ESET Endpoint Protection シリーズ

クライアント管理　クラウド対応オプション（V7.0）

利用手順書

第 4 版

2020 年 11 月

キヤノンマーケティングジャパン株式会社

内容

1. はじめに

○ 本書は、法人向けサーバー・クライアント用製品「ESET クライアント管理 クラウド対応オプション(以下、クラウドオプション)」をご利用になるお客さま向けの手順書となります。

○ 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。

○ 本書内の画面イメージは、Windows10 をベースにして作成しております。そのため、OS によっては記載内容と名称が異なっている場合がございます。

○ 本書内の画面イメージは、ESET Security Management Center V7.0 を使用しています。他のプログラムでも導入の流れに違いはございません。各プログラムのインストールおよび、アンインストール手順に関しましては、弊社ユーザーズサイトで公開しています、各プログラムのユーザーズマニュアルを参照ください。

2. 必要な作業について

クラウドオプションをご利用いただくにあたり、必要な作業は以下の通りです。クラウドオプションのご利用の際には、必ず「3.事前準備」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。

3. 事前準備（P.5）

クラウドオプションのご利用に際し、以下の作業を行います。
- 3.1.動作環境・接続環境の確認
- 3.2.管理可能なプログラムの確認
- 3.3.注意事項、及び禁止事項について
- 3.4.使用できない機能、及び機能制限について
- 3.5.既に ESET 製品をご利用いただいている場合の移行方法の確認
- 3.6.ライセンス情報の確認、ログイン情報の準備

4. 既存のウイルス対策ソフトのアンインストール【クライアント側作業（P.14）

現在インストールされているウイルス対策ソフトをアンインストールします。
すでに ESET 製品をご利用の場合は、以下の作業を参照し、クラウドオプションでクライアント管理を実施します。

5. クラウドオプションへライセンスの登録【管理サーバー側作業】（P.15）

クラウドオプションの ESET Security Management Center（以下 ESMC）にライセンスを追加します。

6. クライアント端末への展開【管理サーバー側作業】【クライアント側作業】（P.19）

クラウドオプションで管理するために、各 OS に応じて以下の導入方法を参照し、クライアント展開を実施してください。
- A）Windows 端末への展開 （P.19）
- B）Mac、Linux 端末への展開（P.53）
- C）Android OS、iOS デバイスへの展開（P.62）

7. クラウドオプションで管理ができていることを確認【管理サーバー側作業（P.89）

「6.クライアント端末への展開」を実施したら、実際にクラウドオプションの管理画面でクライアントの管理ができていることを確認します。

完了

3. 事前準備

3.1. 動作環境・接続環境の確認

クラウドオプションをご利用になる前に、下記 Web ページにて動作環境をご確認いただき、利用可能な環境をご用意ください。

■ESET Endpoint Protection Advanced　動作環境
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html

■ESET Endpoint Protection Standard　動作環境
https://eset-info.canon-its.jp/business/endpoint_protection_std/spec.html

3.2. 管理可能なプログラムの確認

クラウドオプション では、クライアント管理用プログラム「ESET Security Management Center V7.0」をクラウド上にご用意して提供させていただきます。
※従来のバージョン「ESET Remote Administrator」より、名称が変更となりました。

クラウドオプションで管理できる、法人向けサーバー・クライアント用製品のプログラムは以下となります。(2019 年 3 月時点)
対象プログラムとバージョンをご確認のうえ、ご使用ください。

Windows		Mac		Linux	Android	Windows		Linux
EES/EEA		EAVM	EESM/EEAM	EAVL	EESA ※1	EFSW		EFSL ※2
V6.X	V7.X	V4.1	V6.X	V4.0	V2.X	V6.X	V7.X	V4.5
○	○	○	○	○	○	○	○	○

・EES＝ESET Endpoint Security　・EEA=ESET Endpoint アンチウイルス
・EAVM=ESET NOD32 アンチウイルス for Mac　・EESM=ESET Endpoint Security for OS X
・EEAM=ESET Endpoint アンチウイルス for OS X　・EAVL=ESET NOD32 アンチウイルス for Linux Desktop
・EESA=ESET Endpoint Security for Android　・EFSW=ESET File Security for Microsoft Windows Server
・EFSL=ESET File Security for Linux

※1 Android 4.x にインストールされた ESET Endpoint Security for Android は、ESET Security Management Center V7.0 で管理できません。

※2 SUSE Linux Enterprise Server 10 にインストールされた ESET File Security for Linux は、ESET Security Management Center V7.0 で管理できません。

3.3. 注意事項、および禁止事項について

クラウドオプションをご利用いただくうえでの注意事項、および禁止事項がございます。
必ず下記をご確認のうえ、ご利用ください。

【注意事項】

① クラウドオプションで使用する通信ポートについて

クライアント用プログラムを管理するには、クライアント用プログラム および管理画面利用端末から、クラウド上管理サーバーESET Security Management Center(ESMC)の以下のポートへ通信できる必要がありますので､ご注意ください。

- ･2222/TCP ： ESET Management エージェント（EM エージェント）が ESMC と通信する際に利用
- ･443/TCP ： ESMC が､管理画面利用端末からの Web コンソールアクセスを受ける際に利用
- ･80/TCP
- ･443/TCP ： 検出エンジンのアップデート用サーバーがクライアント用プログラムからのアクセスを受ける際に利用

【HTTP プロキシ経由する場合】
HTTP プロキシ経由で ESMC に EM エージェントを接続する場合は、以下の条件を満たす必要がありますので、ご注意ください。

- ･HTTP プロキシが ESMC で利用する TLS/SSL 通信（2222/TCP）を転送できること
- ･HTTP CONNECT メソッドをサポートしていること
- ･プロキシ認証を必要としないこと（ユーザー名/パスワード設定不可）
- ･プロキシサーバーから、上記ポートへ通信できること

Android OS、iOS のモバイルデバイスを管理する方は、以下のポートへも通信できる必要がありますので、ご注意ください。

- ･9980/TCP ： モバイルデバイスを ESMC に登録する際に利用
- ･9981/TCP ： モバイルデバイスが ESMC と通信する際に利用
- ･5228/TCP
- ･5229/TCP
- ･5230/TCP ： モバイルデバイス（Android OS の場合）が Firebase Cloud Messaging へ接続する際に利用
- ･5223/TCP ： モバイルデバイス（iOS の場合）が Apple Push Notification Server へ接続する際に利用

② ウェイクアップコール（ESMC とクライアントの即時通信）について

ESMC は ESET Push Notification Service（EPNS）を利用して EM エージェントにウェイクアップコールを送信し、即時通信することが可能です。
ウェイクアップコールを利用する場合は、以下の条件を満たす必要があります。

- ･EM エージェントが EPNS サーバーへ、8883/MQTT で直接接続できること

接続詳細	
転送セキュリティ	SSL
プロトコル	MQTT（コンピューター間接続プロトコル）
ポート	8883
EPNS サーバーのホストアドレス	epns.eset.com

※ HTTP プロキシを経由することはできません。

③ **モバイルデバイス登録時、クラウドオプションから送信されるメールアドレスについて**

Android、iOS のモバイルデバイス登録時や ESMC の通知機能をご利用になる場合、ESMC から送信されるメールがスパム判定される可能性があります。以下のアドレスはスパム判定されないように除外してください。

era-admin@era-cloud.canon-its.jp

④ **バックアップ及びメンテナンスについて**

クラウドオプションサーバー全体のバックアップを毎日 AM2 時～AM4 時で取得します。バックアップ取得中の数分間、ESMC サーバーが停止します。
この間にタスクを設定するとタスクが実行されない場合があります。
本時間帯でタスクのスケジュールの指定は行わないようにしてください。

⑤ **ESMC 上のログ保存について**

ESMC が取得するクライアント PC からの各種ログデータについては、6 ヶ月間保存します。また、保存期間を変更することはできません。

【禁止事項】

① **ESET Management エージェントの接続間隔について**
ESMC と ESET Management (EM エージェント)の接続間隔は既定で「20 分」に設定しています。接続間隔を 20 分未満に設定しないでください。

② **レポートファイルの過度なダウンロードについて**
レポートファイルをダウンロードする場合、一日に合計 30MB 以上のダウンロードは実施しないでください。

③ **通知メールの過度な送信設定について**
通知機能をご利用になる場合、一日に合計 1,000 通以上通知するように設定しないでください。

④ **メールアドレスの送信先について**
存在しない電子メールアドレスやお客様以外の第三者の電子メールアドレスを通知の送信先、および、モバイルデバイス登録のための送信先として設定しないでください。

⑤ **モバイルデバイスを管理するために表示される ESET Security Management Center への操作について**
ESMC の管理画面のコンピューター一覧に、管理対象の端末として ESMC 自体が下記のコンピュータ名で表示されます。ESMC に対する下記の操作は、クラウドオプションの運用管理に支障をきたしますので、行わないでください。

ip-172-31-xxx-xxx.ap-northeast-1.compute.internal

※ 「172-31-xxx-xxx」は、お客さまによって異なります。

1. コンピューターのシャットダウンタスクによる ESMC サーバーのシャットダウンおよび再起動
2. オペレーティングシステムのアップグレードタスクによる ESMC サーバーの OS のパッチ等のアップデート
3. 管理の停止タスクやアンインストールタスクによる ESMC サーバーの EM エージェントのアンインストール
4. コンポーネントアップグレードによる ESMC サーバーのアップグレード
5. コマンドの実行タスクによる ESMC サーバーに対する任意のコマンド実行
6. 初期設定されている ESMC サーバーのポリシーの変更、および、削除
7. ESMC サーバー自体の削除
8. ESMC サーバーが所属する静的グループの変更

3.4. 使用できない機能、及び機能制限について

クラウドオプションでは下記機能がご使用いただけませんのでご注意ください。

	機能名	詳細	設定場所
1	レポートの電子メールによる送信	レポートを電子メールで送信する機能	[詳細] -[サーバータスク] -[レポートの作成]
2	SNMP トラップサービス、Syslog の送信	通知機能で SNMP トラップの送信、および、Syslog サーバーへ通知する機能	[通知]
3	エージェント展開	EM エージェントをリモートで展開する機能	[詳細] -[サーバータスク] -[エージェント展開]
4	静的グループの同期	AD/VMware/LDAP/Open Directory/Windows ネットワークと連携して、管理サーバー上に静的グループを自動で作成する機能	[詳細] -[サーバータスク] -[静的グループの同期]
5	ユーザー作成	ESMC にログインするための Web コンソールアカウント作成機能（アクセス権の設定）	[詳細]-[ユーザー] [詳細]-[権限設定]
6	監査ログ	監査ログの生成と閲覧機能	[レポート]-[監査ログ]
7	ユーザー同期	AD と連携しユーザー情報を同期する機能	[詳細] -[サーバータスク] -[ユーザー同期]
8	レポートの作成	サーバータスク機能を利用してレポートをサーバー上に作成する機能	[詳細] -[サーバータスク] -[レポートの作成]
9	Rogue Detection sensor を利用したコンピュータ追加	Rogue Detection sensor コンポーネントをインストールし、コンピュータを追加する機能	-

3.5. 既に ESET 製品をご利用いただいている場合の移行方法の確認

(1)個人向け製品を使用。

個人向け製品のプログラムはクラウドオプションで管理することができません。
法人向けサーバー・クライアント用製品のプログラムに入れ替える必要があります。

⇒「3.事前準備」で作業の流れ、必要な情報を確認後、「4.既存のウイルス対策ソフトのアンインストール【クライアント端末側作業】」以降の作業を実施してください。

(2) 既に法人向けサーバー・クライアント用製品プログラムを使用。
クライアント管理は未実施。

ご利用の法人向けサーバー・クライアント用製品プログラムが、クラウドオプションで管理可能なプログラムの場合、EM エージェントを導入することで、クラウドオプションでクライアント管理を行うことができます。

⇒「3.事前準備」で作業の流れ、必要な情報を確認後、「5.クラウドオプションへライセンスの登録【管理サーバー側作業】」から作業を実施してください。
「6.クライアント端末への展開」では、【既存お客様向け】の手順を参照し、クライアント管理を実施してください。

(3) 既に法人向けサーバー・クライアント用製品プログラムを使用。
ERA V6またはESMC V7（オンプレミス）で管理を実施。

クライアントの管理を社内にオンプレミスで構築したERA V6またはESMC V7からクラウドオプションに変更する場合には、現在インストール済みのERAエージェントまたはEMエージェントをアンインストールし、新たにクラウドオプション用のEMエージェントをインストールすることで、クラウドオプションで提供している管理サーバー（ESMC）に管理を変更することができます。

⇒コントロールパネルのプログラムと機能より「EEST Remote Administrator Agent」または「ESET Management Agent」のアンインストールを実施後、「6.クライアント端末への展開」より【既存お客様向け】の手順を参照し、クライアント管理を実施してください。
クライアントプログラムについても、最新バージョンへのバージョンアップをご検討ください。

(4) 既に法人向けサーバー・クライアント用製品プログラムを使用。
クラウドオプション（ERA V6.5）で管理を実施。

すでにクラウドオプションのERA V6.5をご利用で、ESMC V7にバージョンアップされた場合には、現在インストール済みのERA エージェントをESMC用のエージェント「EMエージェント」にバージョンアップする必要があります。

⇒ESMCのタスク機能を利用し、バージョンアップが可能です。
ユーザーズマニュアルよりダウンロード可能な「ESET Security Management Center ユーザーズマニュアル」より「4.1 コンポーネントアップグレードタスク」を実施してください。
※本タスクを実行すると、各クライアントからのネットワーク負荷がかかるため台数や時間を分けるなど、実行タイミングを分散することを推奨します。

現在ご利用中のクライアントプログラムのバージョン確認方法
ESET 製品をご利用の端末で、クライアント端末にインストールされている ESET 製品のバージョンがご不明の場合は、下記 Web ページよりご確認ください。

【プログラムのバージョンの確認方法】
https://eset-support.canon-its.jp/faq/show/140?site_domain=business

3.6. ライセンス情報・ログイン情報の準備

クラウドオプションを利用するにあたり以下 2 種類の情報が必要です。お手元にご用意ください。

(1)ESET ライセンス製品 ライセンス情報

「ESET ライセンス製品」をお申し込みいただいたお客様にメールで、「ESET セキュリティ ソフトウェアシリーズ用 ユーザーズサイト ログイン情報のご案内」をお送りしておりますのでご参照ください。

- シリアル番号　※メール本文に記載
- ユーザー名　※ライセンス製品新規購入後の電子納品メールに記載
- 製品認証キー　※下記ユーザーズサイトに記載
- パスワード　※下記ユーザーズサイトに記載

(2)クラウドオプション　ログイン情報

「ESET クライアント管理 クラウド対応オプション」をお申込みいただいたお客様へ、ユーザーズサイトの「ライセンス情報」に下記情報を記載しておりますので、ご参照ください。

- Web コンソール（管理画面）ログイン用 URL　※下記ユーザーズサイトに記載
- ESMC サーバー/ERA サーバーの IP アドレス　※下記ユーザーズサイトに記載
- ログイン名　※下記ユーザーズサイトに記載
- 初回ログインパスワード　※下記ユーザーズサイトに記載
- 証明書パスフレーズ

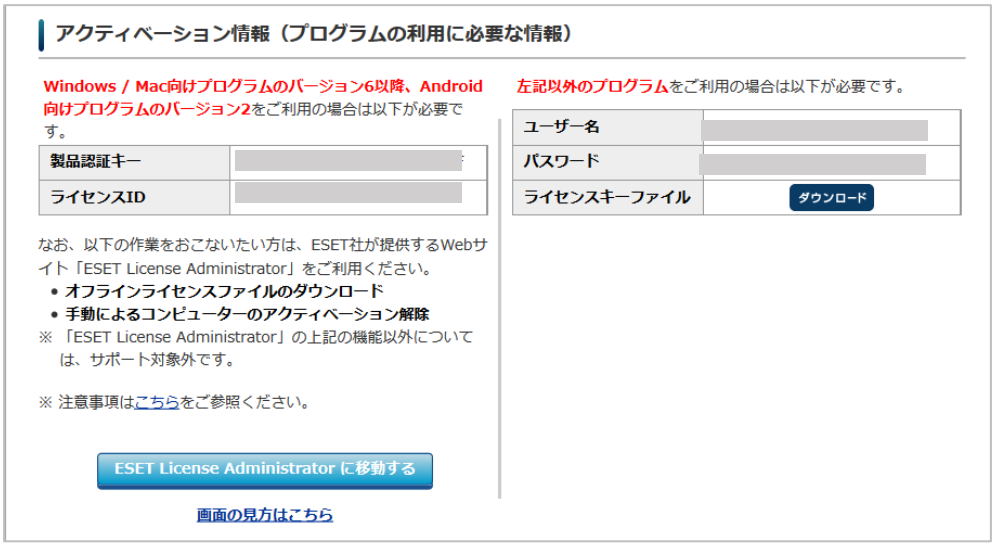
下記弊社ユーザーズサイトにて、ライセンス情報や各種プログラム、マニュアルを公開しております。
ライセンス情報やプログラムの各種設定につきましては、ユーザーズサイトをご参照ください。

■ **ESET Endpoint Protection シリーズ ユーザーズサイト**
https://canon-its.jp/product/eset/users/
※ログイン時に「シリアル番号」、「ユーザー名」が必要です。

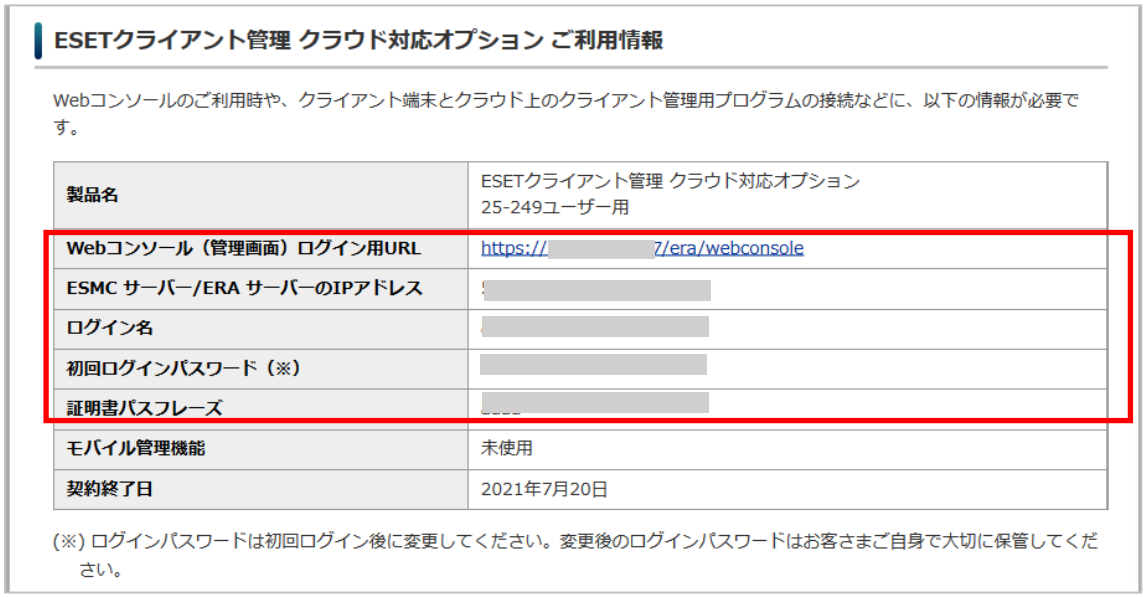
1. ユーザーズサイトログイン後、「ライセンス情報/申込書作成」をクリックしてください。
※ マニュアルについては、「プログラム/マニュアル」タブよりダウンロードすることができます。

2. クラウドオプションのライセンス情報、またはログイン情報は、以下をご参照ください。

ア)ESET ライセンス製品 ライセンス情報

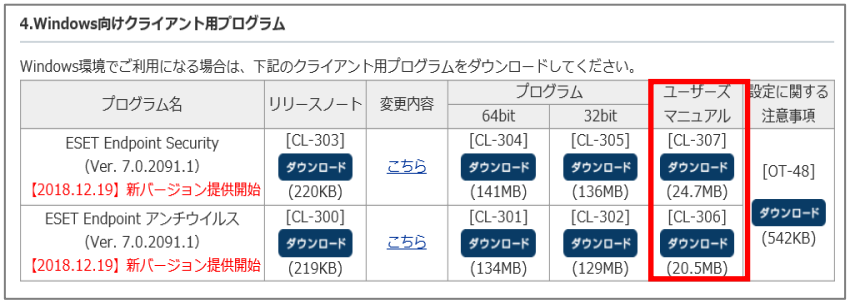


イ)クラウド対応オプション　ログイン情報



【参考】

ユーザーズサイト「プログラム/マニュアル」より、「最新バージョンをダウンロード」または「プログラム一覧からダウンロード」を選択すると、以下のようなダウンロードページが表示され、各種プログラムやマニュアルのダウンロードが可能です。



4. 既存のウイルス対策ソフトのアンインストール【クライアント端末側作業】

クライアント端末に他社製のウイルス対策ソフトがインストールされている場合は、ESET をご利用いただく前にアンインストールする必要があります。

現在、クライアント端末にウイルス対策ソフトがインストールされていない場合は、「**5.クラウドオプションへのライセンスの追加【管理サーバー側作業】**」に進んでください。

・他社製ウイルス対策ソフトのアンインストール

現在、他社製ウイルス対策ソフトをインストールしている端末で、ESET 製品を導入する場合は、必ず他社製ウイルス対策ソフトをアンインストールしてください。
複数のウイルス対策ソフトの併用は、パフォーマンスの低下やトラブルの原因となります。

