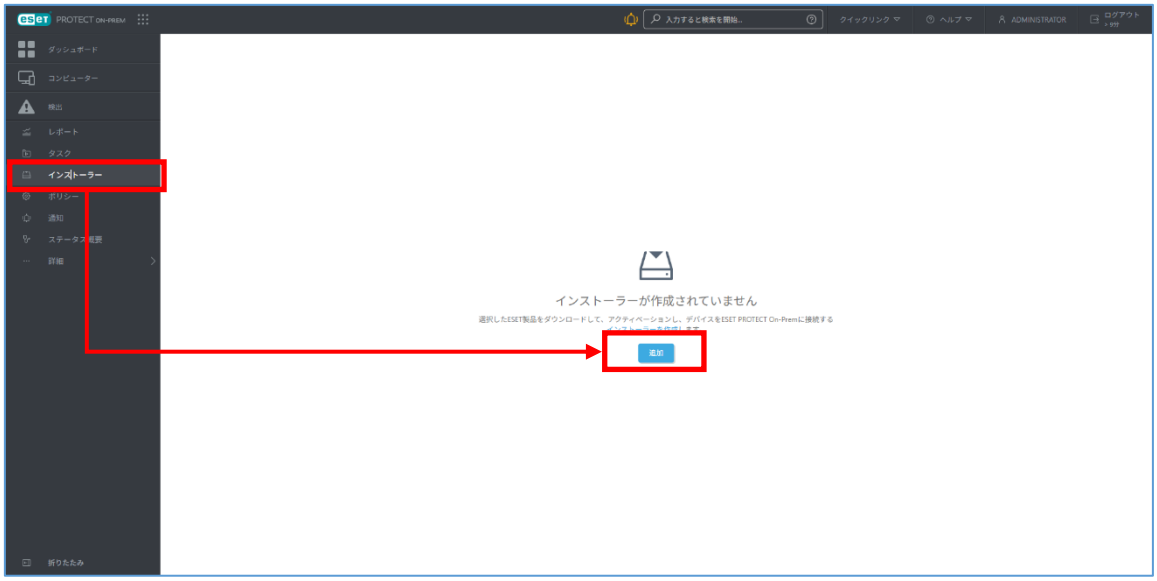


7.2(ii) オールインワンインストーラーによる EI Connector の展開

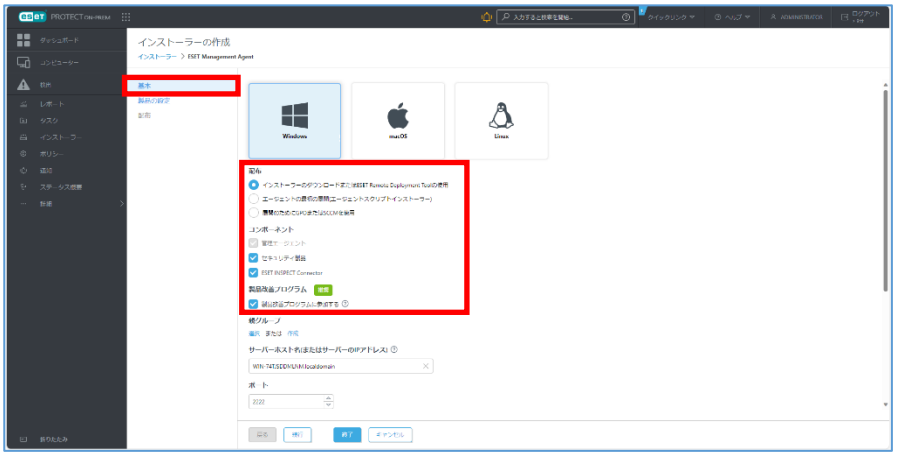
EP on-prem でクライアントを管理していない場合は、EP on-prem で作成したオールインワンインストーラーを使用して、EM Agent とクライアント用プログラムと同時に EI Connector のインストールが可能です。

※ 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]->[追加]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。