他社製ウイルス対策ソフトのアンインストール後は、本資料「**6.クライアント端末への展開【管理サーバー側作業】**」へ進んでください。

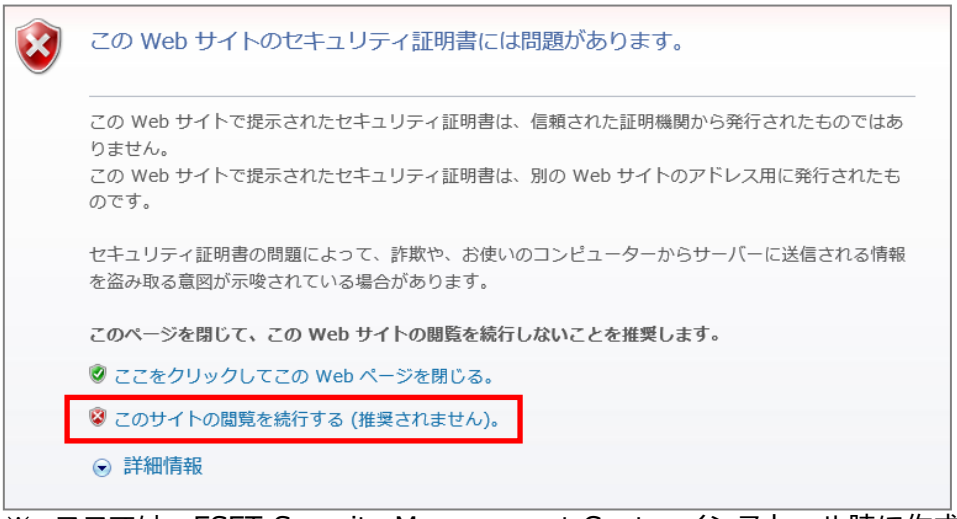
他社製ウイルス対策ソフトのアンインストール方法がご不明の場合は、
下記の WEB ページをご参照ください。
【他社製ウイルス対策ソフトのアンインストールについて】
https://eset-support.canon-its.jp/faq/show/81?site_domain=business

5. クラウドオプションへのライセンスの追加【管理サーバー側作業】

以下の手順を参照し、ライセンスの追加を行ってください。

1. Web ブラウザより、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「Web コンソール（管理画面）ログイン用 URL」にアクセスします。

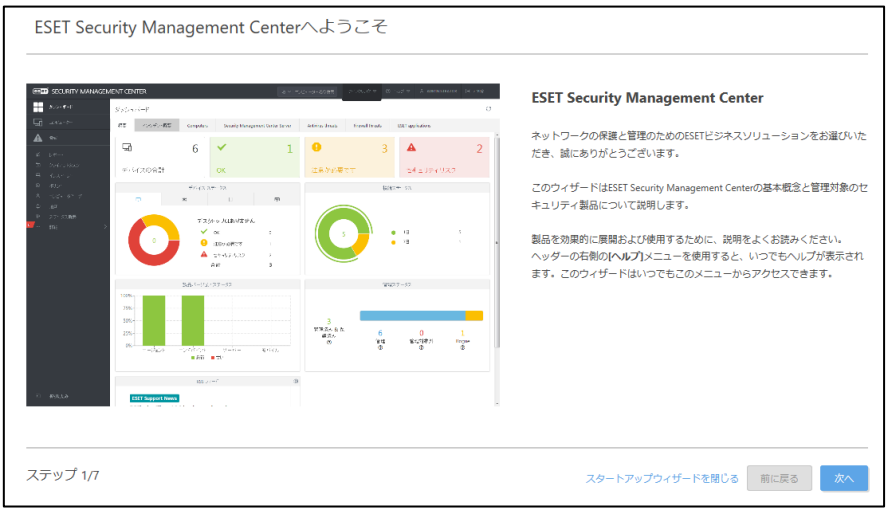
   以下の画面が表示されますので、「このサイトの閲覧を続行する（推奨されません）。」をクリックします。



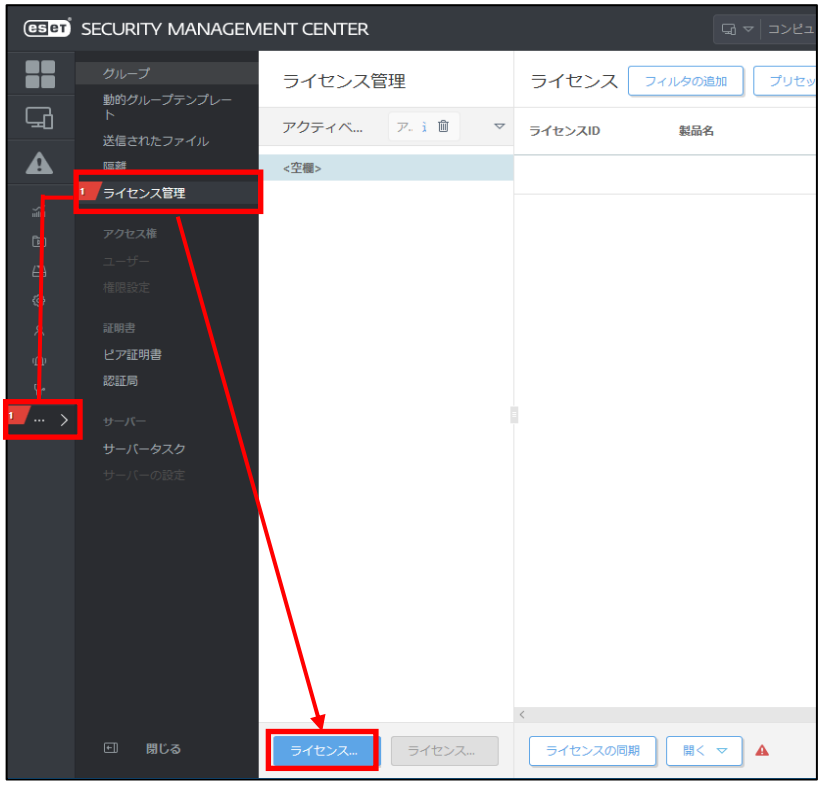
※ ここでは、ESET Security Management Center インストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
※ お使いのブラウザより、表示内容が異なります。

2. 「**3.6.ライセンス情報・ログイン情報の準備**」で確認した
①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。
※ 初回ログイン時、また、パスワード有効期限が切れた場合は、画面の指示に従ってパスワード変更を行ってください。また、左下の「パスワード変更」から変更することも可能です。

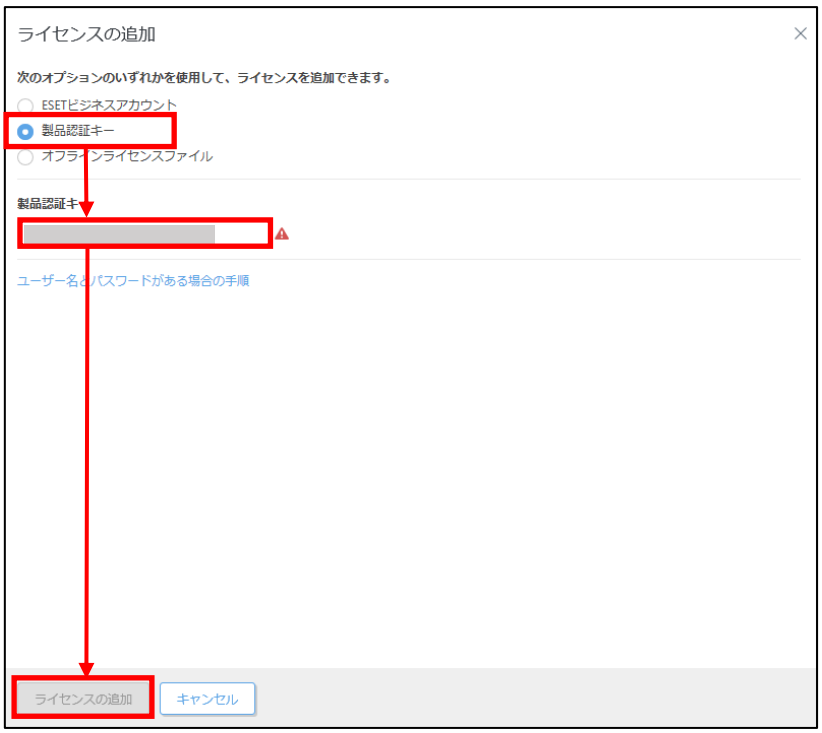
3. ESET Security Management Center スタートアップウィザードが表示された場合は「次へ」で進むか、また、閉じる場合は「スタートアップウィザードを閉じる」をクリックします。
※ 続いて新機能紹介が表示された場合は、「×」で閉じてください。



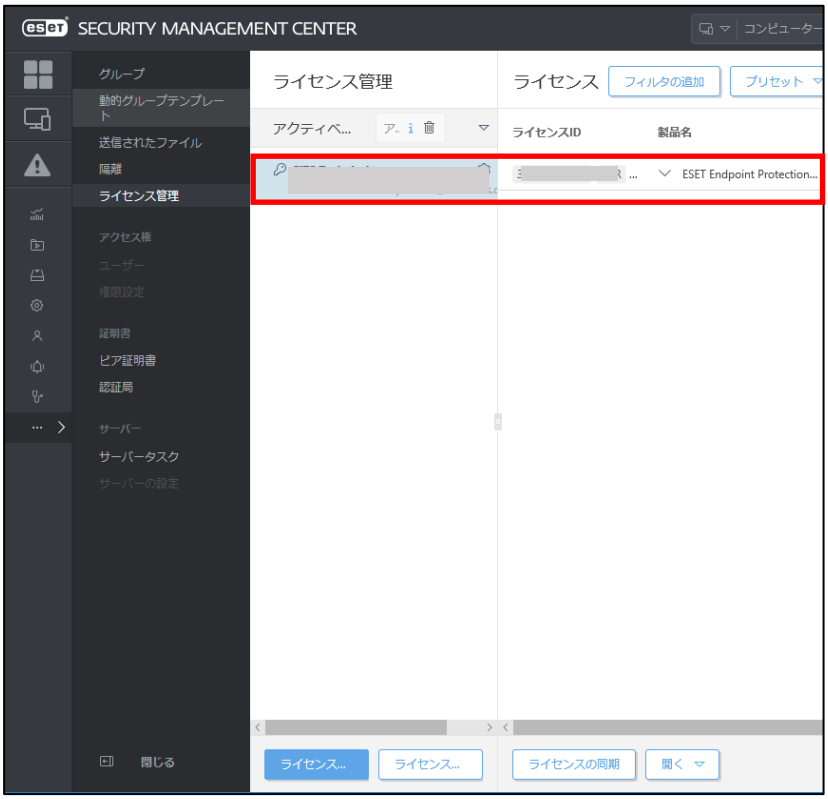
4. 画面左側のメニューより、「詳細」→「ライセンス管理」をクリックします。
「ラインセンスの追加」をクリックします。



5. 「製品認証キー」を選択し、「**3.6. ライセンス情報・ログイン情報の準備**」で確認した製品認証キーを入力し、「ライセンスの追加」をクリックします。



6. ライセンスが追加されていることを確認します。



以上で、クラウドオプションへのライセンスの登録は完了です。
続いて、「6．クライアント端末への展開」を実施してください。

6. クライアント端末への展開【管理サーバー側作業】【クライアント端末側作業】

クラウドオプションでクライアント管理を行う手順について、【新規お客様向け】また【既存お客様向け】に以下２通りの手順を記載しております。
ご利用状況に応じて、以下を参考にクラウドオプションでの管理を開始してください。
Windows 以外の端末への導入については、「B) Mac、Linux 端末への展開」「C) Android、iOS への展開」をご確認ください。

A）Windows 端末への展開

【新規お客様向け】

クライアント用プログラムがインストールされていない

【既存お客様向け】

すでにクライアント用プログラムがインストールされている

＜事前準備＞HTTP プロキシを経由する場合【管理サーバー側作業】

HTTP プロキシ経由で ESMC へ接続する場合、EM エージェントとクライアントプログラムの両プログラムに対して、HTTP プロキシ経由用の設定をポリシーで作成します。
HTTP プロキシを経由しない場合は、下記の手順に進んでください。

A-1-1. オールインワンインストーラーの作成【管理サーバー側作業】

「ESET クライアント用プログラム」と、「EM エージェント」を一括にインストールするオールインワンインストーラーを ESMC で作成します。
オールインワンインストーラー作成後はクライアント端末に配布します。

A-1-2. オールインワンインストーラーの実行【クライアント側作業】

インストールが完了すると、クラウドオプションの ESMC と通信が自動的に行われます。

A-2-1. オールインワンインストーラー（EM エージェントのみ）の作成【管理サーバー側作業】

「EM エージェント」のみをインストールするためのオールインワンインストーラーで作成します。
オールインワンインストーラー作成後はクライアント端末に配布します。

A-2-2. オールインワンインストーラーの実行【クライアント側作業】

インストールが完了すると、クラウドオプションの ESMC と通信が自動的に行われます。

7. クラウドオプションで管理ができていることを確認【管理サーバー側作業】

Web ブラウザからクラウドオプションの ESMC にアクセスし、クライアントの管理状況を確認します。

＜事前準備＞HTTP プロキシを経由する場合【管理サーバー側作業】

各クライアントが HTTP プロキシを経由してクラウドオプションの ESMC に接続する場合は、事前に EM エージェントとクライアントプログラムの両プログラムに対して、HTTP プロキシ経由用の設定をポリシーで作成します。

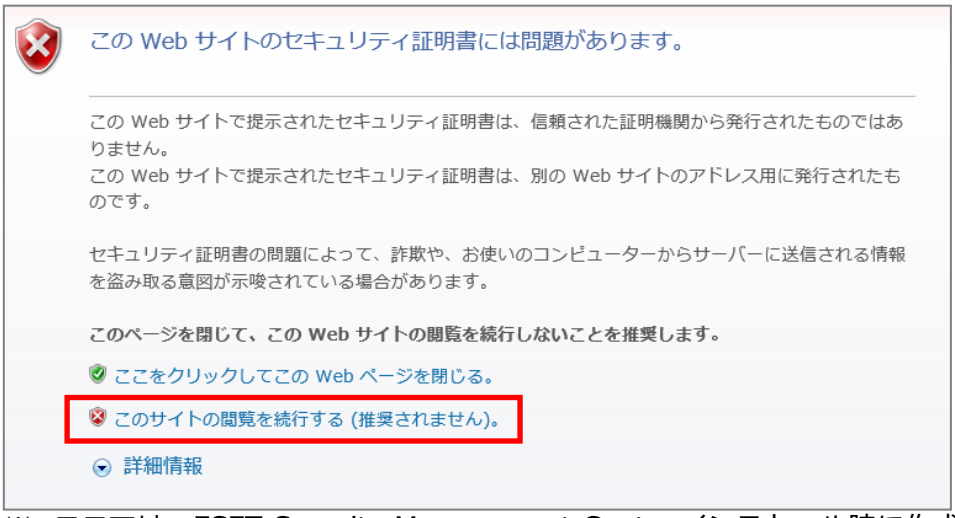
HTTP プロキシを経由しない場合は、新規または既存お客様向け手順に応じて、オールインワンインストーラー作成に進んでください。

以下に、各プログラムのポリシー作成手順を記載します。

【EM エージェント向け、HTTP プロキシ経由ポリシー作成方法】

1. Web ブラウザより、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「Web コンソール（管理画面）ログイン用 URL」にアクセスします。

   以下の画面が表示されますので、「このサイトの閲覧を続行する（推奨されません）。」をクリックします。

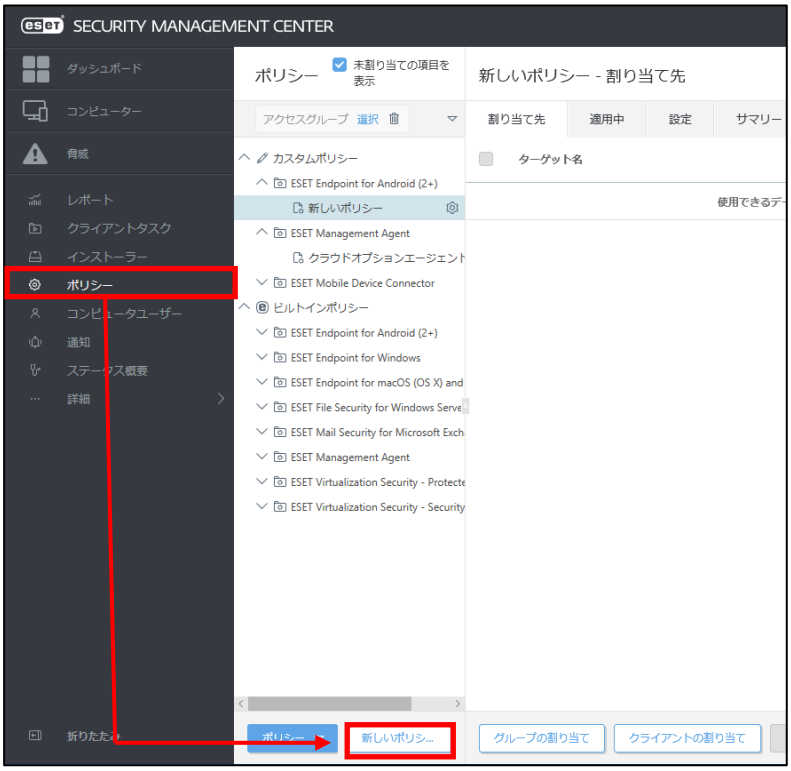


※ ここでは、ESET Security Management Center インストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。

※ お使いのブラウザより、表示内容が異なります。

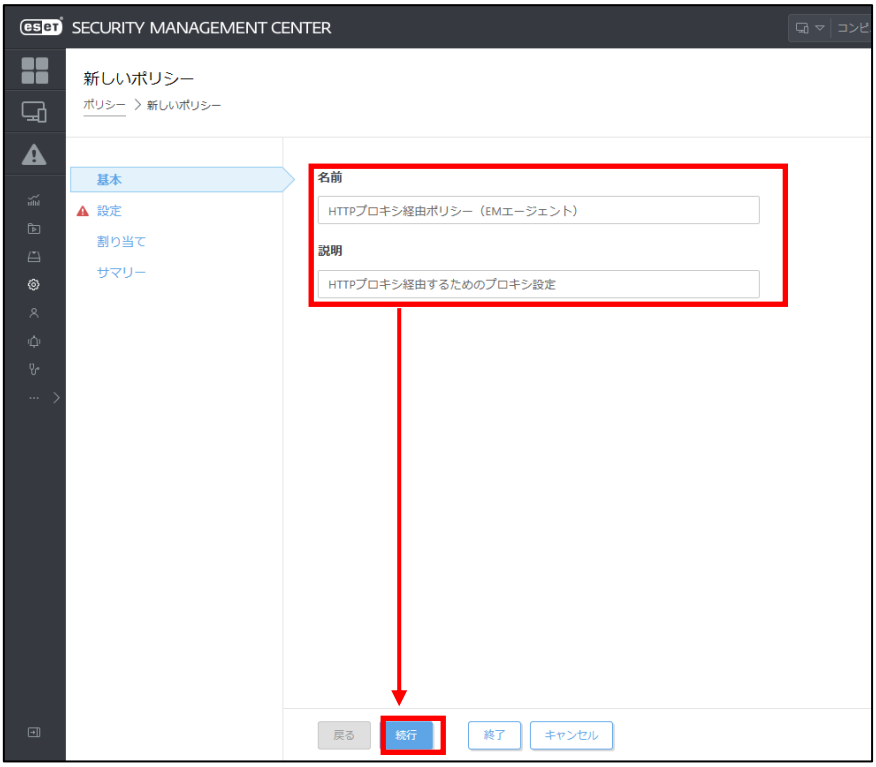
2. 「**3.6.ライセンス情報･ログイン情報の準備**」で確認した①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。
   ※ 初回ログイン時、また、パスワード有効期限が切れた場合は、画面の指示に従ってパスワード変更を行ってください。また、左下の「パスワード変更」から変更することも可能です。

3. 「ポリシー」→「新しいポリシー」をクリックします。



4. 以下を参考に入力し、「続行」をクリックします。

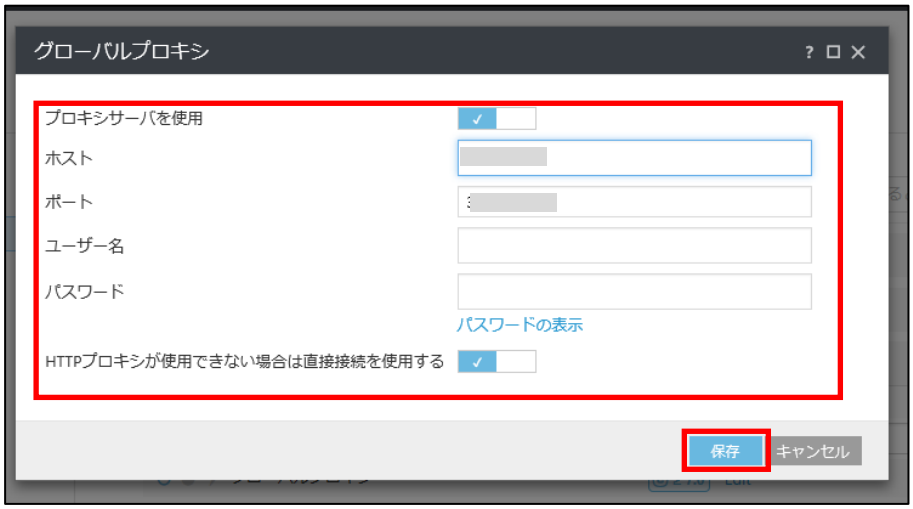
名前	HTTP プロキシ経由ポリシー（EM エージェント）
説明（任意）	HTTP プロキシを経由するためのプロキシ設定



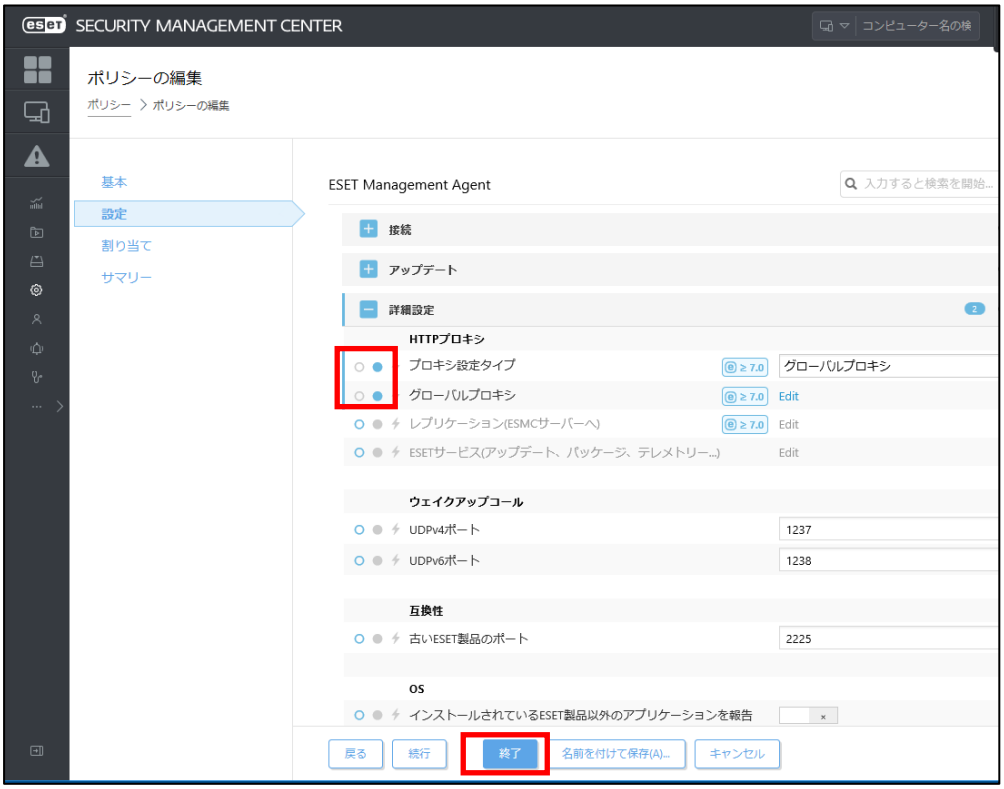
5. 「ESET Management Agent」を選択し、「詳細設定」を展開します。
プロキシ設定タイプにて、「グローバルプロキシ」が選択されていることを確認し、
左側アイコンで真ん中の「●」を選択します。
グローバルプロキシの「Edit」をクリックします。

6. 以下の通り入力し、「保存」をクリックします。

プロキシサーバを使用	**有効**にする
ホスト	HTTP プロキシサーバーのホスト名または IP アドレス
ポート	HTTP プロキシサーバーのポート番号
ユーザー名	プロキシ認証に対応していないため設定不可
パスワード	
HTTP プロキシが使用できない場合は直接接続を使用する	接続する場合は有効にする



7. 「プロキシ設定タイプ」と「グローバルプロキシ」のアイコンが、真ん中の「●」であることを確認し、「終了」をクリックします。

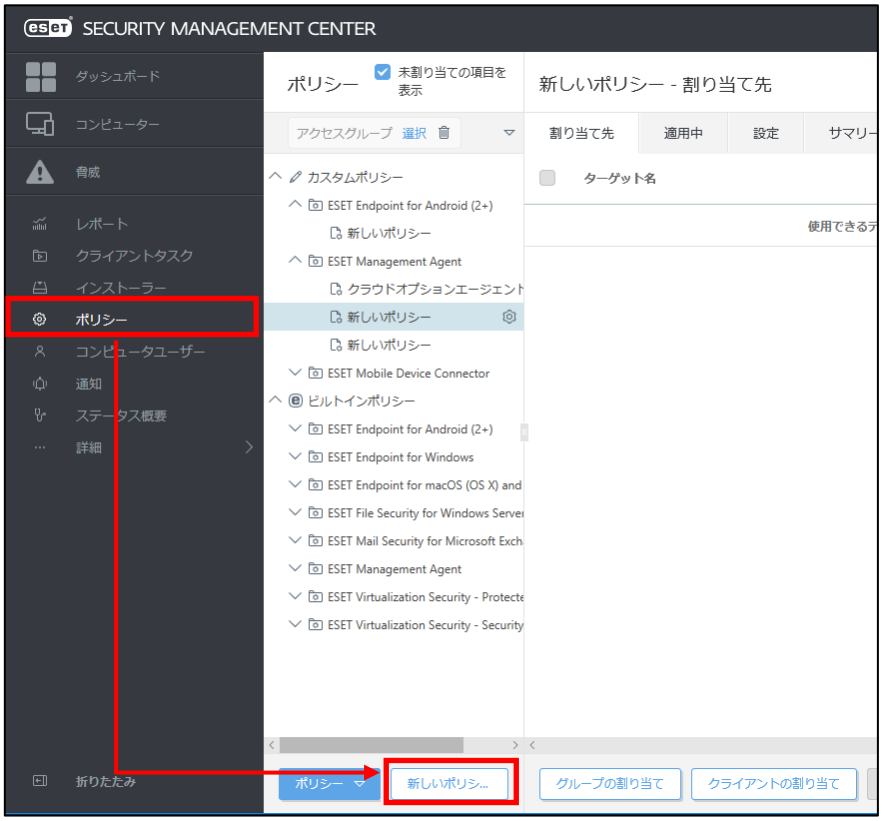


以上で、EM エージェント向け、HTTP プロキシ経由ポリシーの作成は完了です。
本ポリシーは、展開時にインストーラーに組み込むことで適用されます。

続いて、クライアントプログラムが HTTP プロキシを経由するためのポリシーを作成します。

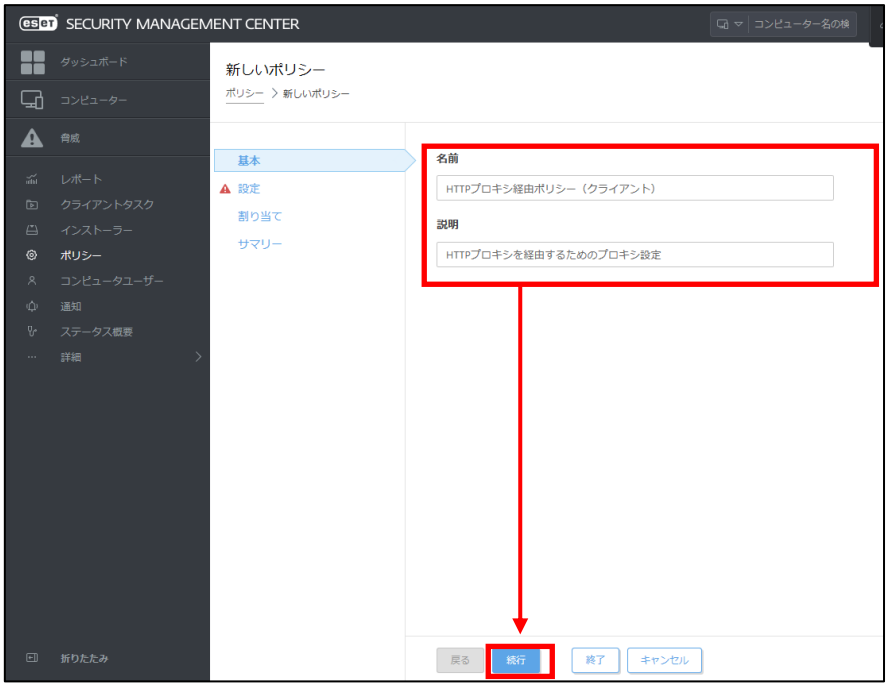
【クライアントプログラム向け、HTTP プロキシ経由ポリシー作成方法】

1. ESMC にログインし、「ポリシー」→「新しいポリシー」をクリックします。

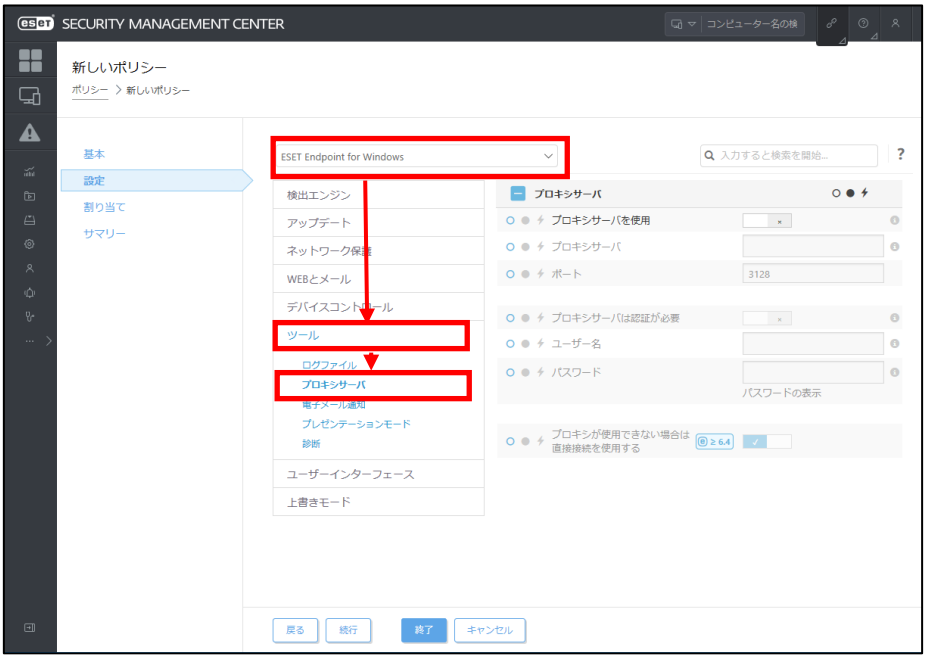


2. 以下を参考に入力し、「続行」をクリックします。

名前	HTTP プロキシ経由ポリシー（クライアント）
説明（任意）	HTTP プロキシを経由するためのプロキシ設定

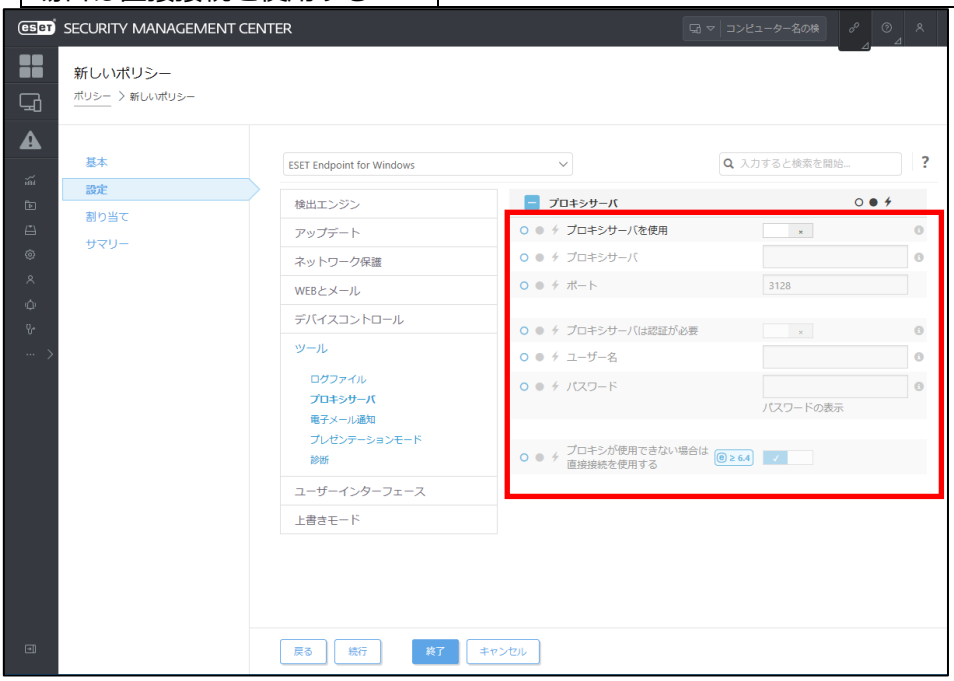


3. クライアント OS の場合「ESET Endpoint for Windows」、サーバーOS の場合「ESET File Security for Windows Server(V6+)」を選択し、「ツール」→「プロキシサーバ」と展開します。

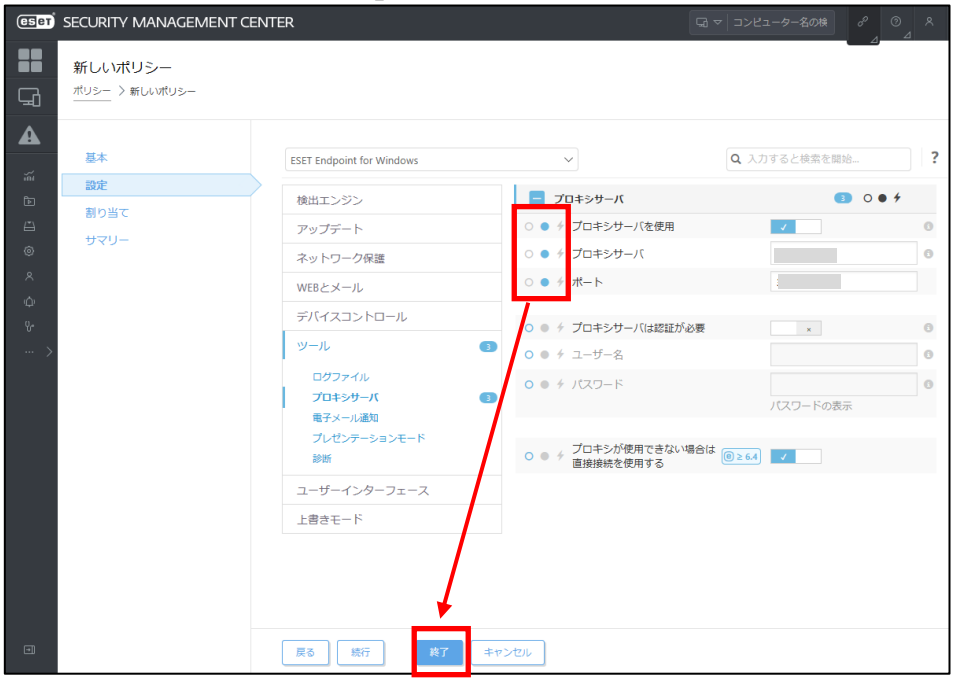


4. 以下の通り入力します。

プロキシサーバを使用	**有効**にする
プロキシサーバ	HTTP プロキシサーバーのホスト名または IP アドレス
ポート	HTTP プロキシサーバーのポート番号
プロキシサーバは認証が必要	プロキシ認証に対応していないため設定不可
ユーザー名	
パスワード	
HTTP プロキシが使用できない場合は直接接続を使用する	接続する場合は有効にする



5. 「プロキシサーバを使用」「プロキシサーバ」「ポート」のアイコンが、真ん中の「●」であることを確認し、「終了」をクリックします。



以上で、クライアントプログラム向け、HTTP プロキシ経由ポリシーの作成は完了です。
本ポリシーは、展開時にインストーラーに組み込むことで適用されます。

続いて、新規、もしくは、既存環境に応じて、オールインワンインストーラーの作成・実行に進んでください。

ポリシーの作成について、詳細は以下 Web ページもご参考ください。
【ESET Security Management Center V7.0 を利用して、新しいポリシーを作成する手順】
https://eset-support.canon-its.jp/faq/show/11854?site_domain=business

【新規お客様向け】

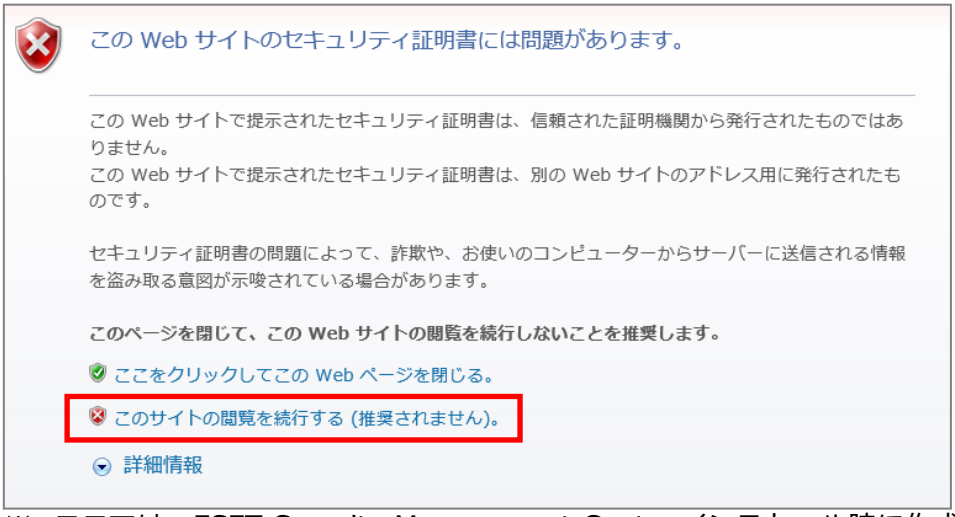
A-1-1. オールインワンインストーラーの作成【管理サーバー側作業】

クラウドオプションでクライアントの管理を行うためには、ESET クライアント用プログラムに加えて、ESET Management Agent（以降 EM エージェント）のインストールが必要です。管理サーバーでは、EM エージェントと ESET クライアント用プログラムを一つにまとめたインストーラーパッケージ「オールインワンインストーラー」を作成することができます。

以下に、オールインワンインスト―ラーの作成手順を記載します。

1. Web ブラウザより、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「Web コンソール（管理画面）ログイン用 URL」にアクセスします。

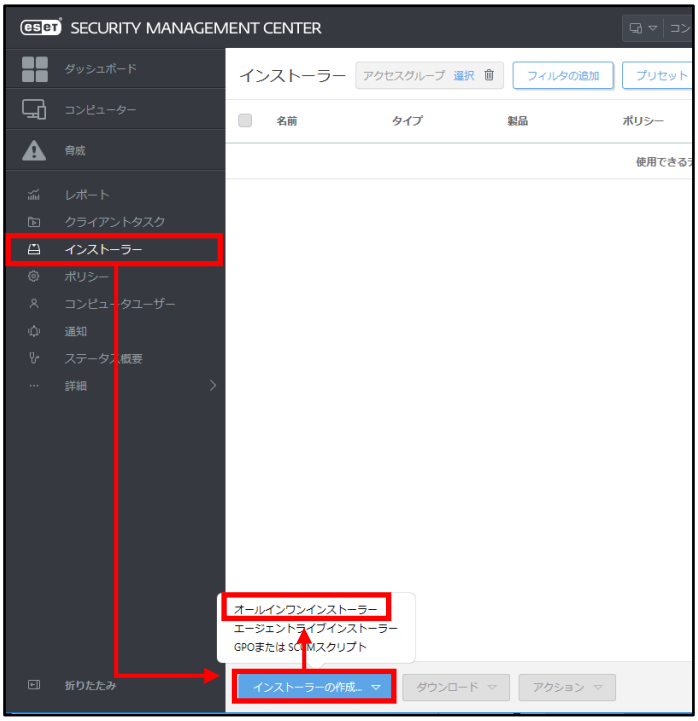
   以下の画面が表示されますので、「このサイトの閲覧を続行する（推奨されません）。」をクリックします。



※ ここでは、ESET Security Management Center 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。
※ お使いのブラウザより、表示内容が異なります。

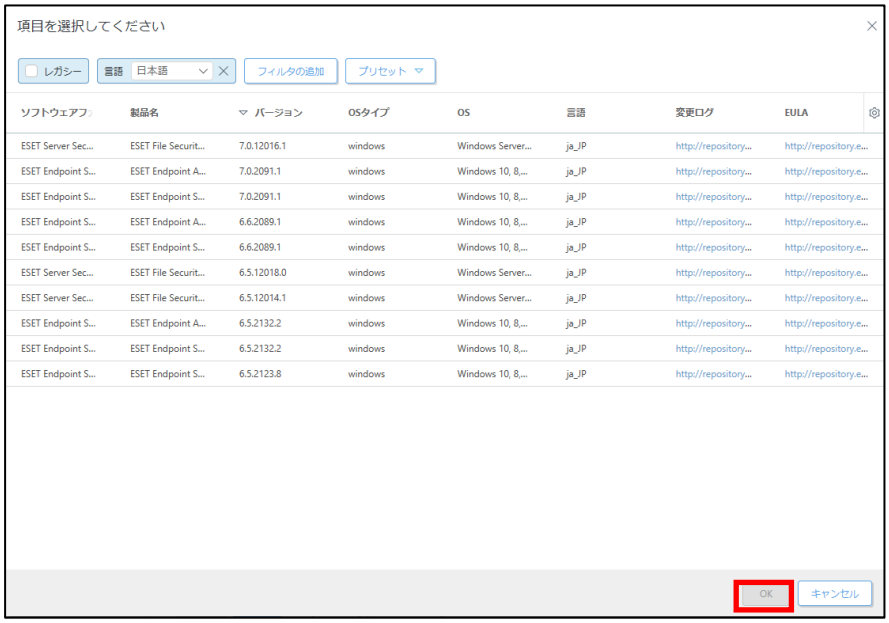
2. 「**3.6.ライセンス情報･ログイン情報の準備**」で確認した①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。
   ※ 初回ログイン時、また、パスワード有効期限が切れた場合は、画面の指示に従ってパスワード変更を行ってください。また、左下の「パスワード変更」から変更することも可能です。

3. 「インストーラー」→「インストーラーの作成」→「オールインワンインストーラー」をクリックします。

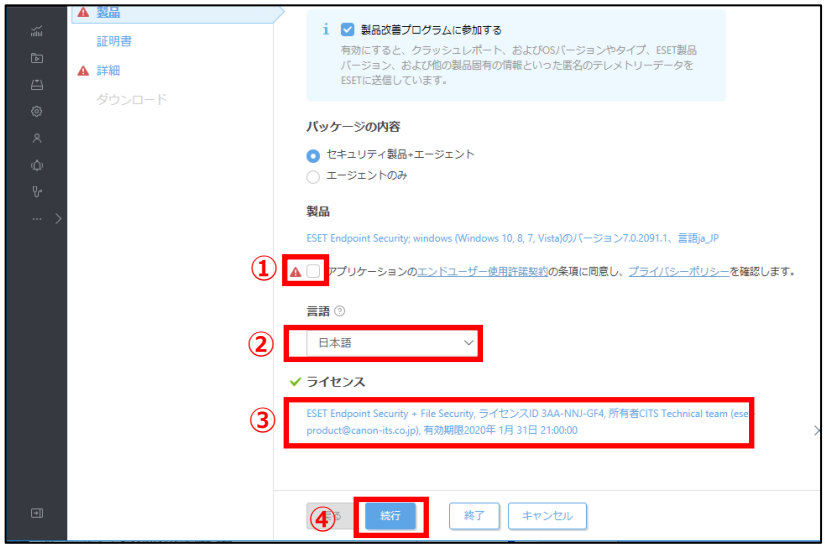


4. 「セキュリティ製品＋エージェント」を選択します。
製品にて、すでに設定されているクライアント用プログラムをクリックします。
※ 既定で設定されている製品は、登録したライセンスにより変わります。