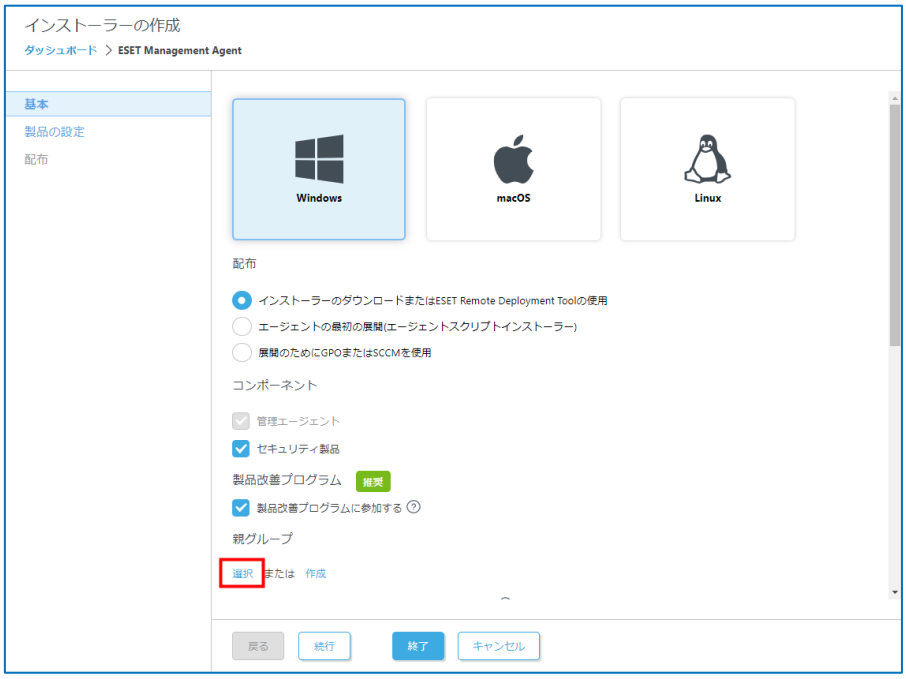
セキュリティ製品	チェックを入れます
ESET Inspect Connector	チェックを入れます

※「管理エージェント」には規定でチェックが入っています。

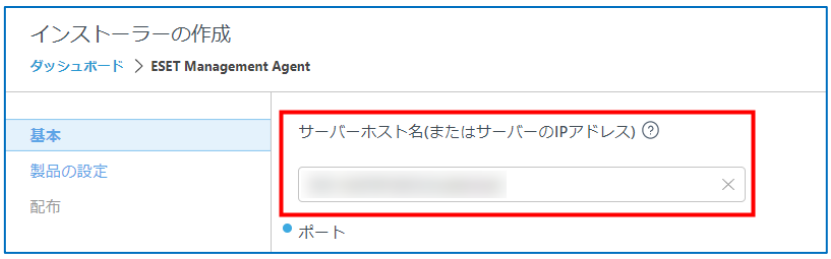
(3).インストールするクライアント端末をすでに作成されたグループに登録する場合は、［親グループ］の［選択］をクリックしてグループを指定します。