5. インストールしたいクライアント用プログラムを選択して、「OK」ボタンをクリックします。

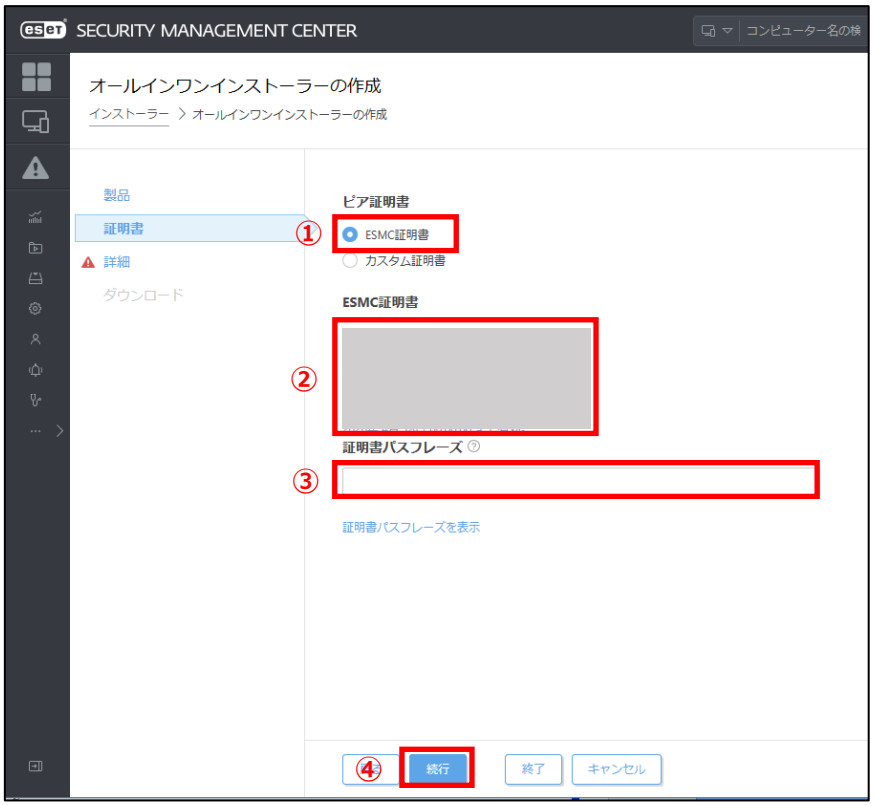


6. ①「アプリケーションエンドユーザー使用許諾契約に同意します」に**チェックを入れます**。
②「日本語」が選択されていることを確認します。
③「ライセンス（任意）」にライセンスが登録されていることを確認します。
④「続行」をクリックします。



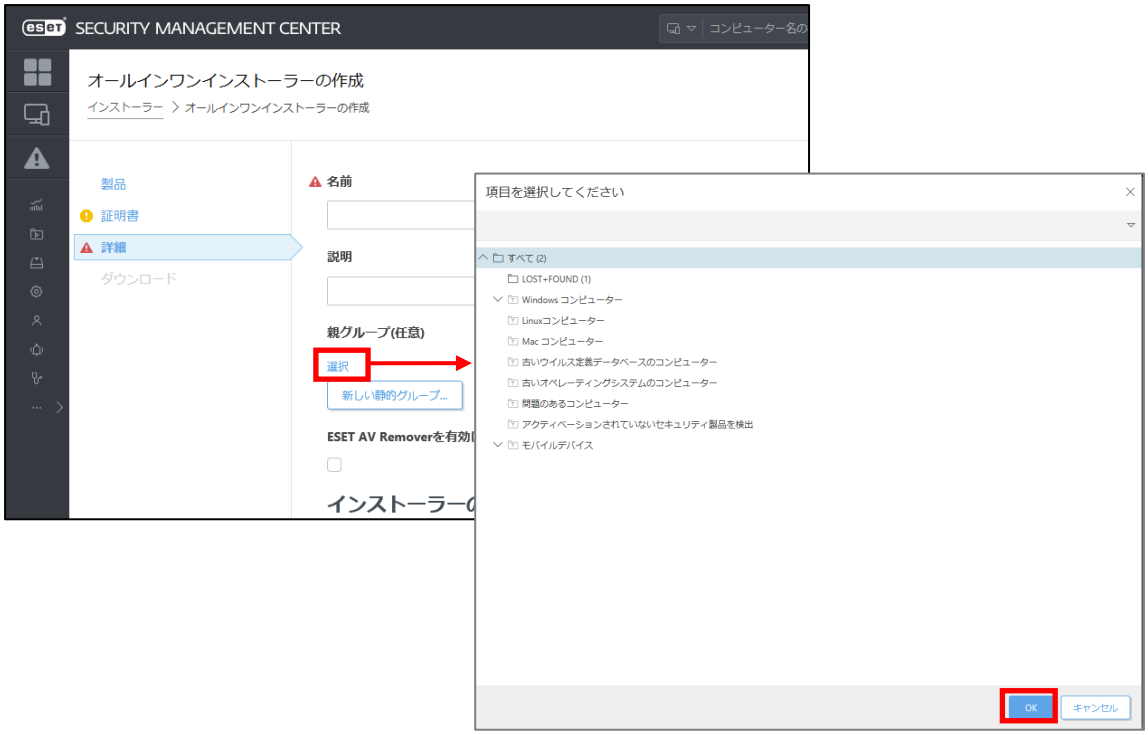
7. ①「ESMC 証明書」が選択されていることを確認します。
② ESMC 証明書に証明書が登録されていることを確認します。
③「証明書パスフレーズ」には、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「証明書パスフレーズ」を入力します。

⑤ 「続行」をクリックします。



8. 名前を入力します。
※ 説明の入力は任意です。

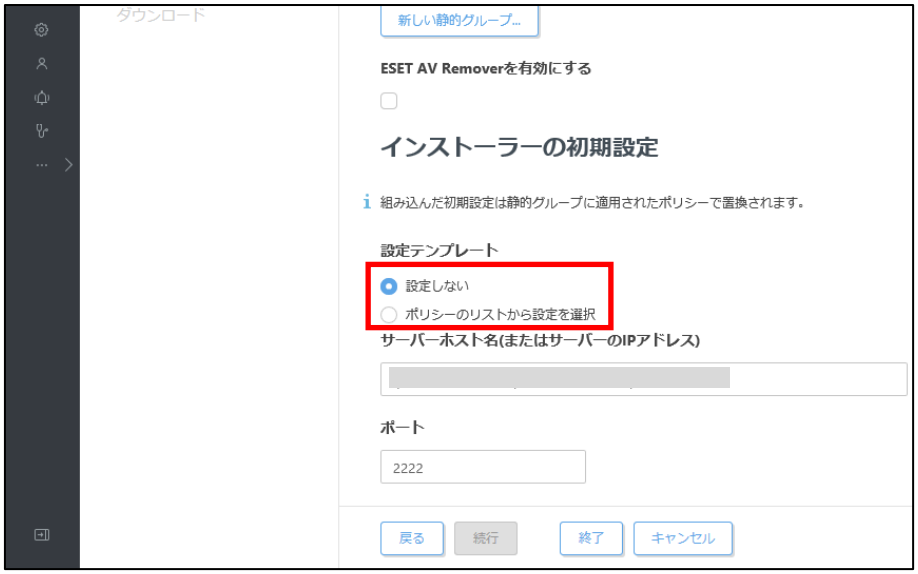
9. 「親グループ（任意）」を選択すると、インストール直後にクライアントが所属する静的グループを選択することができます。
※ 既定では「LOST+FOUND」グループに所属します。



10. [ESET AV Remover を有効にする]に**チェックが入っていない**ことを確認します。チェックが入っていた場合は外してください。

11. 「インストーラーの初期設定」の「設定テンプレート」では、以下を参考に設定します。

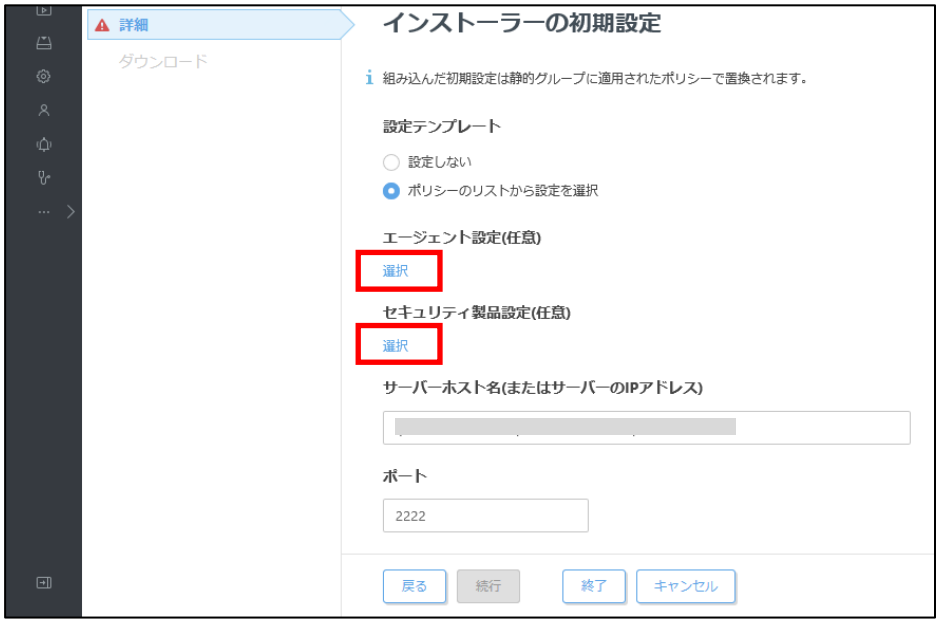
設定しない	既定の設定から変更せずに、クライアント端末にインストールする場合
ポリシーのリストから設定を選択	既存のポリシーを適用させて、クライアント端末にインストールする場合 ※HTTP プロキシを経由する場合はこちらを選択します。



新しいポリシーを作成する場合は、下記の WEB ページをご参照ください。
【ESET Security Management Center V7.0 を利用して、新しいポリシーを作成する手順】
https://eset-support.canon-its.jp/faq/show/11854?site_domain=business

12. 手順 11 で「ポリシーのリストから設定を選択」を選択した場合は、以下を参考に、「選択」をクリックし、EM エージェントとクライアント用プログラムに適用したいポリシーを選択して「OK」ボタンをクリックします。

エージェントの設定（任意）	クライアント端末にインストールする EM エージェントにポリシーを適用する場合に設定 ※HTTP プロキシを経由する場合は、＜事前準備＞ HTTP プロキシを経由する場合で作成した「HTTP プロキシ経由ポリシー（EM エージェント）」を選択します。
セキュリティ製品設定（任意）	クライアント端末にインストールするクライアント用プログラムにポリシーを適用する場合に設定 ※HTTP プロキシを経由する場合は、＜事前準備＞ HTTP プロキシを経由する場合で作成した「HTTP プロキシ経由ポリシー（クライアント）」を選択します。



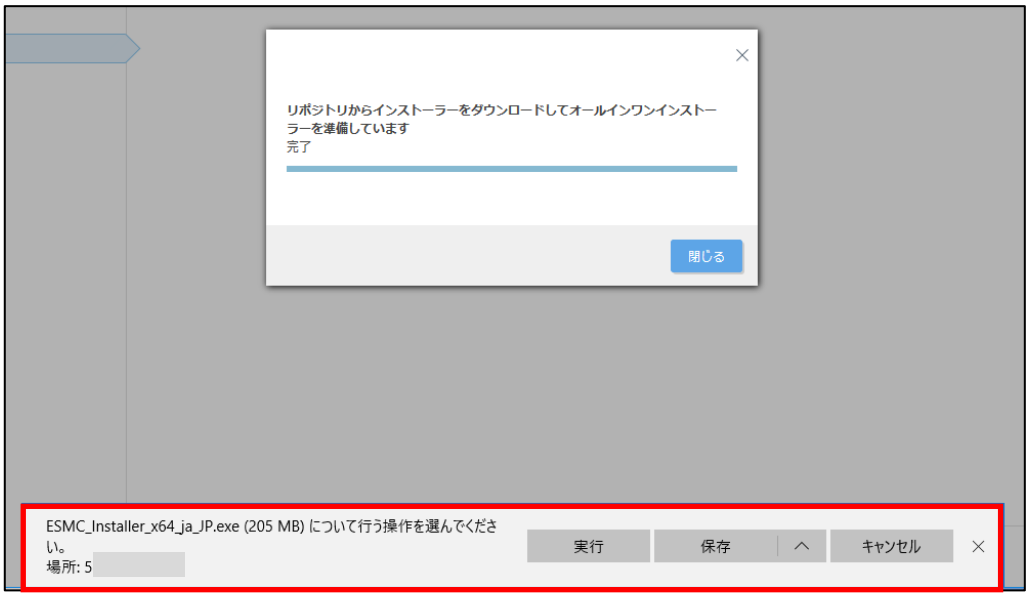
13. ①「サーバーホスト名（またはサーバーの IP アドレス）」に「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「ESMC サーバー/ERA サーバーの IP アドレス」を入力してください。
②「ポート」にポート番号「**2222**」が入力されていることを確認します。
③「終了」をクリックします。

14. 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]または「64bit 版をダウンロード」をクリックします。

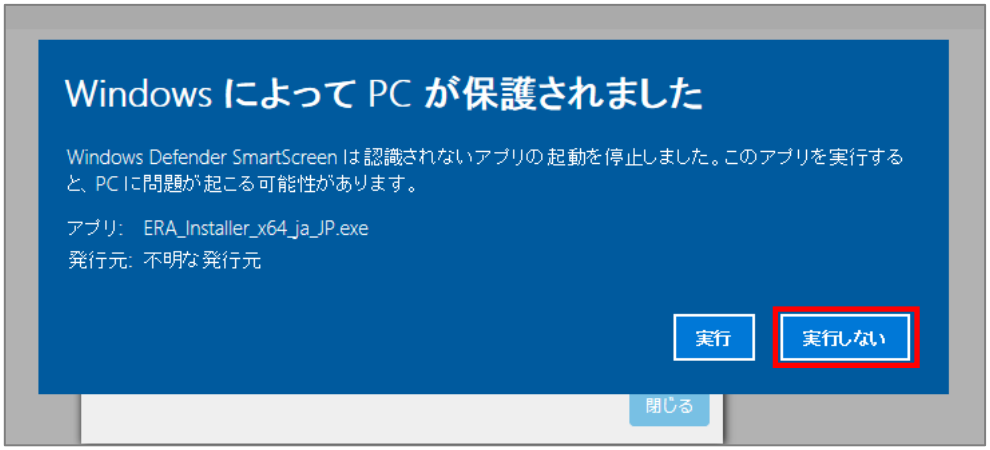
Point

ご利用のネットワーク環境によって、オールインワンインストーラーのダウンロードに時間がかかる場合があります。
プログレスバーが動かない場合でも、プログラムのダウンロードを行っていますので、しばらくお待ちください。

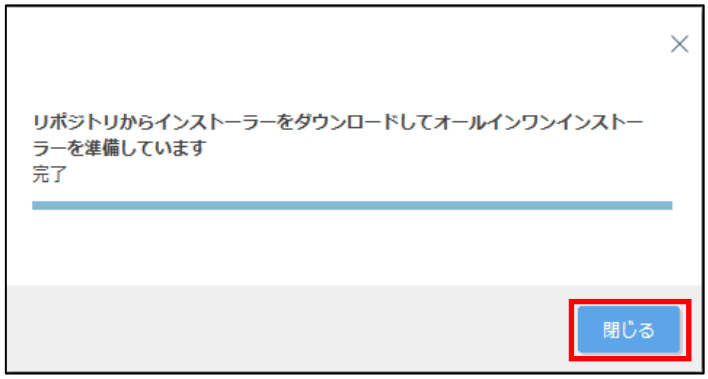
15. ファイルの保存を促す画面が表示されたら、任意の保存先を指定してインストーラーを保存します。
    ※　ファイル名は、32bit 用のオールインワンインストーラーの場合「ESMC_Installer_x86_ja_JP.exe」、64bit 用のオールインワンインストーラーの場合「ESMC_Installer_x64_ja_JP.exe」です。



16. 以下画面が表示されたら、「実行しない」を選択してください。



17. 終了したら「閉じる」ボタンをクリックします。



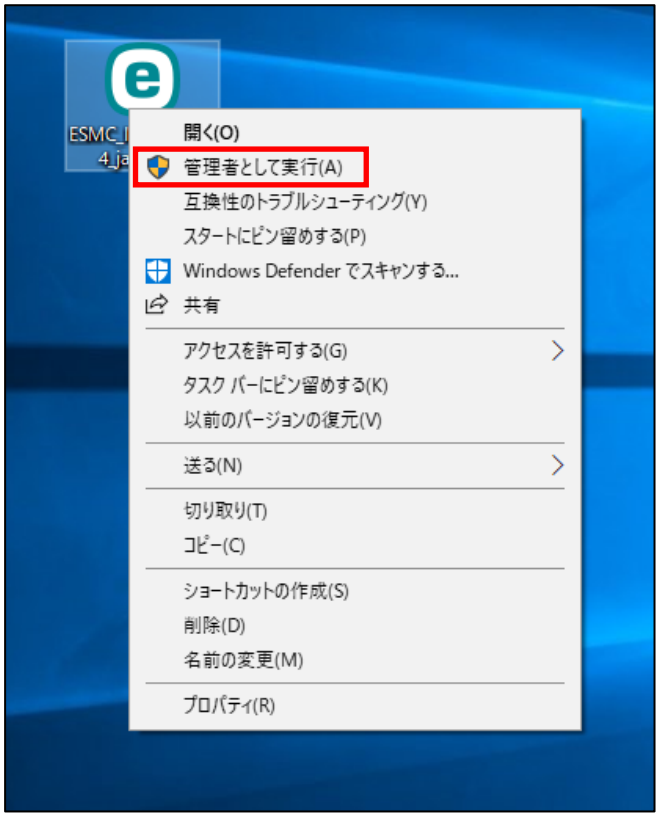
以上でオールインワンインストーラーの作成は完了です。
手順 15 で指定した場所に、オールインワンインストーラーが保存されていることを確認し、クライアントに配布してください。

A-1-2. オールインワンインストーラーの実行【クライアント側作業】

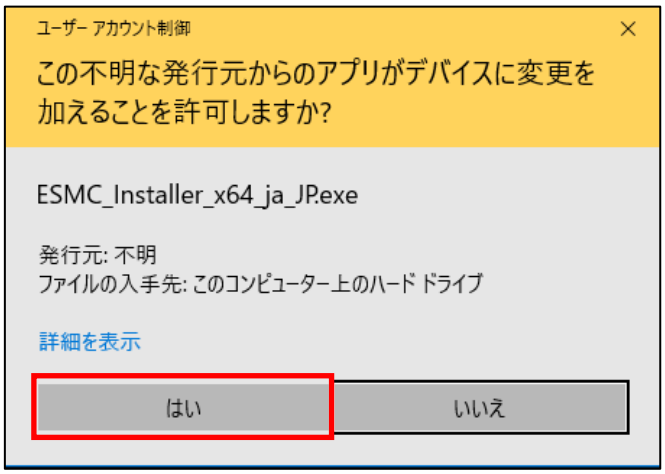
オールインワンインストーラーを各クライアント端末上で実行し、EM エージェントと ESET クライアント用プログラムをインストールします。

以下にオールインワンインストーラーの実行手順を記載します。

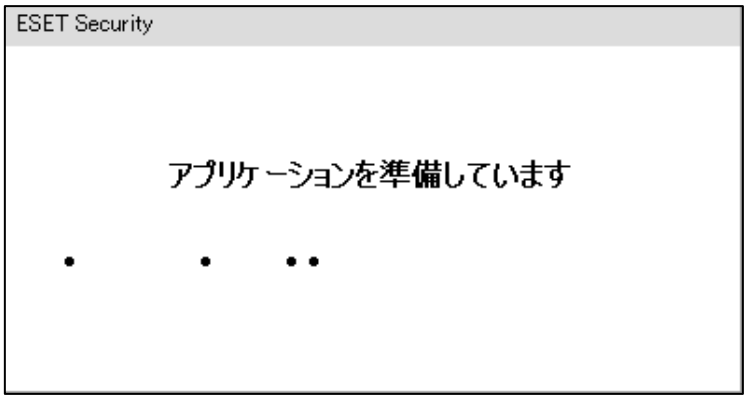
1. オールインワンインストーラーを右クリックより、「管理者として実行」をクリックします。



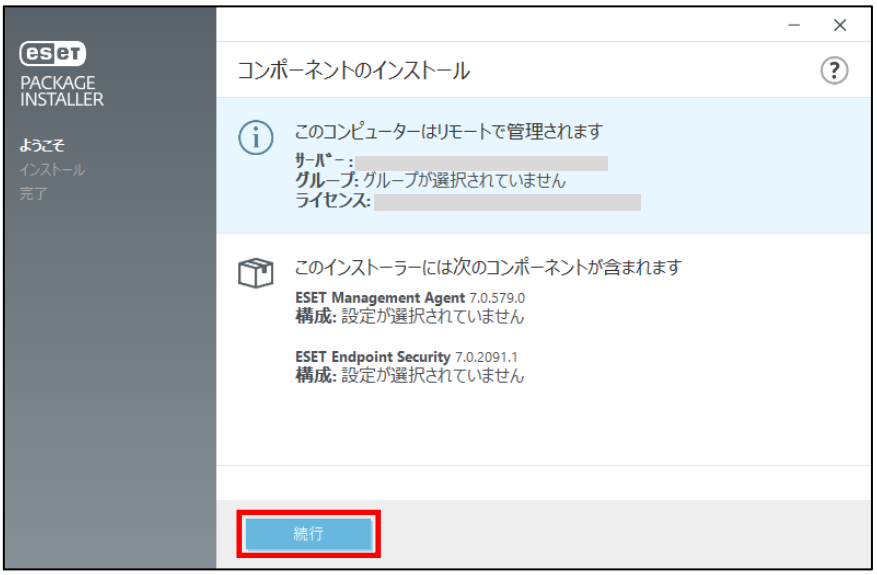
2. 「ユーザーアカウント制御」画面が表示された場合は、「はい」ボタンをクリックします。