※ 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。

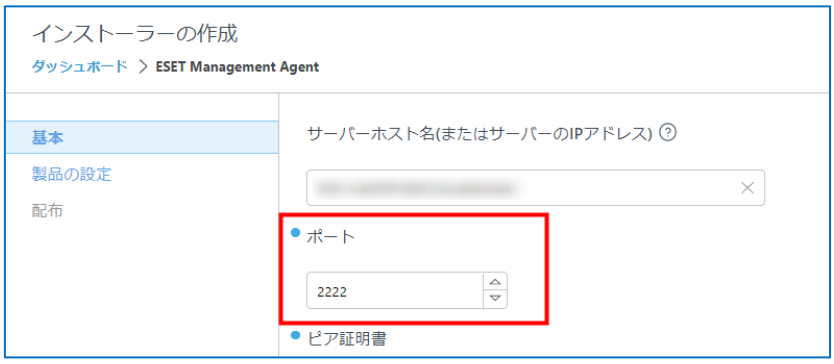
※ 新しくグループを作成したい場合は、［作成］をクリックして作成します。



(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。

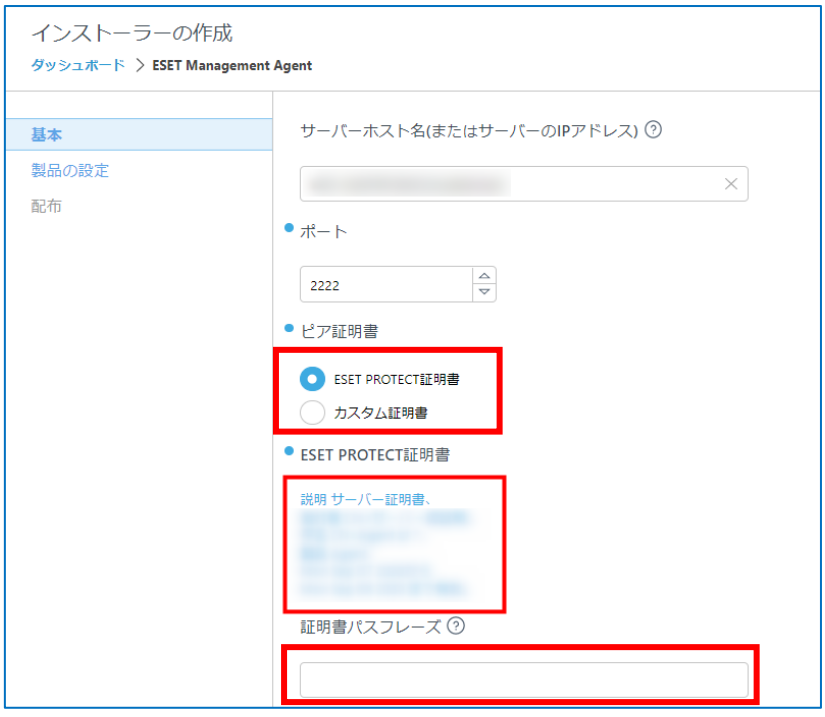


(5).ポート番号「2222」が入力されていることを確認します。

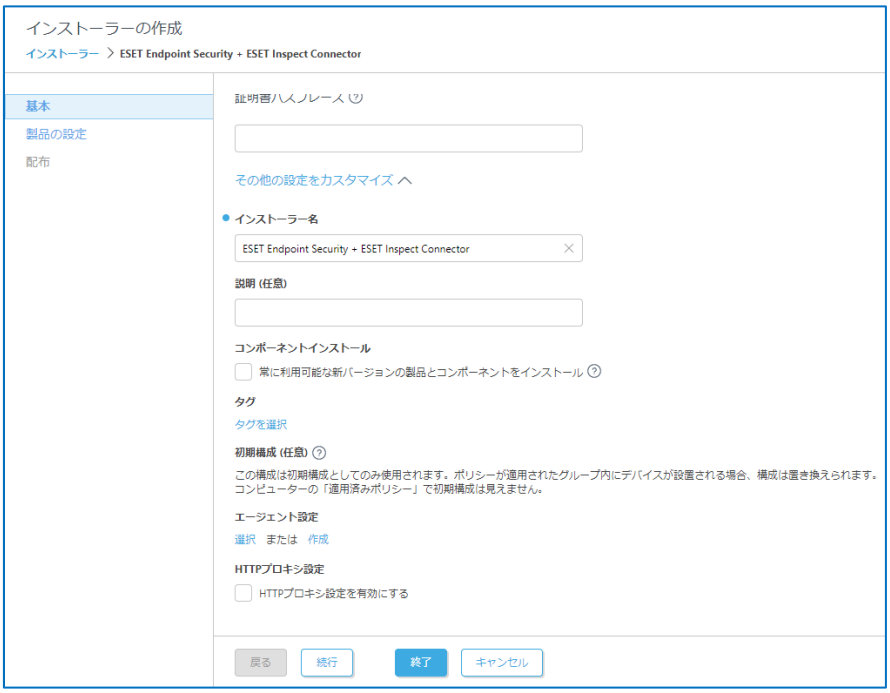


(6).［ピア証明書］の［ESET PROTECT 証明書］を選択し、証明書が正しいことを確認します。

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。



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



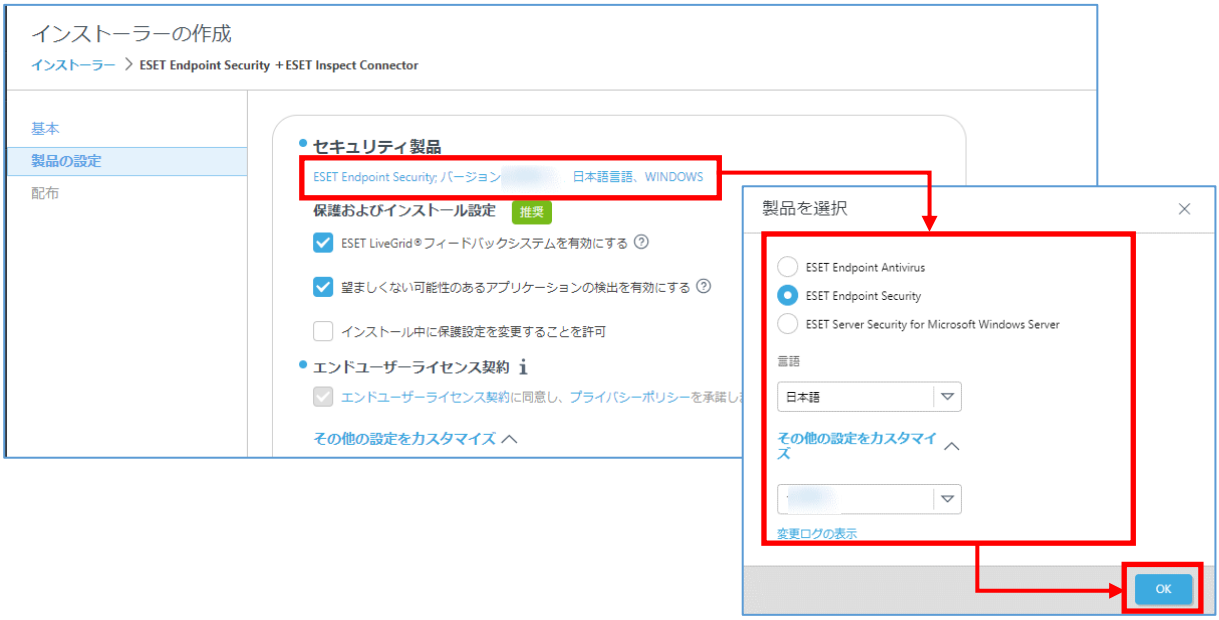
インストーラー名	任意の名前を入力します。
コンポーネントインストール	チェックを入れるとリポジトリに公開されている最新バージョンがインストールされます。
エージェント設定	ESET Management エージェントにポリシーを適用する場合、［選択］または[作成]をクリックします。

(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



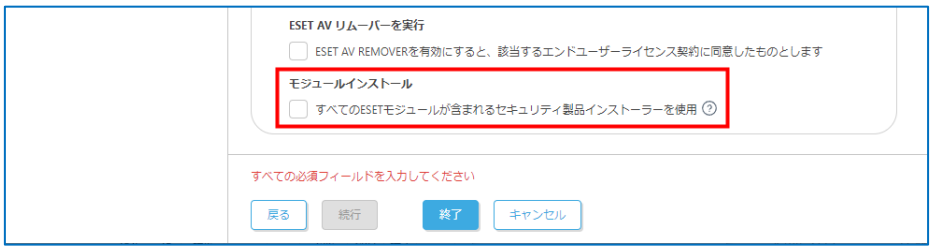
(9).［エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。］にチェックを確認します。

(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。

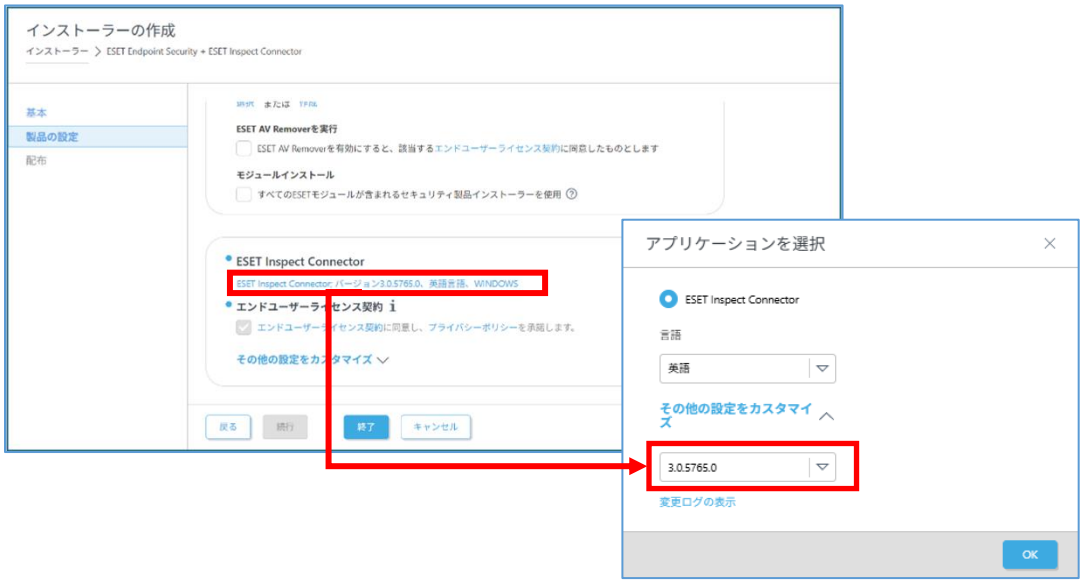
(12).［ESET AV リムーバーを実行］に**チェックが入っていない**ことを確認します。