3. 以下の画面が表示され、アプリケーションが起動します。



4. 「続行」ボタンをクリックします。

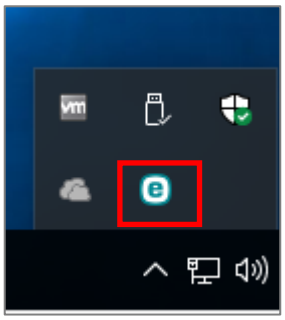


5. 「保護の設定」画面で、以下を参考に設定し、「インストール」ボタンをクリックします。

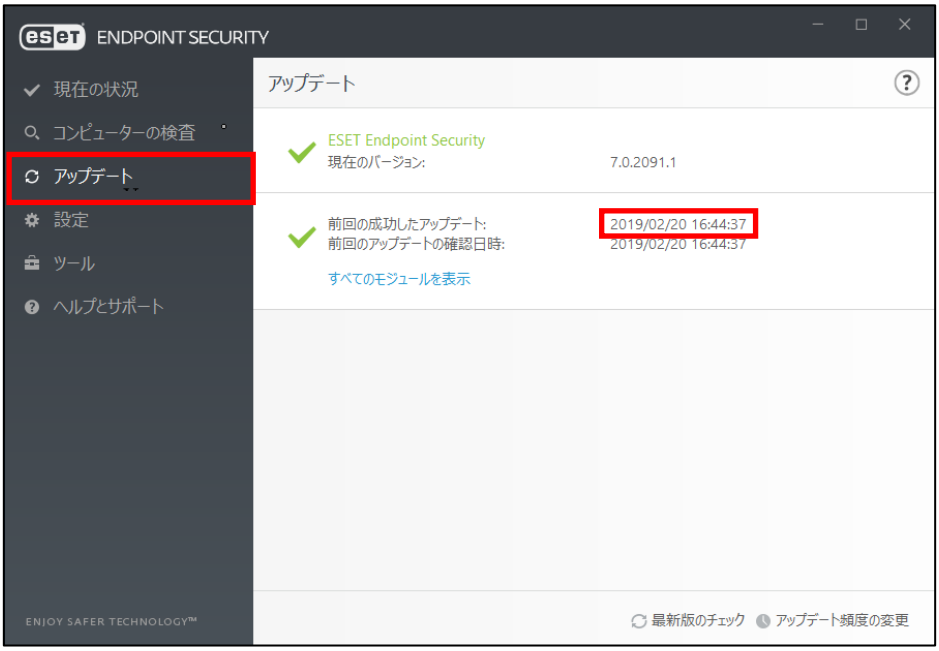
ESET LiveGrid フィードバックシステムを有効にする	チェックを入れると、本プログラムが新しい脅威を発見した場合に ESET 社へその情報を提出します。
望ましくない可能性のあるアプリケーションの検出	望ましくないアプリケーションの検出有無を選択します。 ※ ESET 製品は「不審なアプリケーション」を「望ましくない可能性のあるアプリケーション」として検出します。

6. 「インストール成功」画面が表示されたら、「完了」ボタンをクリックしてください。

7. タスクトレイの ESET アイコンをダブルクリックし、ESET のメイン画面が開きます。



8. 「アップデート」より、検出エンジンのアップデートが自動で開始され、「前回の成功したアップデート」に現在の時刻が入っていることを確認してください。
※初回アップデートが完了すると、コンピュータの検査が開始いたします。



以上でオールインワンインストーラーの実行は完了です。
続いて「7．クラウドオプションで管理ができていることを確認」に進んでください。

【既存お客様向け】

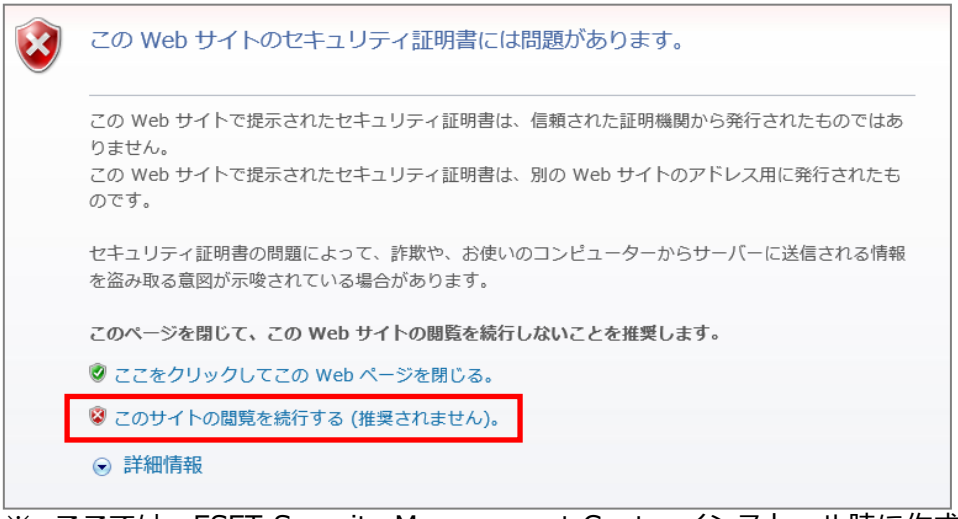
A-2-1. オールインワンインストーラー（EM エージェントのみ）の作成 【管理サーバー側作業】

クラウドオプションでクライアントの管理を行うためには、EM エージェントのインストールが必要です。すでに、クライアント用プログラムをご利用の方は ESMC で作成した EM エージェントインストール用の exe ファイルを実行することでクラウドオプションで管理を行うことが可能です。

以下に、オールインワンインストーラー（EM エージェントのみ）の作成手順を記載します。

1. Web ブラウザより、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「Web コンソール（管理画面）ログイン用 URL」にアクセスします。

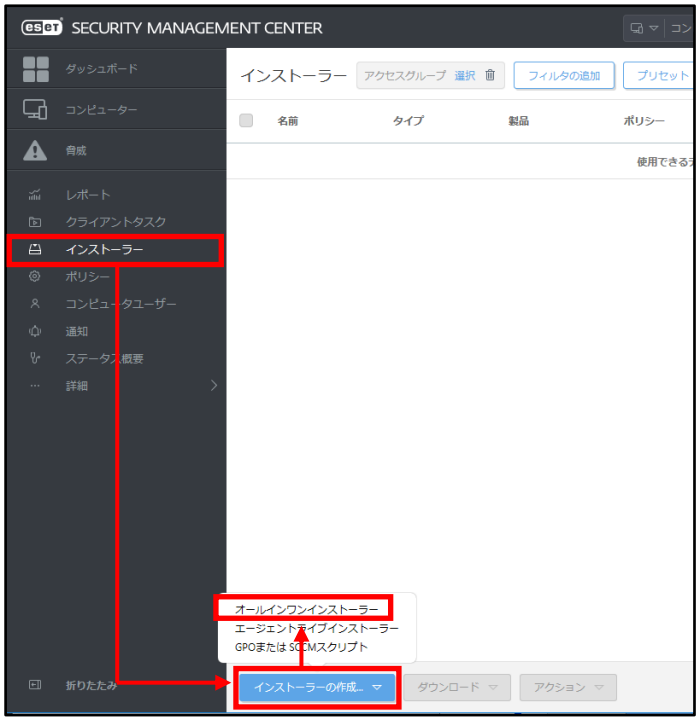
   以下の画面が表示されますので、「このサイトの閲覧を続行する（推奨されません）。」をクリックします。



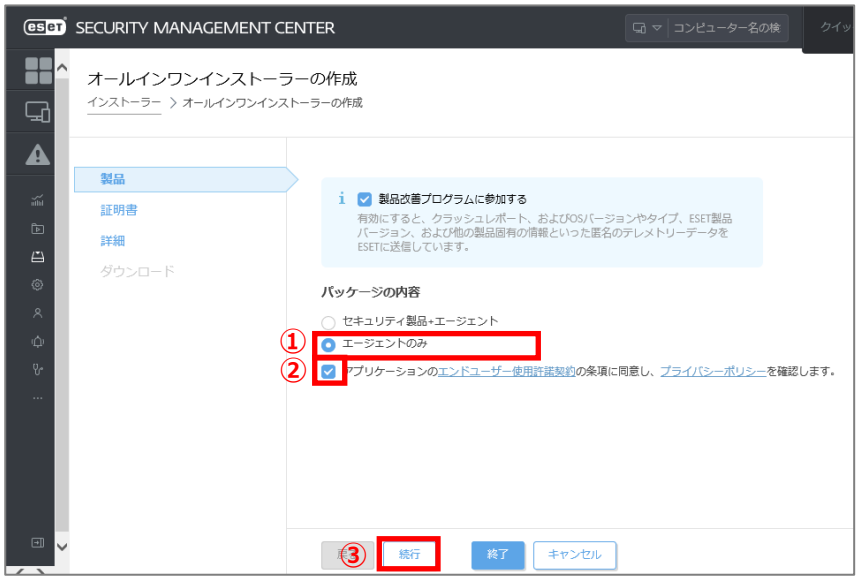
※ ここでは、ESET Security Management Center インストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
※ お使いのブラウザより、表示内容が異なります。

2. 「**3.6.ライセンス情報･ログイン情報の準備**」で確認した①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。

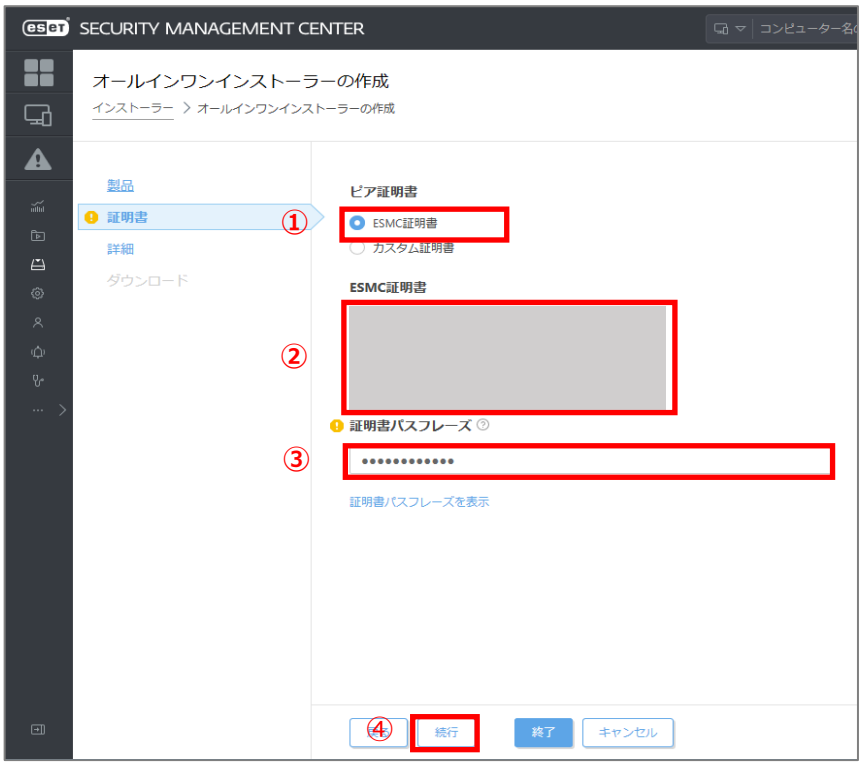
3. 左メニューより、「インストーラー」→「インストーラーの作成」→「オールインワンインストーラー」をクリックします。



4. ①「エージェントのみ」を選択します。
②「アプリケーションエンドユーザー使用許諾契約に同意します」に**チェックを入れます**。
③「続行」をクリックします。

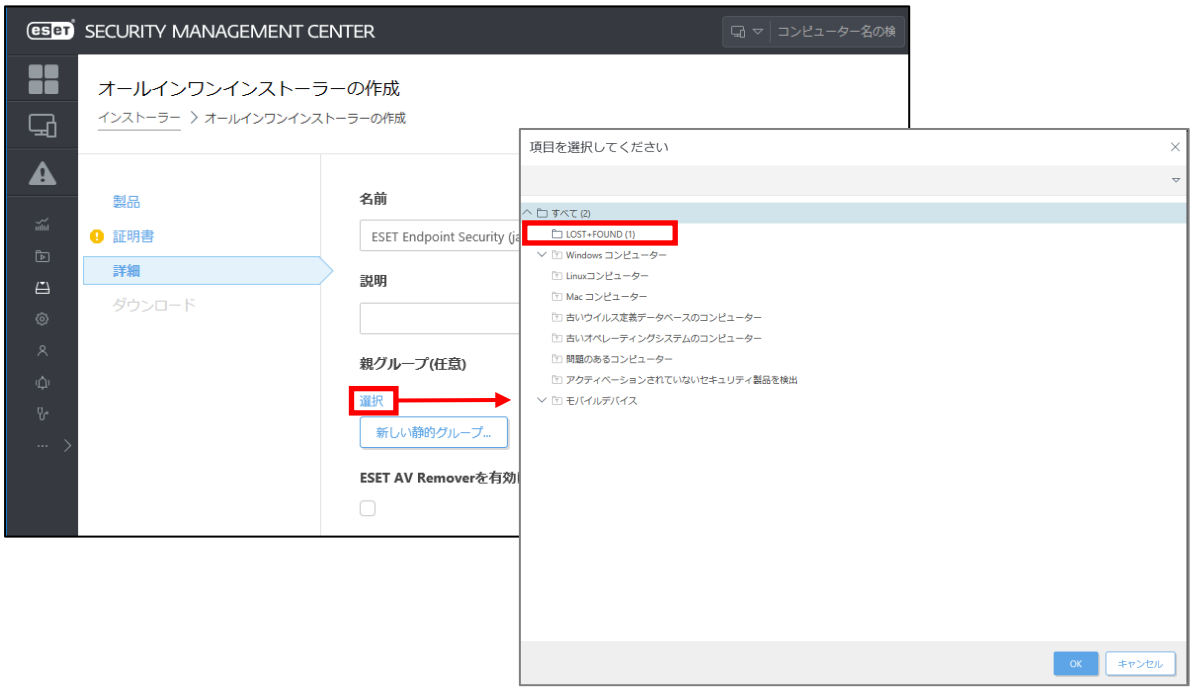


5. ①「ESMC 証明書」が選択されていることを確認します。
② ESMC 証明書に証明書が登録されていることを確認します。
③「証明書パスフレーズ」には、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「証明書パスフレーズ」を入力します。
④「続行」をクリックします。



6. 名前を入力します。
   ※説明の入力は任意です。

7. 「親グループ（任意）」を選択すると、インストール直後にクライアントが所属する静的グループを選択することができます。
   ※ 既定では「LOST+FOUND」グループに所属します。



8. [ESET AV Remover を有効にする]に**チェックが入っていない**ことを確認します。チェックが入っていた場合は外してください。

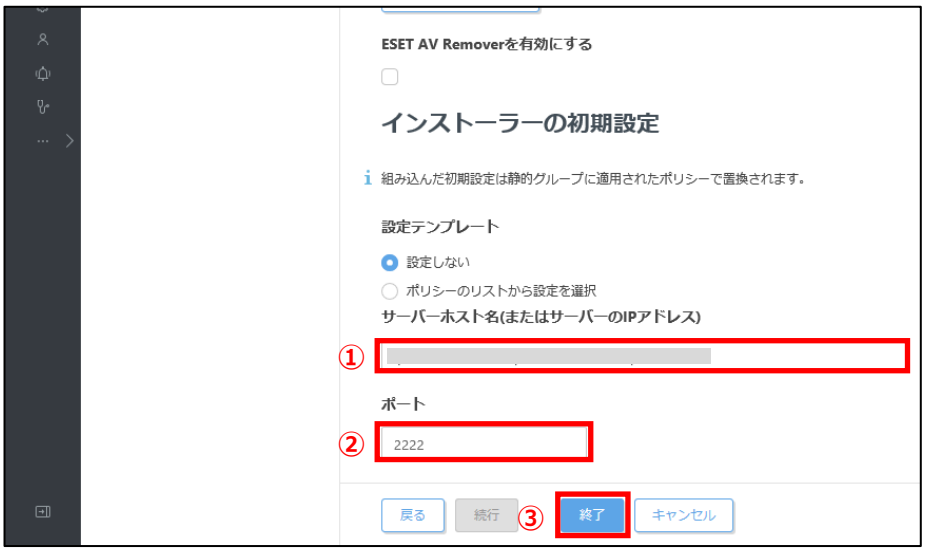
9. 「インストーラーの初期設定」の「設定テンプレート」では、以下を参考に設定します。

設定しない	既定の設定から変更せずに、クライアント端末にインストールする場合
ポリシーのリストから設定を選択	既存のポリシーを適用させて、クライアント端末にインストールする場合 ※HTTP プロキシを経由する場合は、こちらを選択します。

10. 手順 9 で「ポリシーのリストから設定を選択」を選択した場合は、以下を参考に、「選択」をクリックし、EM エージェントのポリシーを選択して「OK」ボタンをクリックします。

エージェントの設定（任意）	クライアント端末にインストールする EM エージェントにポリシーを適用する場合に設定 ※HTTP プロキシを経由する場合は、＜事前準備＞HTTP プロキシを経由する場合で作成した「HTTP プロキシ経由ポリシー（EM エージェント）」を選択します。

11. ①「サーバーホスト名（またはサーバーの IP アドレス）」に「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「ESMC サーバー/ERA サーバーの IP アドレス」を入力してください。
②「ポート」にポート番号「**2222**」が入力されていることを確認します。
③「終了」をクリックします。

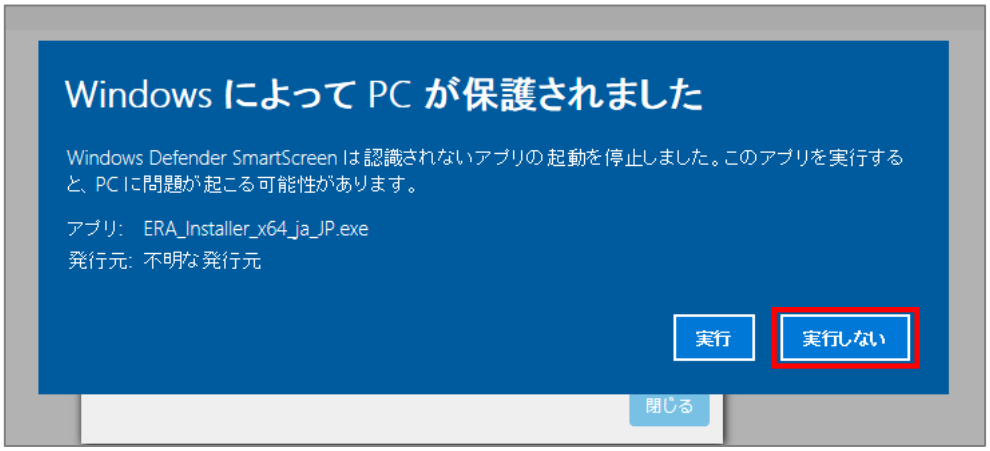


12. インストールするクライアント端末の環境にあわせて、[32bit 版をダウンロード]または「64bit 版をダウンロード」をクリックします。

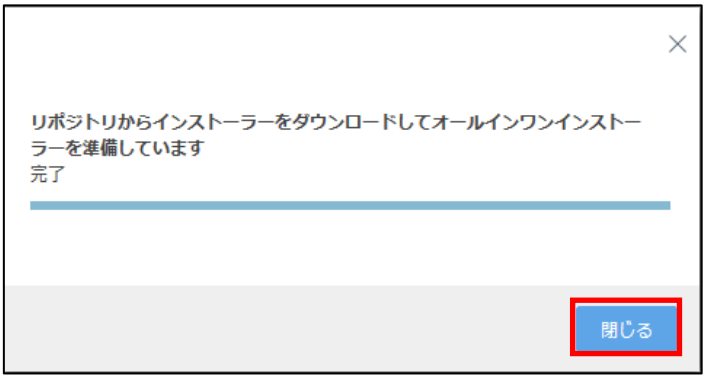
13. ファイルの保存を促す画面が表示されたら、任意の保存先を指定してインストーラーを保存します。
    ※ ファイル名は、32bit 用のオールインワンインストーラーの場合「ESMC_Installer_x86.exe」、64bit 用のオールインワンインストーラーの場合「ESMC_Installer_x64.exe」です。

ご利用のネットワーク環境によって、オールインワンインストーラーのダウンロードに時間がかかる場合があります。
プログレスバーが動かない場合でも、プログラムのダウンロードを行っていますので、しばらくお待ちください。

14. 以下の画面が表示されたら、「実行しない」を選択してください。



15. 終了したら「閉じる」ボタンをクリックします。



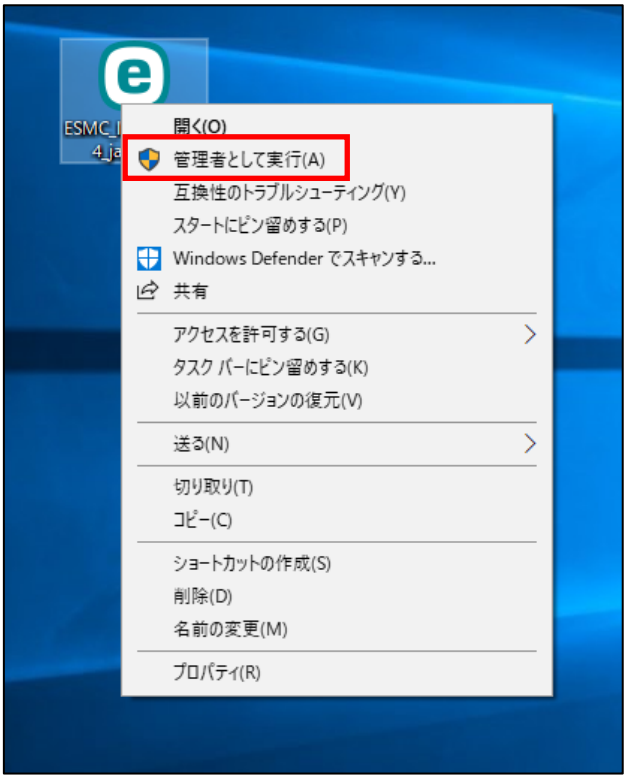
以上でオールインワンインストーラーの作成は完了です。
手順 13 で指定した場所に、オールインワンインストーラーが保存されていることを確認し、クライアントに配布してください。

A-2-2. オールインワンインストーラー（EM エージェントのみ）の実行 【クライアント側作業】

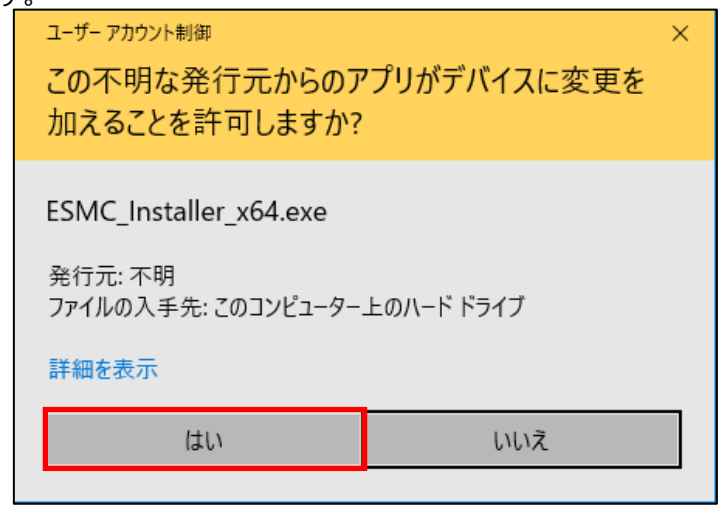
オールインワンインストーラーを各クライアント端末上で実行し、EM エージェントをインストールします。

以下にオールインワンインストーラーの実行手順を記載します。

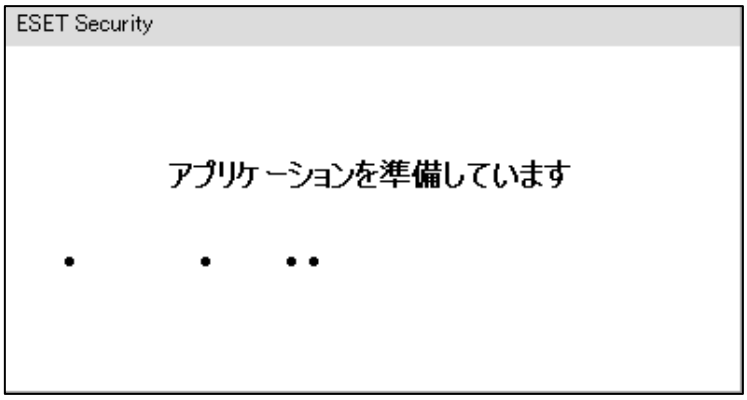
1. オールインワンインストーラーを右クリックより、「管理者として実行」をクリックします。



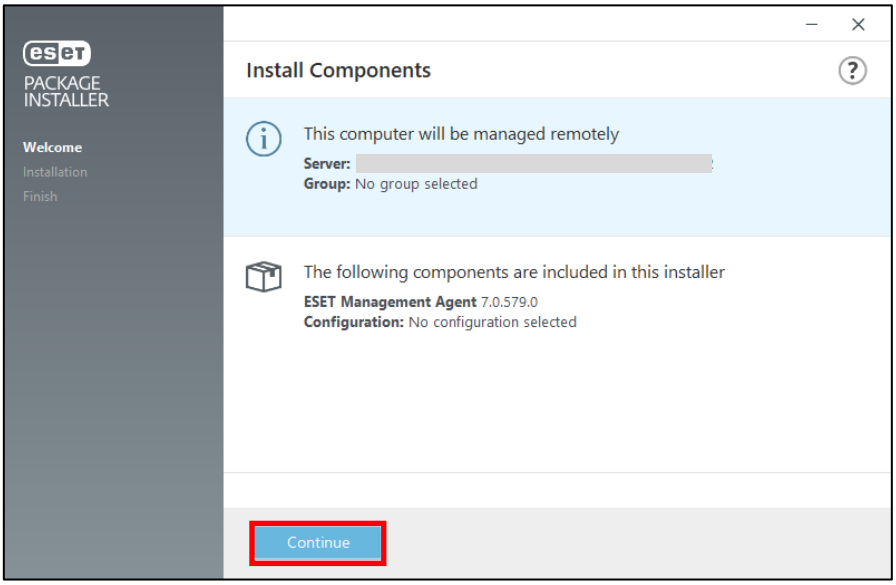
2. 「ユーザーアカウント制御」画面が表示された場合は、「はい」ボタンをクリックします。



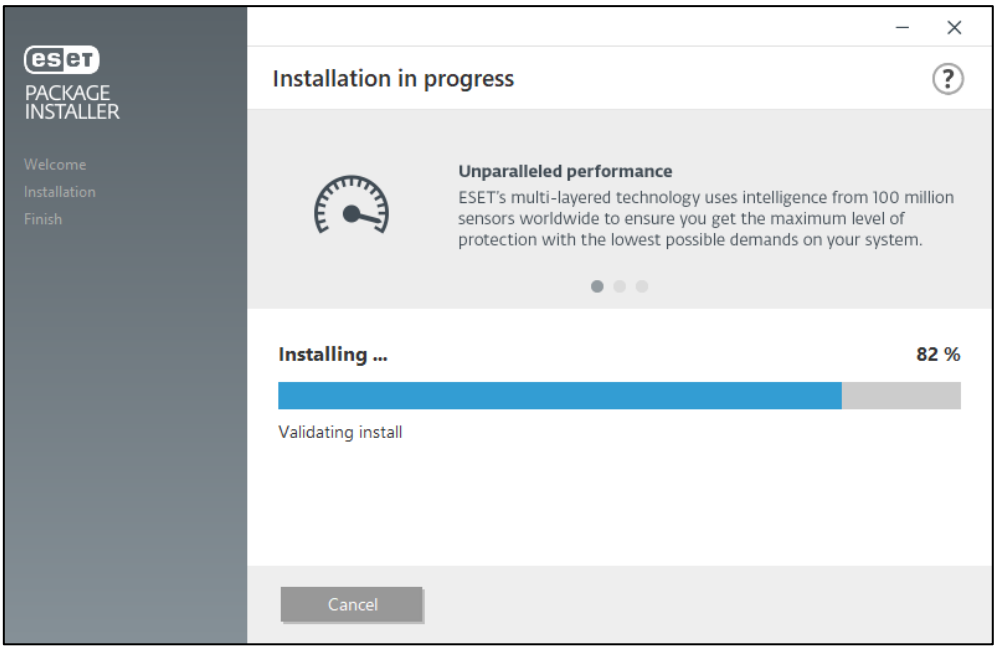
3. 以下の画面が表示され、アプリケーションが起動します。



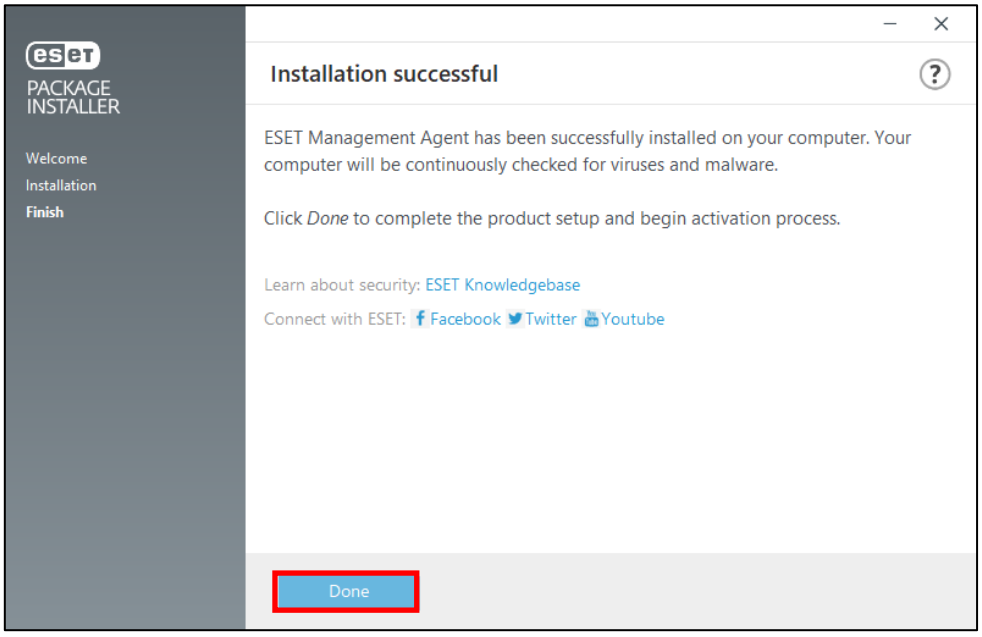
4. 「Continue」をクリックします。



5. 以下のような画面が表示され、自動的にインストールが進みます。



6. 「Installation successful」画面が表示されたら、「Done」ボタンをクリックしてください。



以上で、EM エージェントのインストールは完了です。
続いて、「7. クラウドオプションで管理ができていることを確認」に進んでください。

B）Mac、Linux 端末への展開

【新規お客様向け】

クライアント用プログラムがインストールされていない

【既存お客様向け】

すでにクライアント用プログラムはインストールされている

B-1-1. クライアント用プログラムのインストール【クライアント側作業】

ESET クライアント用プログラムを各クライアント端末上で実行します。

⇩

B-1-2. エージェントライブインストーラーの作成【管理サーバー側作業】

「EM エージェント」をインストールするためのエージェントライブインストーラーを ESMC で作成します。プログラム作成後はクライアント端末に配布します。

⇩

＜事前準備＞HTTP プロキシを経由する場合【管理サーバー側作業】

HTTP プロキシ経由で ESMC へ接続する場合、EM エージェントとクライアントプログラムの両プログラムに対して、HTTP プロキシ経由するための設定を行います。
HTTP プロキシを経由しない場合は、本手順は必要ございません。
下記の手順に進んでください。

⇩

B-1-3. エージェントライブインストーラーの実行【クライアント側作業】

インストールが完了すると、クラウドオプションの ESMC と通信が自動的に行われます。

⇩

7. クラウドオプションで管理ができていることを確認【管理サーバー側作業】

Web ブラウザからクラウドオプションの ESMC にアクセスし、クライアントの管理状況を確認します。

B-1-1. クライアント用プログラムのインストール【クライアント側作業】

各クライアント端末に ESET クライアント用プログラムをインストールします。

インストール方法につきまして、ユーザーズサイトよりダウンロード可能な各プログラムのユーザーズマニュアルをご参照ください。

クラウドオプションの ERA のソフトウェアインストールタスクを利用して、クライアントプログラムをリモートでインストールすることも可能です。
実施手順につきまして、以下の Web ページをご参照ください。
※先に EM エージェントを導入する必要がございます。
【【V6.2 以降】クライアント管理用プログラムに搭載されているソフトウェアインストールタスクを使用して、クライアント用プログラムをリモートインストールするには？】
https://eset-support.canon-its.jp/faq/show/5165?site_domain=business

【HTTP プロキシを経由する場合】
インターネット接続にプロキシサーバーを経由する場合は、以下参照しプロキシサーバー設定を行ってください。
詳細は、各プログラムのユーザーズマニュアルをご参照ください。

◆Mac クライアント用プログラム
「詳細設定」→「プロキシサーバー」

◆Linux サーバー用プログラム
Web インターフェースより、「Configuration」→「Grobal」→「Deamon options」→「Proxy address」と「Proxy port」

◆Linux クライアント用プログラム
「詳細設定」→「その他」→「プロキシサーバー」

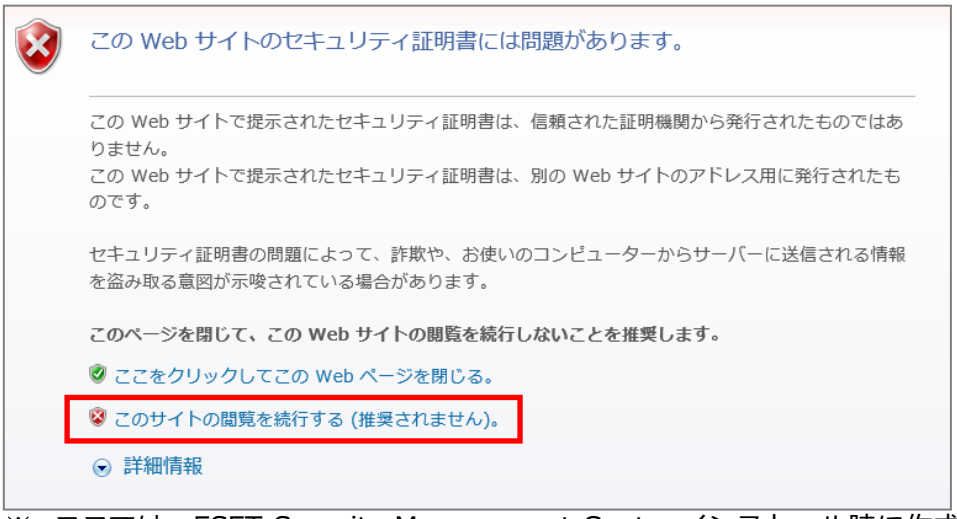
B-1-2. エージェントライブインストーラーの作成【管理サーバー側作業】

クラウドオプションでクライアントの管理を行うためには、クライアント用プログラムのほかに EM エージェントのインストールが必要です。EM エージェントをインストールするには、EM エージェントインストール用の bat ファイル「エージェントライブインストーラー」を利用します。

以下に、エージェントライブインストーラーの作成手順を記載します。

1. Web ブラウザより、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「Web コンソール（管理画面）ログイン用 URL」にアクセスします。

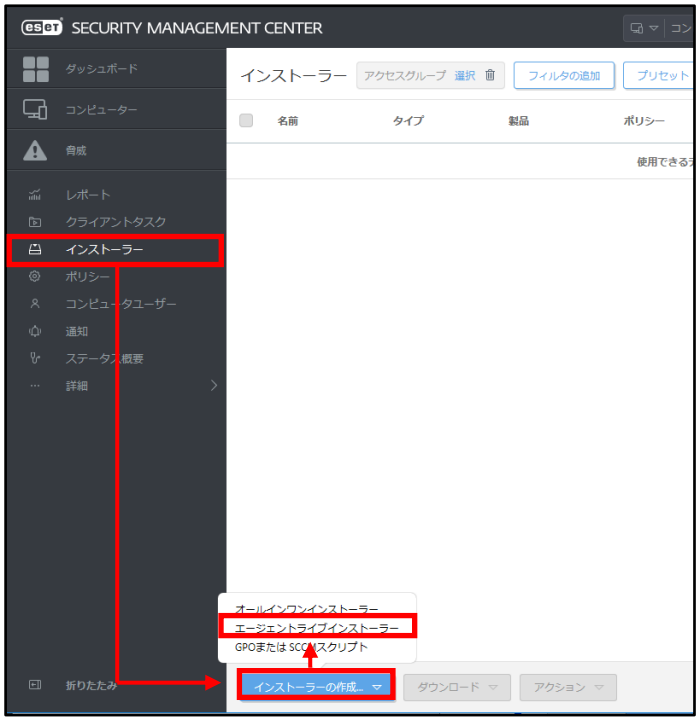
   以下の画面が表示されますので、「このサイトの閲覧を続行する（推奨されません）。」をクリックします。



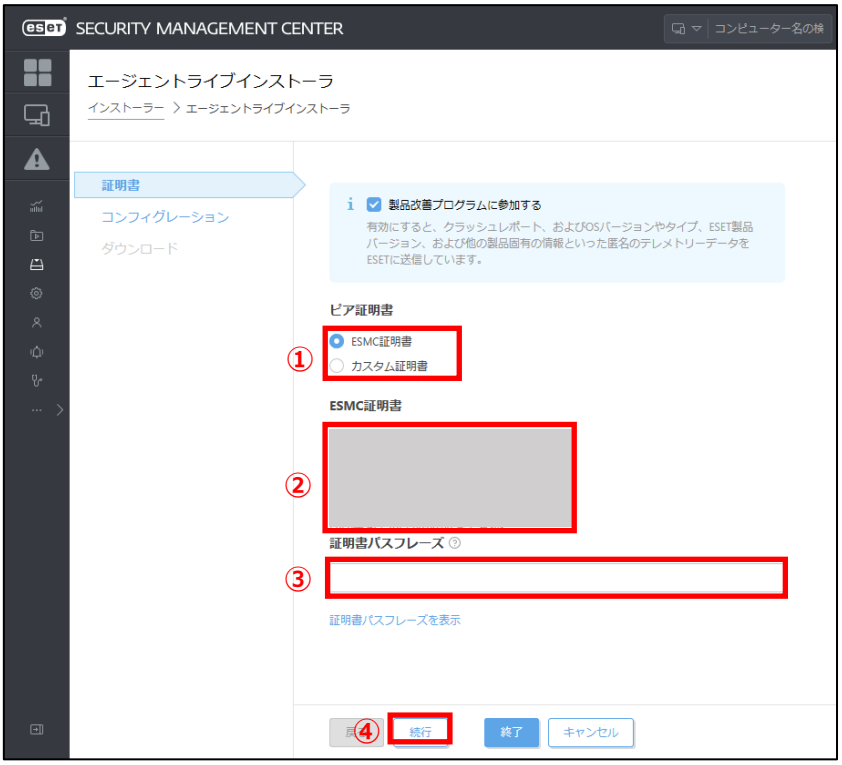
※ ここでは、ESET Security Management Center インストール時に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
※ お使いのブラウザより、表示内容が異なります。

2. 「**3.6.ライセンス情報･ログイン情報の準備**」で確認した①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。

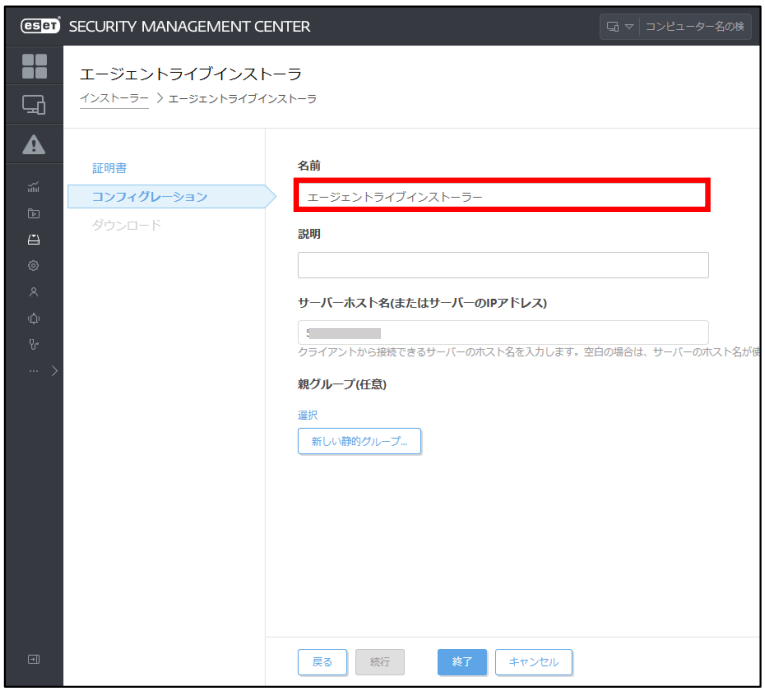
3. 左メニューより、「インストーラー」→「インストーラーの作成」→「エージェントライブインストーラー」をクリックします。



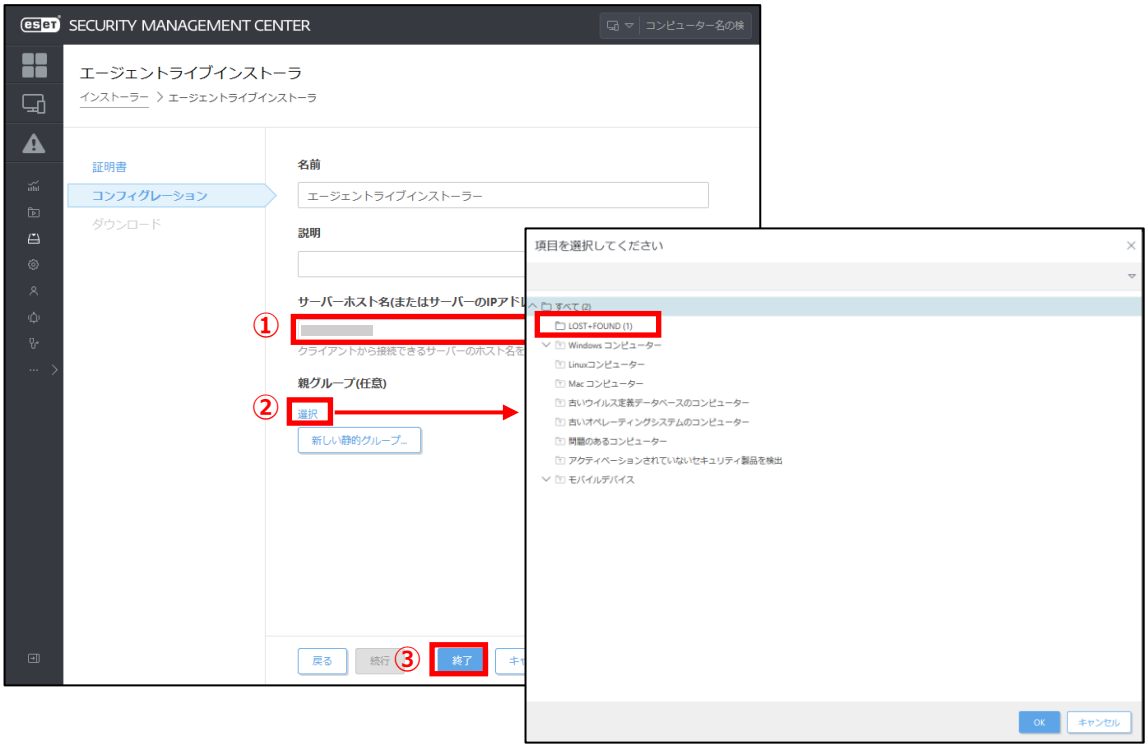
4. ①「ESMC 証明書」が選択されていることを確認します。
② ESMC 証明書に証明書が登録されていることを確認します。
③「証明書パスフレーズ」には、「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「証明書パスフレーズ」を入力します。
④「続行」をクリックします。



5. 名前を入力します。
※説明の入力は任意です。



6. ①「サーバーホスト名（またはサーバーの IP アドレス）」に「**3.6.ライセンス情報・ログイン情報の準備**」で確認した「ESMC サーバー/ERA サーバーの IP アドレス」を入力してください。
②「親グループ（任意）」を選択すると、インストール直後にクライアントが所属する静的グループを選択することができます。
※ 既定では「LOST+FOUND」グループに所属します
③「終了」をクリックします。



7. ご利用の OS に応じて、「Linux 用エージェントインストーラ」または「Mac 用エージェントインストーラ」をダウンロードします。
※「ESMCAgentInstaller.tar.gz」がダウンロードされます。