(13).［モジュールインストール］に以下の通り設定します。



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。

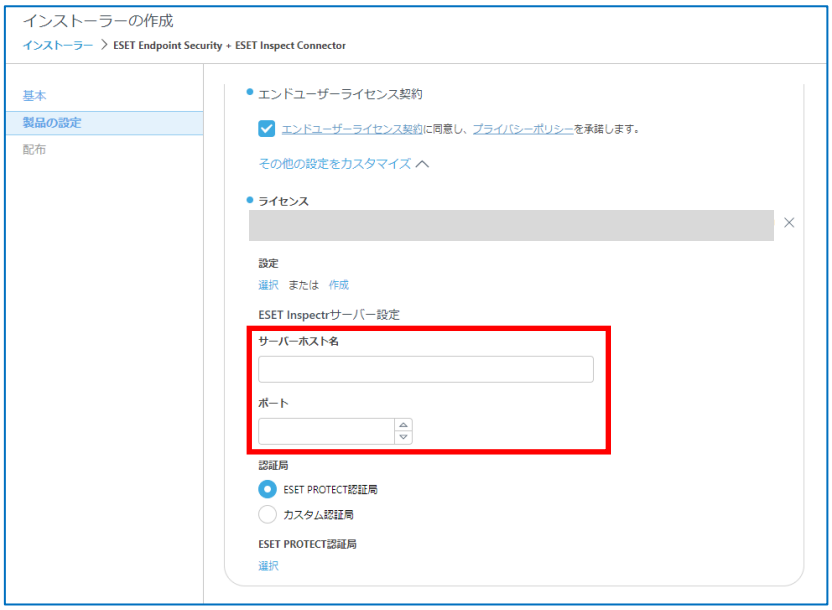


(15).［エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。］にチェックを確認します。

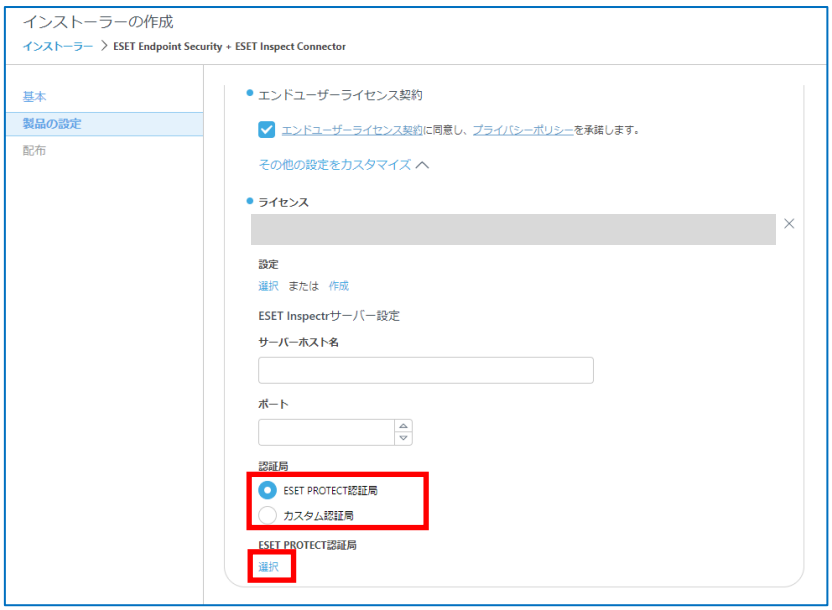
(16).［その他の設定をカスタマイズ］をクリックし、以下の設定をします。

・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

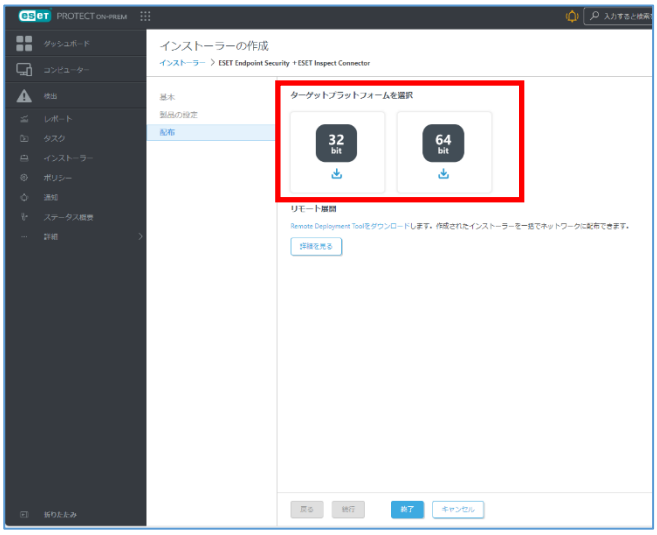
・ポートに 8093(既定)を入力



(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。



(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。



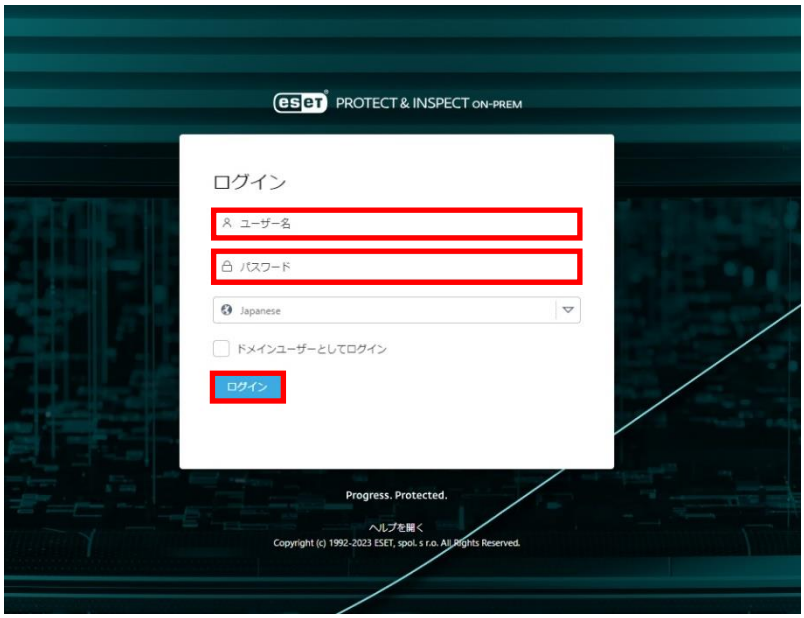
(19).ダウンロードしたオールインワンインストーラーを各クライアントに展開して実行します。

8. EI Web Console の確認【EI 側作業】

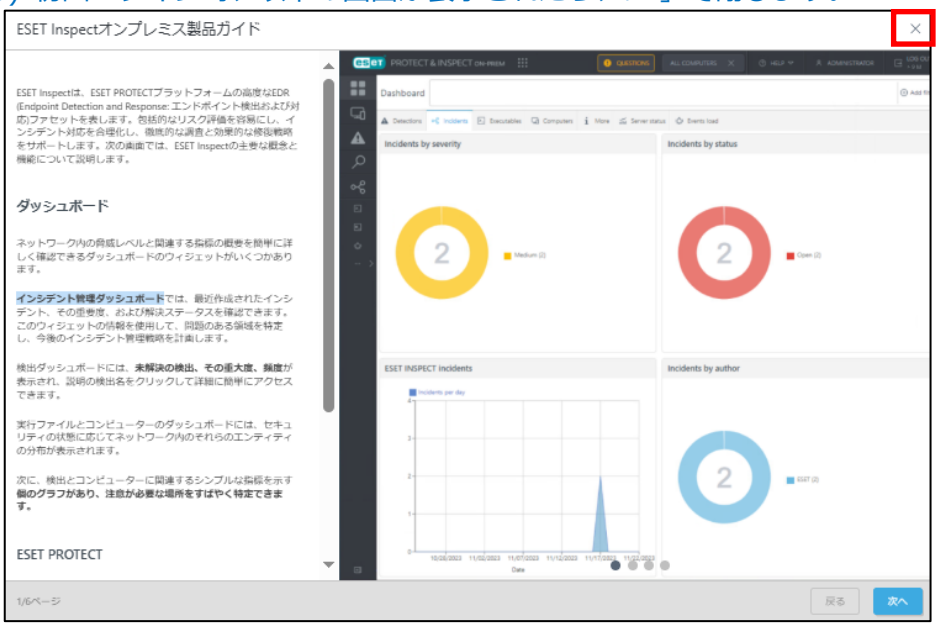
(1). https://(EI Server を導入したサーバーの IP アドレス)にアクセスします。
以下の画面が表示されますので、「xxx.xxx.xxx.xxx にアクセスする（安全ではありません）」をクリックします。

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。

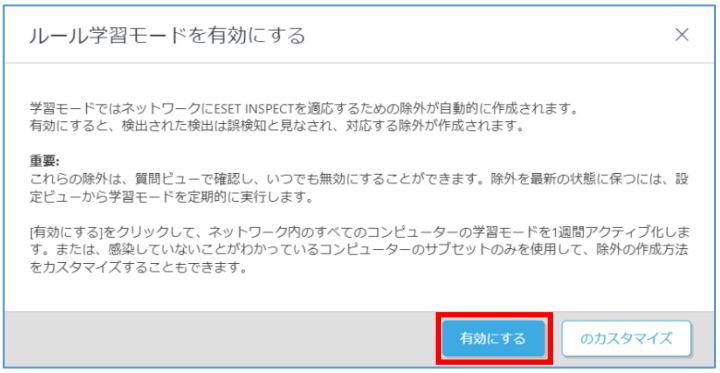
(2). 言語「日本語」を選択して「項番 4.3 ユーザーアカウント作成（例:本手順書では EI_SERVER）」で作成した、ユーザー名、パスワードを入力し [ログイン]をクリックします。