ダウンロードが完了したら、各クライアントに配布し実行します。

＜事前準備＞HTTP プロキシを経由する場合【管理サーバー側作業】

各クライアントが HTTP プロキシを経由してクラウドオプションの ESMC に接続する場合は、エージェントライブインストーラーにプロキシ設定を行います。

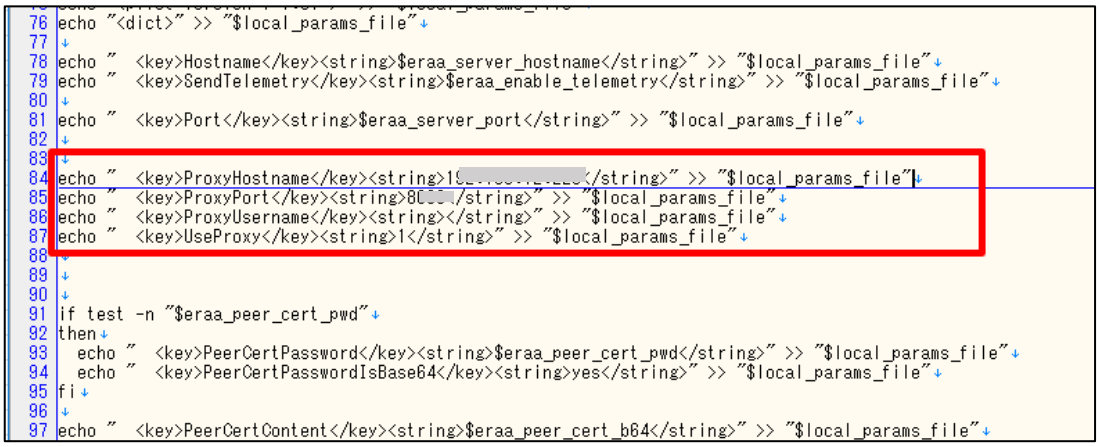
HTTP プロキシを経由しない場合は、「**B-1-3.エージェントライブインストーラーの実行**」に進んでください。

【HTTP プロキシを経由する場合、エージェントライブインストーラー変更方法】

◆Mac 用エージェントライブインストーラー

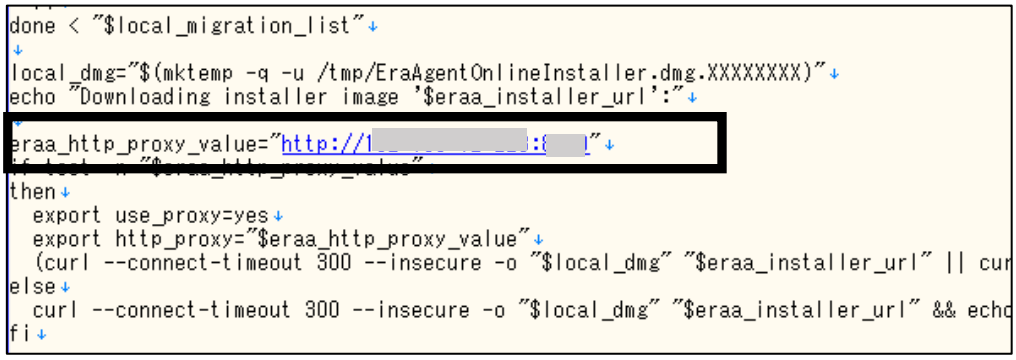
1. 「ESMCAgentInstaller.tar.gz」を展開し、ESMCAgentInstaller.sh に以下を追記します。

```
echo "  <key>ProxyHostname</key><string>プロキシサーバーの IP アドレス</string>" >> "$local_params_file"
echo "  <key>ProxyPort</key><string>プロキシサーバーのポート</string>" >> "$local_params_file"
echo "  <key>ProxyUsername</key><string></string>" >> "$local_params_file"
echo "  <key>UseProxy</key><string>1</string>" >> "$local_params_file"
```



2. さらに、以下を変更します。

```
eraa_http_proxy_value="http://プロキシサーバーの IP アドレス:ポート"
```



3. 設定を保存し、クライアントに配布します。

◆Linux 用エージェントライブインストーラー

1. 「ESMCAgentInstaller.tar.gz」を展開し、ESMCAgentInstaller.sh に以下を追記します。

```
--proxy-hostname=プロキシサーバーの IP アドレス ¥
--proxy-port=ポート ¥
```

※ ¥かバックスラッシュかはエディタによって表示が変わります。

```
export _ERAAGENT_PEER_CERT_PASSWORD="$eraa_peer_cert_pwd"

echo
echo Running installer script $local_installer
echo

$usesudo /bin/sh "$local_installer"\
   --skip-license \
   --hostname "$eraa_server_hostname"\
   --port "$eraa_server_port"\
   --proxy-hostname=1[redacted] \
   --proxy-port=8[redacted] \
   --cert-path "$local_cert_path"\
   --cert-password "env:_ERAAGENT_PEER_CERT_PASSWORD"\
   --cert-password-is-base64\
   --initial-static-group "$eraa_initial_sg_token"\
   --disable-imp-program\
   $(test -n "$local_ca_path" && echo --cert-auth-path "$local_ca_path")\
   $(test -n "$eraa_product_uuid" && echo --product-guid "$eraa_product_uuid")\
   $additional_params
```

2. さらに、以下を変更します。

```
eraa_http_proxy_value="http://プロキシサーバーの IP アドレス:ポート"
```

```
fi

local_installer="$(mktemp -q -u)"

eraa_http_proxy_value="http://1[redacted]:8[redacted]"
if test -n "$eraa_http_proxy_value"
then
  export use_proxy=yes
  export http_proxy="$eraa_http_proxy_value"
  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "
--no-proxy --no-check-certificate -O "$local_installer" "$eraa_installer_url
"$eraa_installer_url" > "$local_installer") && echo "$local_installer" >> "$
else
```

3. 設定を保存し、クライアントに配布します。

以上で、HTTP プロキシ経由する場合のエージェントライブインストーラー変更作業は完了です。

B-1-3. エージェントライブインストーラーの実行【クライアント側作業】

エージェントライブインストーラーを各クライアント端末上で実行し、EM エージェントをインストールします。

実行手順につきましては、ユーザーズサイトからダウンロード可能な「ESET Security Management Center V7.0 ユーザーズマニュアル」の P224「エージェントライブインストーラーの実行」より、使用する OS の実行方法をご参照ください。

以上で、EM エージェントインストールは完了です。

続いて「7. クラウドオプションで管理ができていることを確認」に進んでください。

C）Android OS、iOS デバイスへの展開

C-1. Mobile Device Connector のアクティベーション【管理サーバー側作業】】

Android OS、iOS のモバイルデバイスを管理するためのコンポーネント「Mobile Device Connector」のアクティベーションを行います。

⇩

C-2. APN 証明書の作成と登録用ポリシーの作成【管理サーバー側作業】

APN 証明書の作成と、iOS モバイルデバイス登録用ポリシーを作成します。
※iOS のモバイルの管理を行う方のみ必要な作業となります。

⇩

C-3. モバイルデバイスの登録【管理サーバー側作業】

管理する Android OS、iOS のモバイルデバイス情報を、事前に ESMC に登録します。事前に各モバイルデバイスの「電子メールアドレス」と「デバイス名」を記載した CSV ファイルをご用意ください。
登録を行うとモバイルデバイス利用者に登録用リンクのメールが送信されます。

⇩

C-4. クライアント用プログラムの展開【クライアント端末側作業】

メールにて送信された登録用リンクをクリックして、「ESET Endpoint Security for Android」または「ESET iOS Management profile」を各モバイルデバイスに展開します。
※ESET iOS Management profile にウイルス対策機能はございません。

D）Android OS デバイスへ「ESET Endpoint Security for Android」の展開
E）iOS デバイスへ「ESET iOS Management profile」の展開

⇩

C-5. 管理サーバーパスワード適用ポリシーの作成【管理サーバー側作業】

各 Android OS のモバイルデバイスに管理者パスワード設定を行います。

⇩

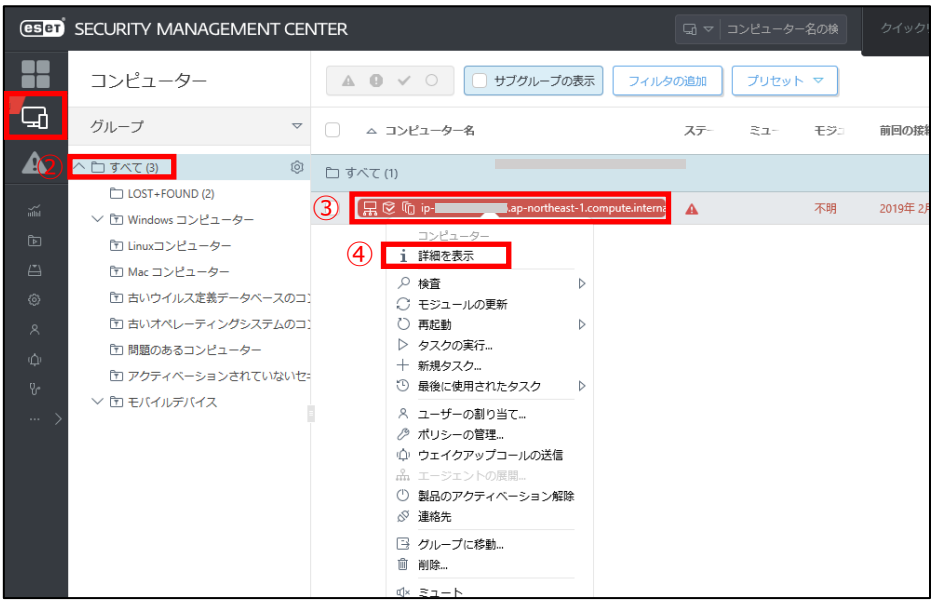
7. クラウドオプションで管理ができていることを確認【管理サーバー側作業】

C-1. Mobile Device Connector のアクティベーション【管理サーバー側作業】】

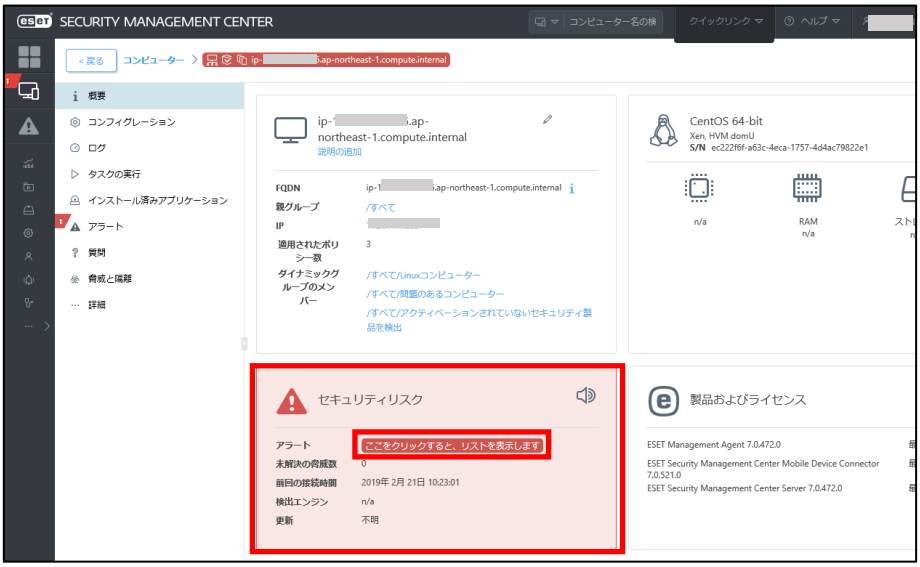
モバイルデバイスを管理するためのコンポーネント「Mobile Device Connector（以下、MDC）」のアクティベーションを行います。

以下の手順を実施し、MDC のアクティベーションを行ってください。

1. 左メニューの①「コンピューター」、②「すべて」をクリックし、 ③「ESMC サーバー <ip-172-31-xxx-xxx.ap-northeast-1.compute.internal>」→ ④「詳細を表示」をクリックします。
   ※「172-31-xxx-xxx」は、お客さまによって異なります。



2. 「セキュリティリスク」の「ここをクリックすると、リスクを表示します」をクリックします。



3. コンピュータの詳細が、下記の通りであることを確認します。

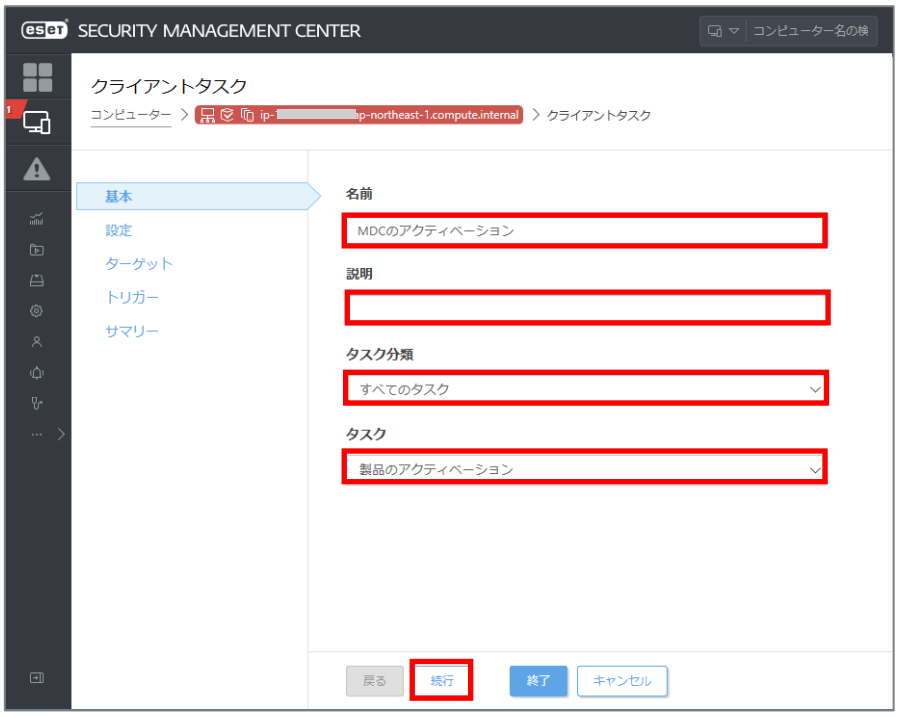
①問題	アクティベーションされていません
②製品	ESET Security Management Center モバイルデバイスコネクター

ここでは、「Mobile Device Connector」がインストールされた ESMC サーバーが正しく選択されていることをここで確認します。

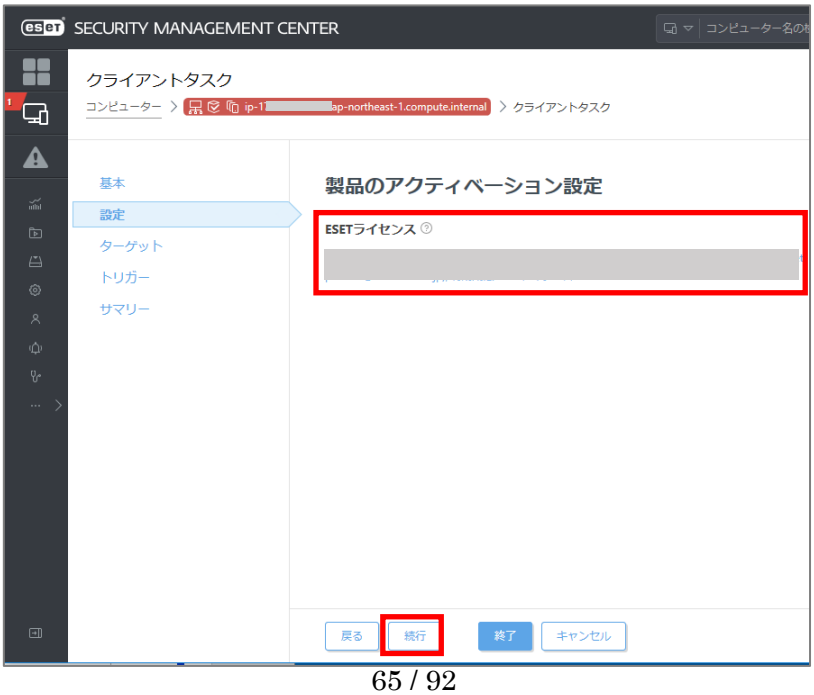
4. 画面右下の「コンピューター」→［新規タスク］をクリックます。

5. クライアントタスクの作成画面が開いたら、以下の通り設定し、「続行」をクリックします。

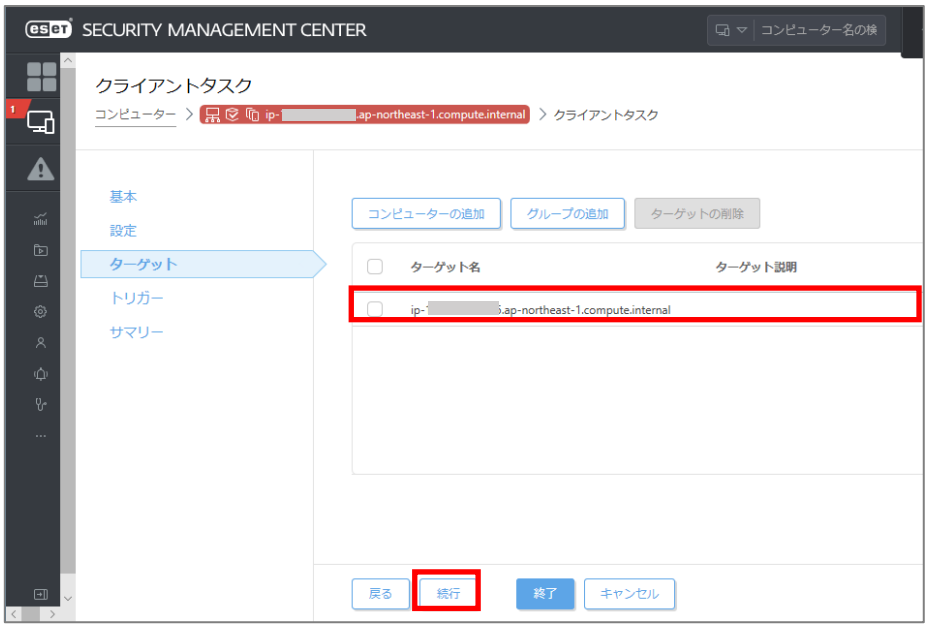
名前	任意のタスク名 例「MDC のアクティベーション」
説明	任意のタスク説明 例「Mobile Device Connector のアクティベーション」
タスク分類	すべてのタスク
タスク	製品のアクティベーション



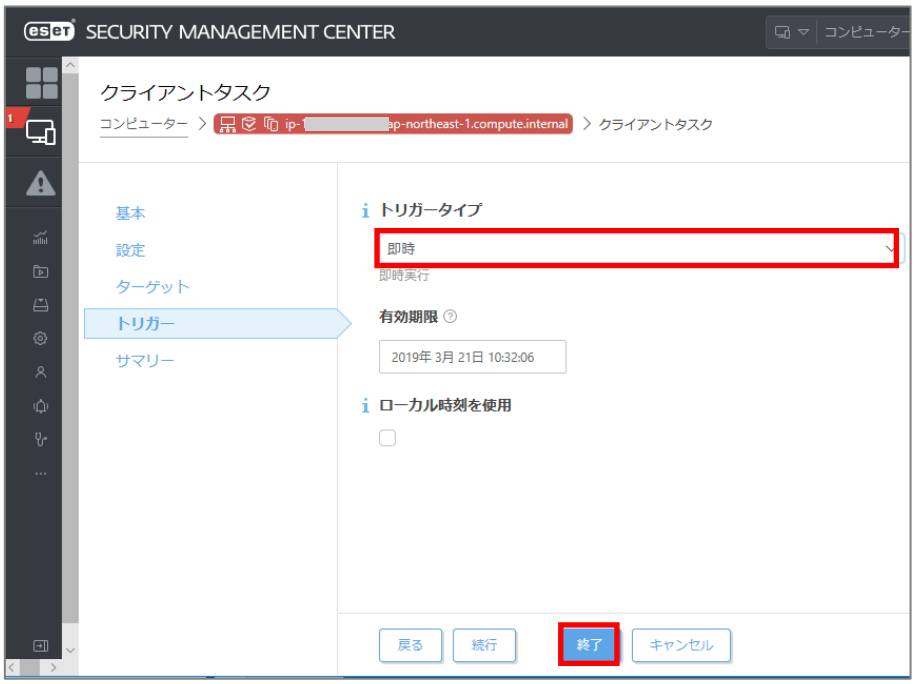
6. ESET ライセンスが選択されていることを確認し、「続行」をクリックします。



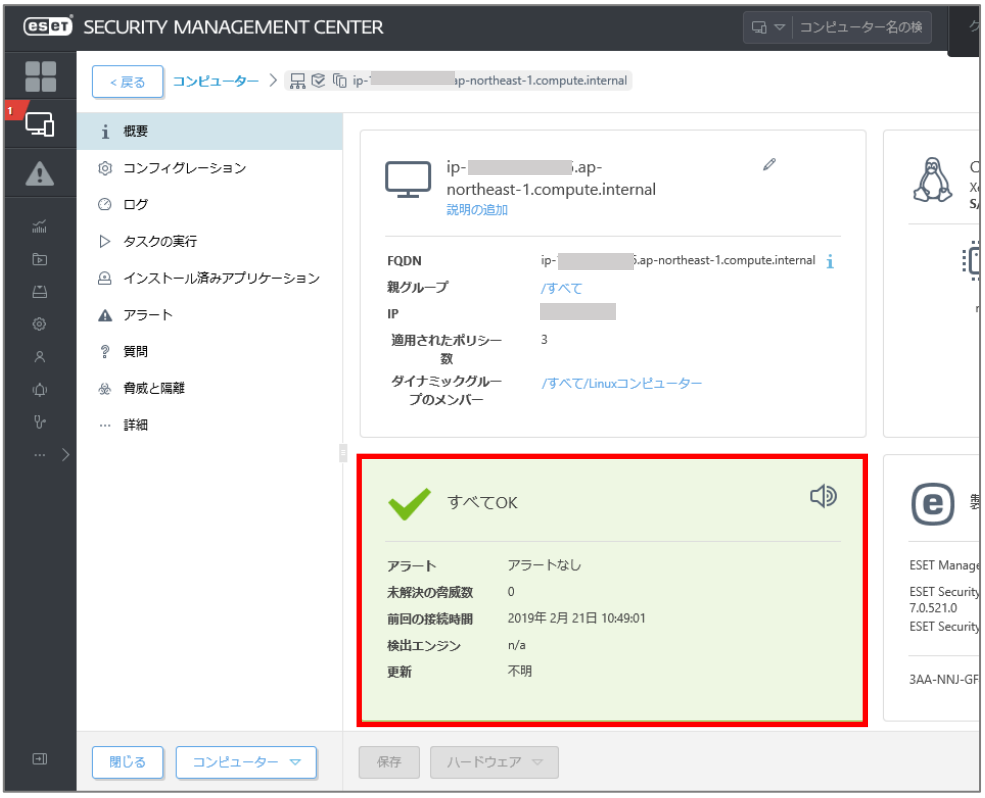
7. 「ターゲット名」で［ESMC サーバー＜ip-172-31-xxx-xxx.ap-northeast-1.compute.internal＞］が選択されていることを確認し、「続行」をクリックします。