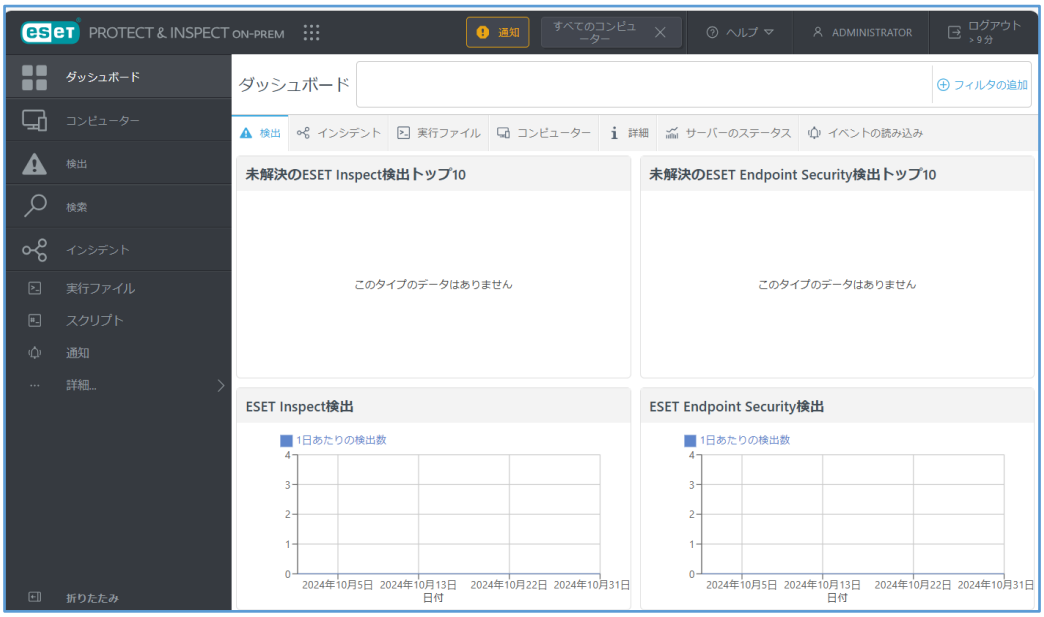
(3). 初回ログイン時、以下の画面が表示されたら、「×」で閉じます。



(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。

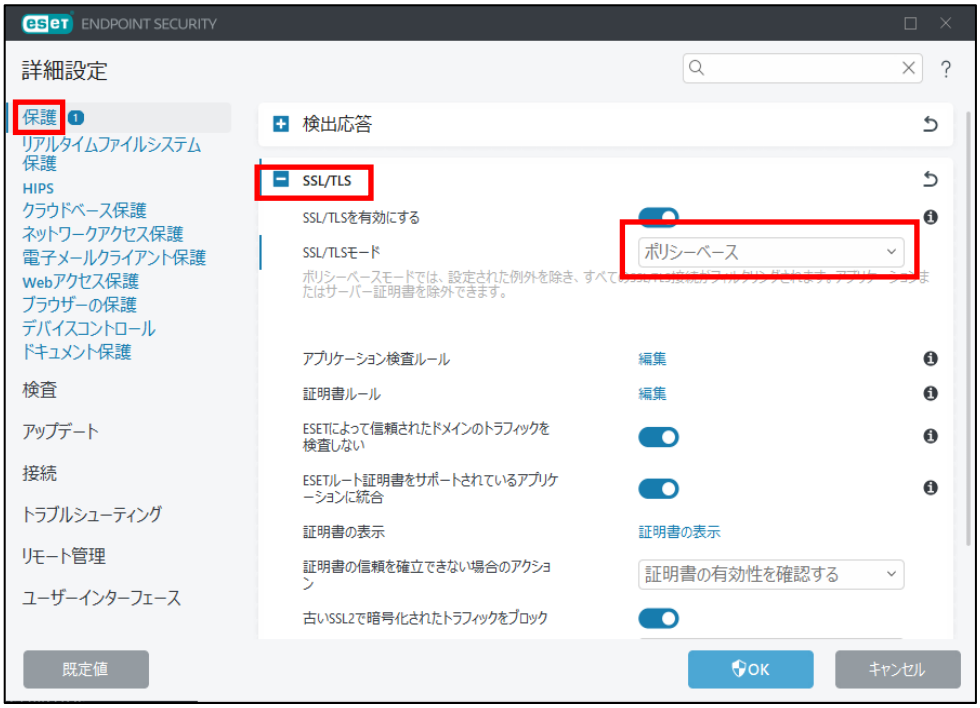
9. EI on-prem 導入時の ESET Endpoint 製品の推奨設定

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。

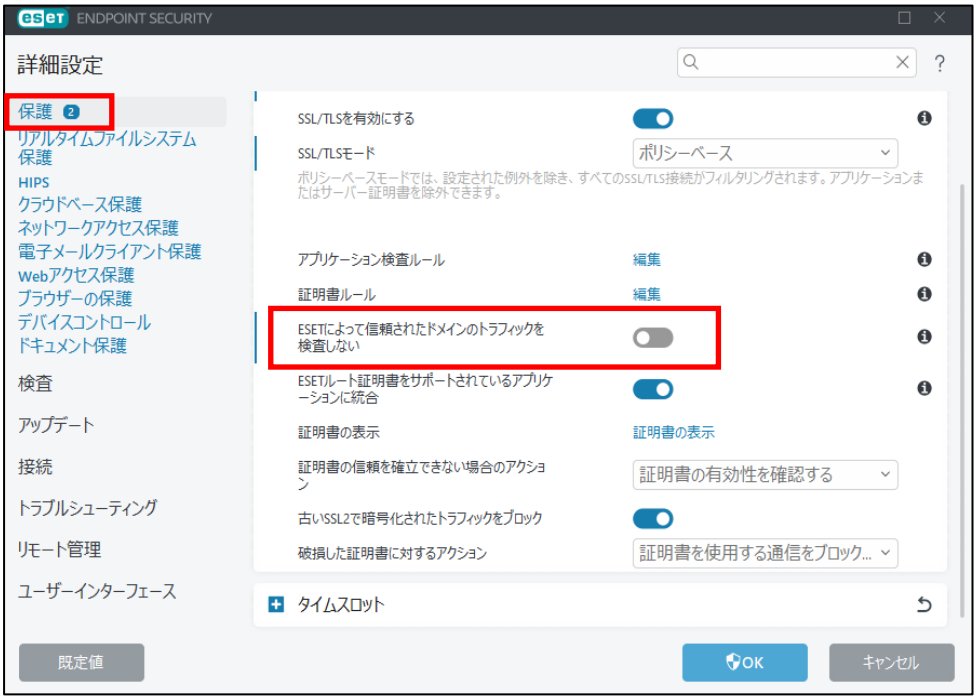
(2). 【SSL/TLS モード】をポリシーベースモードにします。



※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。

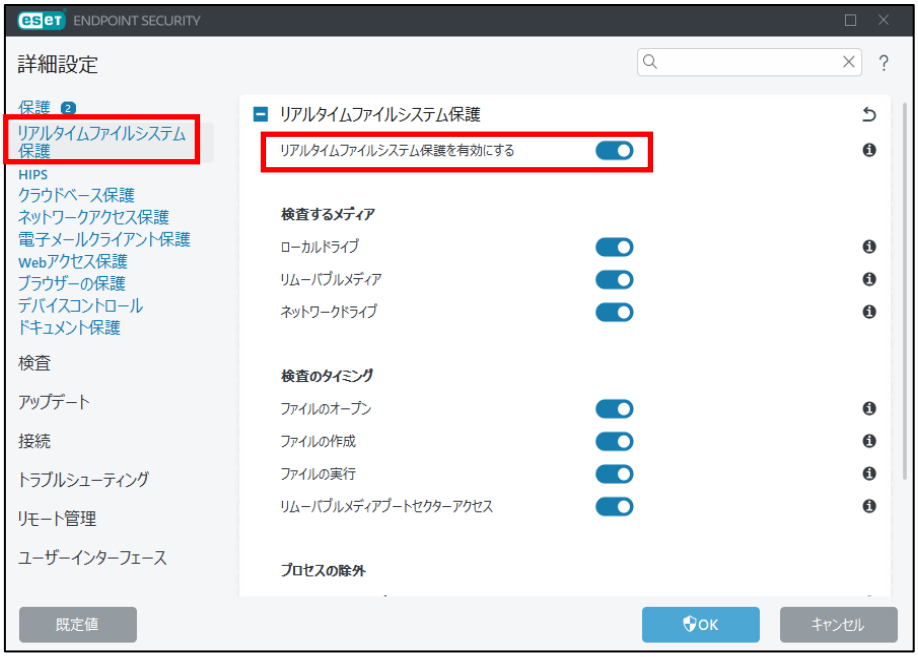
(3). 【ESET によって信頼されたドメインのトラフィックを検査しない】を無効にします。

※ドメインフロンティング攻撃に対応する為の設定です。



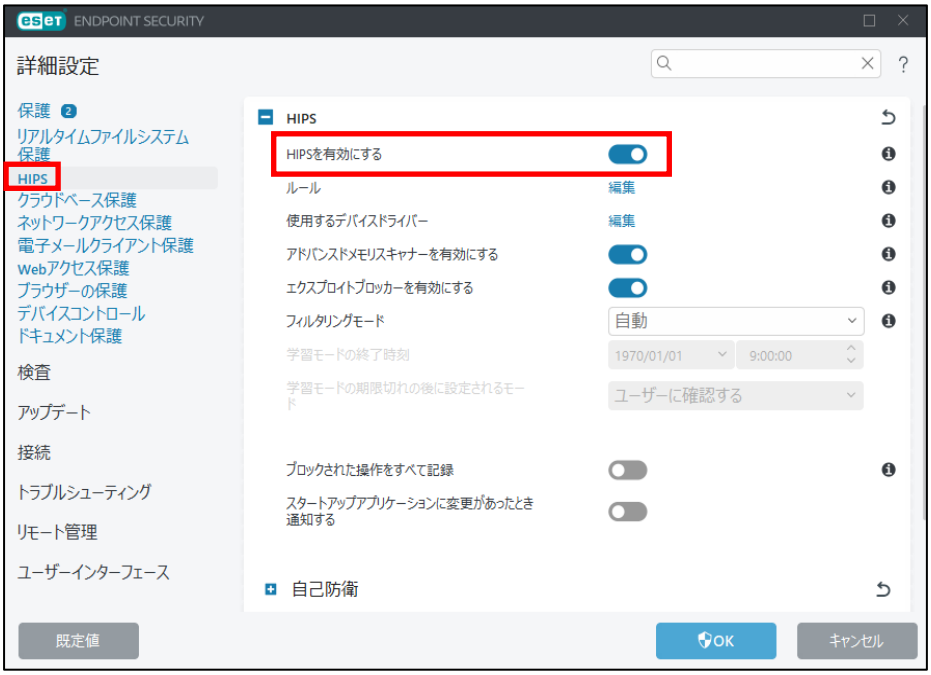
(4).【リアルタイムファイルシステム保護を有効にする】を有効にします。

※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。