8. トリガータイプに「即時」が選択されていることを確認し、「終了」をクリックします。しばらくするとタスクが実行されます。



9. 「コンピューター」→「すべて」→「ESMC サーバー <ip-172-31-xxx-xxx.ap-northeast-1.compute.internal> 」→ [詳細を表示] より、アラートが消えていることを確認します。
   ※ 上記以外の問題が発生している場合は、適宜対応してください。



以上で、Mobile Device Connector のアクティベーション作業は完了です。

C-2. APN 証明書の作成と登録用ポリシーの作成【管理サーバー側作業】

iOS のモバイルデバイスの管理を行うための APN 証明書の作成と iOS のモバイルデバイス登録用ポリシーを作成します。

※ iOS のモバイルデバイスの管理をご利用にならない場合は、「C-3. モバイルデバイスの登録」に進んでください。

（1）APN 証明書の作成

APN 証明書の作成方法は、弊社ユーザーズサイトに公開してあります ESET Security Management Center V7.0 ユーザーズマニュアルの［8.14.6.4 APN 証明書（P571)］をご参照ください。

（2）iOS デバイス登録用のポリシーを作成する

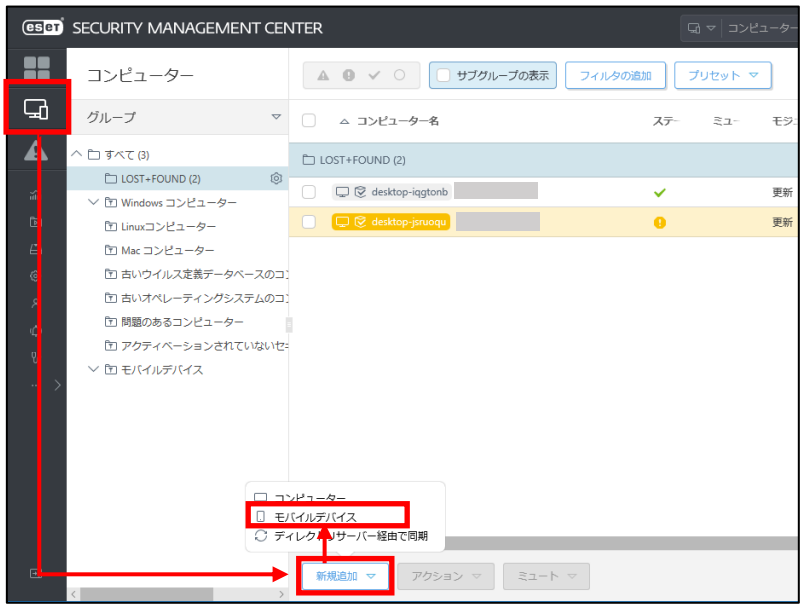
iOS のモバイルデバイス登録用のポリシー作成方法は、弊社ユーザーズサイトに公開してあります ESET Security Management Center V7.0 ユーザーズマニュアル［9.3.2 Mobile Device Connector ポリシーを利用して iOS 登録で APNS/DEP 有効にする（P695)］をご参照ください。

C-3. モバイルデバイスの登録【管理サーバー側作業】

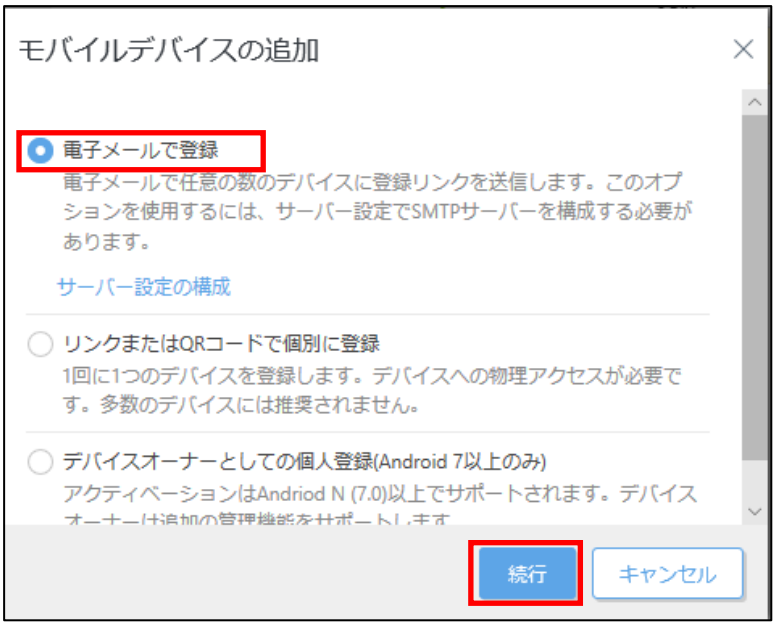
クラウドオプションから各クライアント端末へクラウドオプションで管理するための登録リンク、簡単なインストール手順の説明をメールで送信します。
各クライアント端末は、メールを受信したら登録用リンクにアクセスすることで、管理が開始されます。

そのため、各モバイルデバイスの電子メール情報を事前にクラウドオプションに登録します。
以下に、登録方法を記載します。

1. ESMC にログインし、「コンピューター」をクリックします。
   モバイルデバイスを登録したいグループをクリックし、「新規追加」→「モバイルデバイス」をクリックします。



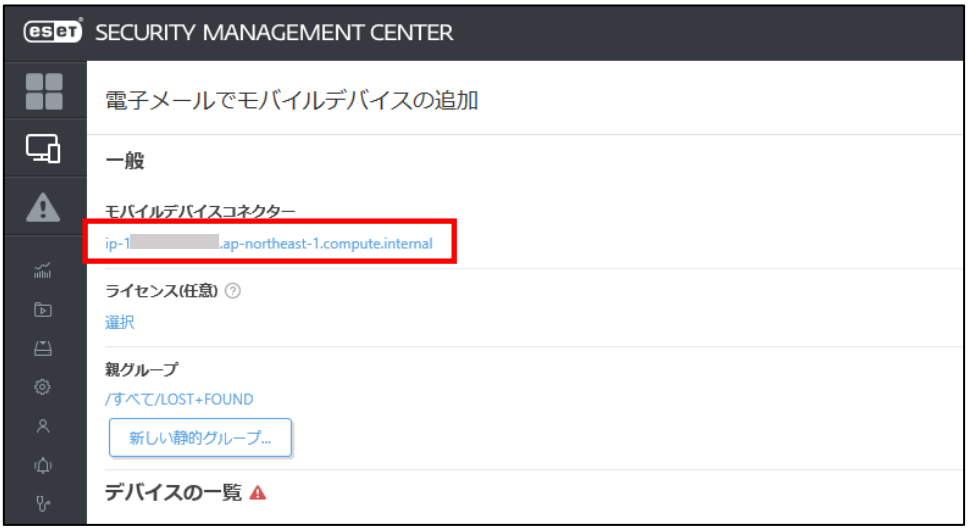
2. 「電子メールで登録」を選択し、「続行」をクリックします。



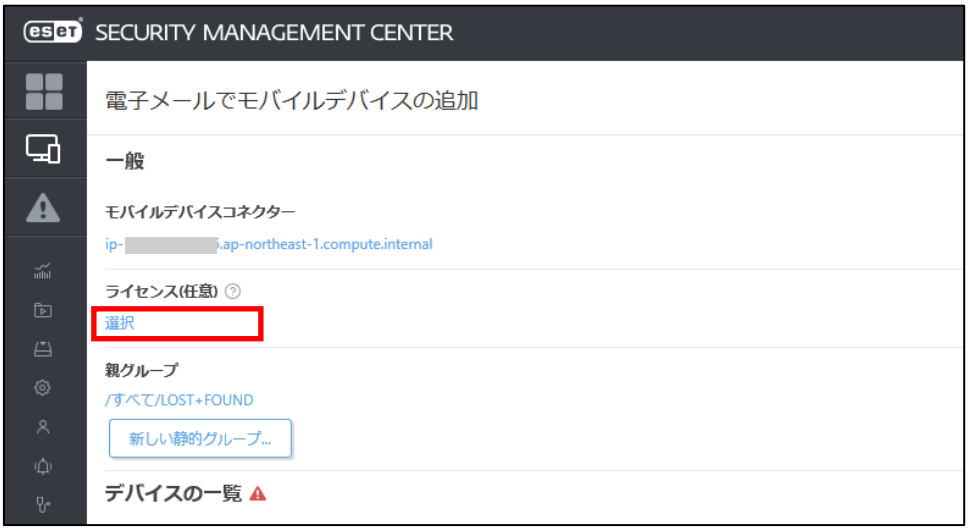
3. 「モバイルデバイスコネクター」に以下が選択されていることを確認します。

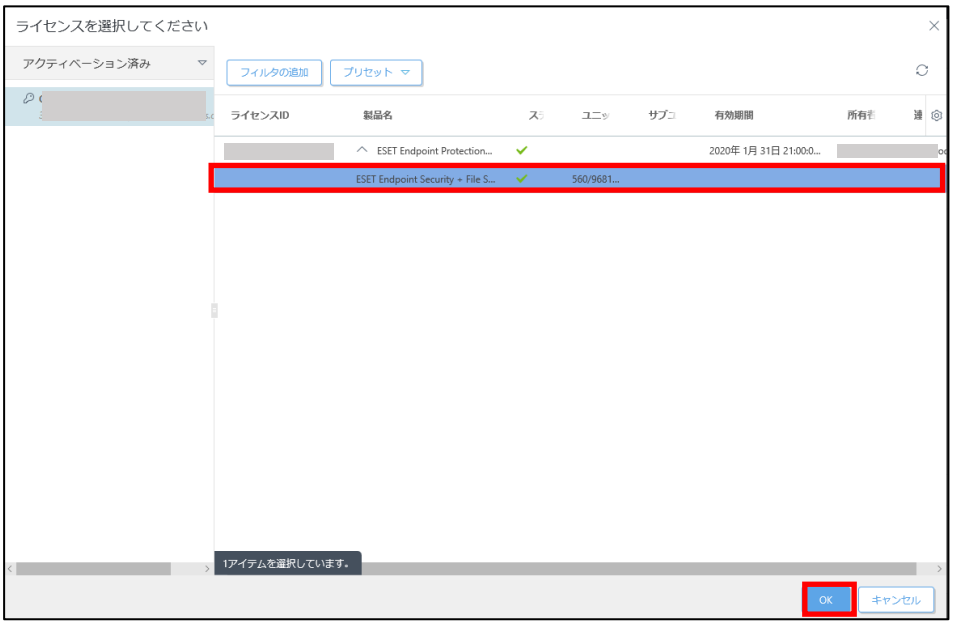
ip-172-31-xxx-xxx.ap-northeast-1.compute.internal

※「172-31-xxx-xxx」はお客さまごとに異なります。



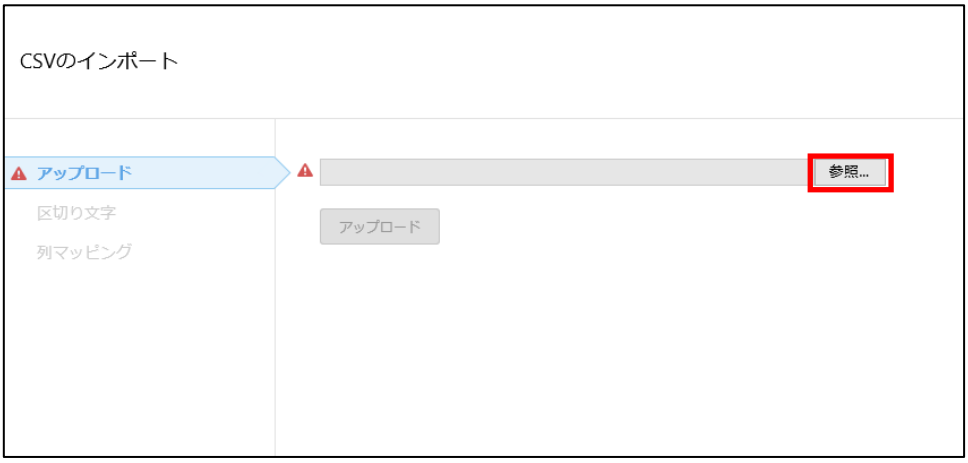
4. 「ライセンス(任意)」の「選択」をクリックし、「5. クラウドオプションへのライセンスの登録」で追加したライセンスを選択します。
※製品のアクティベーションを実施するため、クライアントタスクがモバイルデバイス用に作成されます。





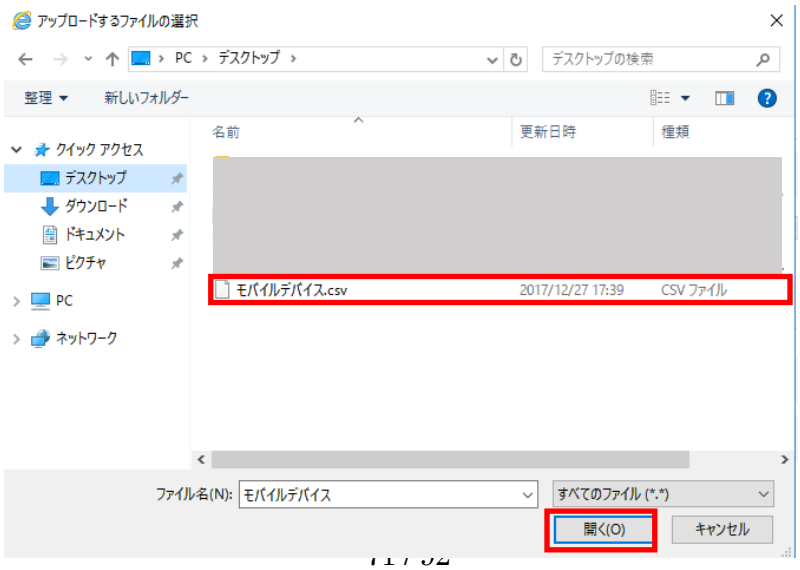
5. 「CSV のインポート」をクリックします。

6. アップロードより、「参照」をクリックします。



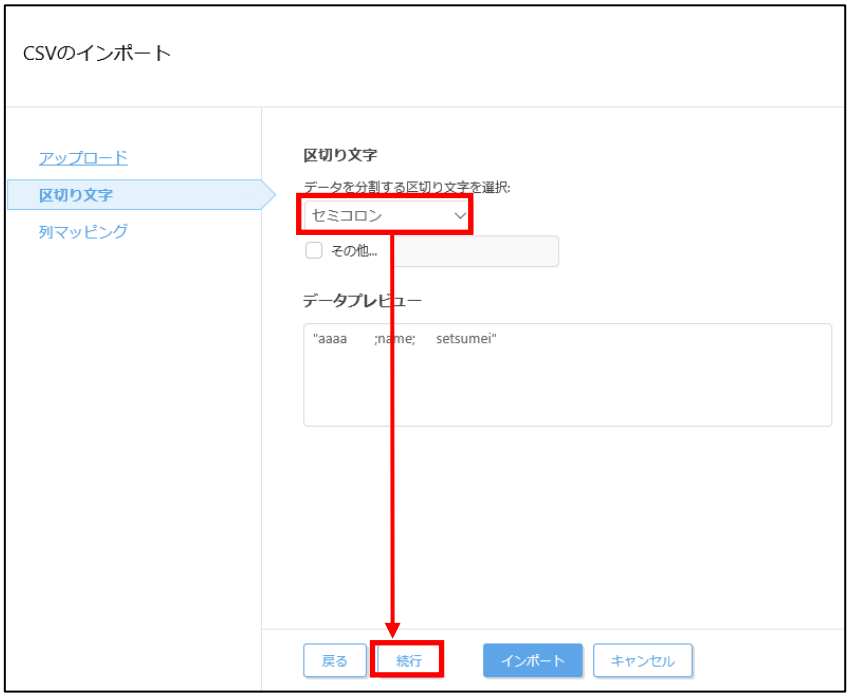
7. 用意しておいた CSV 形式のファイルを選択し、「開く」をクリックします。
※CSV 形式ファイル 例）

【列 1】 【列 2】 【列 3】
<電子メールアドレス>;<デバイス名>;<説明（任意）>
<電子メールファイル>;<デバイス名>;<説明（任意）>

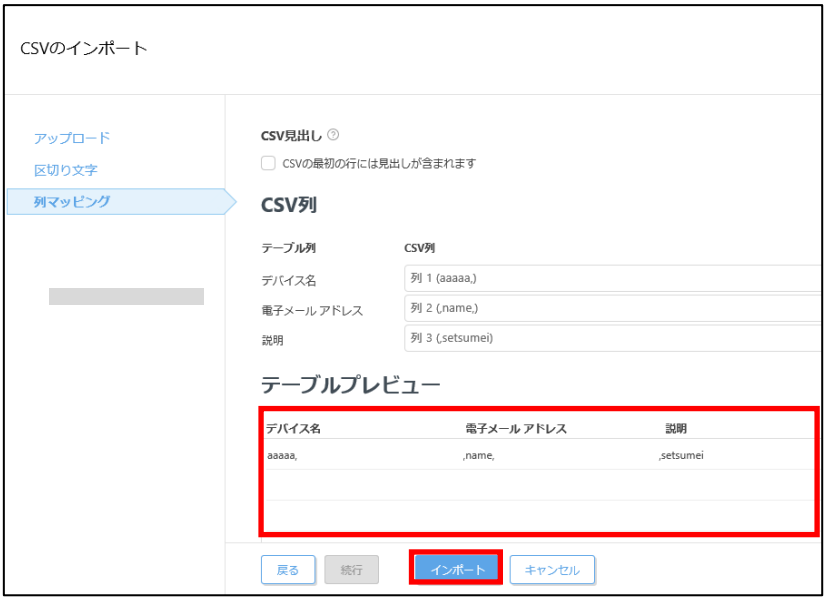


8. 「アップロード」をクリックします。
読み込んだ CSV 形式のファイルのプレビューが表示されます。

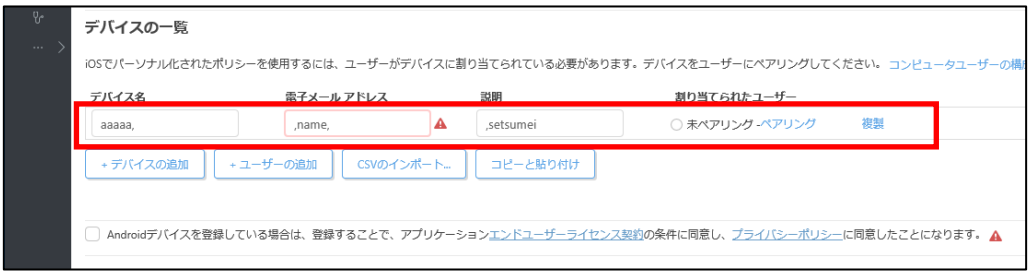
9. [区切り文字]より、「データを分割する区切り文字の選択」から用意した CSV ファイルの列区切り文字を選択します。
※（例）の通り入力いただいた場合、「セミコロン」を選択してください。
「続行」をクリックします。



10. テーブルプレビューにて、作成した CSV 形式通りに文字列が並んでいることを確認し、「インポート」をクリックします。



11. CSV ファイルから読み込まれた情報に問題がないか確認します。



12. Android デバイスを登録する場合、エンドユーザーライセンス契約をご確認のうえ、同意いただいたらチェックを入れます。
登録電子メールメッセージの内容を確認し、「登録」をクリックします。
しばらくすると、入力した電子メールと手順が記載された電子メールが送信されます。

13. モバイルデバイスでメールを受信したら、電子メールに記載されているリンクをタップし「ESET Endpoint Security for Android」や、iOS の「ESET iOS Management Profile」のインストールを行います。

以上で、モバイルデバイスの登録は完了です。
続いて、各モバイルデバイスでのクライアント展開を実施します。

C-4. クライアント用プログラムの展開【クライアント側作業】

モバイルデバイスを ESET Security Management Center に登録したら、Android OS デバイスには［ESET Endpoint Security for Android］、iOS デバイスには［ESET iOS Management Profile］を展開します。

「C-3. モバイルデバイスの登録」の手順 11 の電子メールアドレス宛てに、以下のアドレスからメールが送信されます。以下のアドレスから送信されるメールがスパム判定されないよう、あらかじめ設定をお願いいたします。

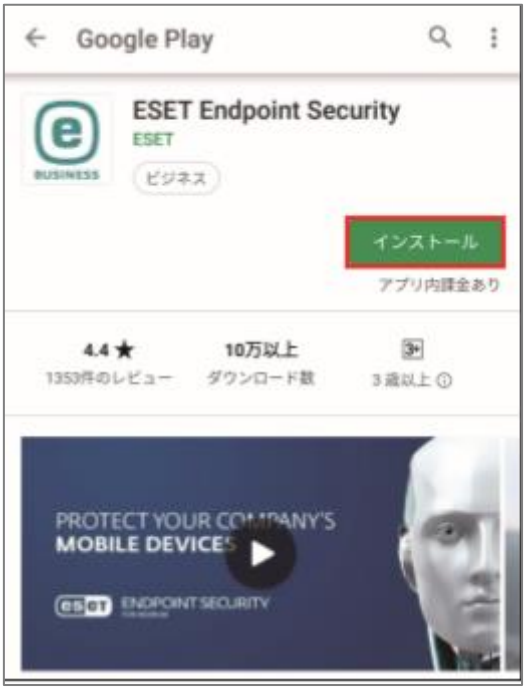
【era-admin@era-cloud.canon-its.jp】

D）Android OS デバイスへ「ESET Endpoint Security for Android」の展開

1. クラウドオプションから受信したメールに記載の登録リンクをタップします。
   ［接続］ボタンをタップします。

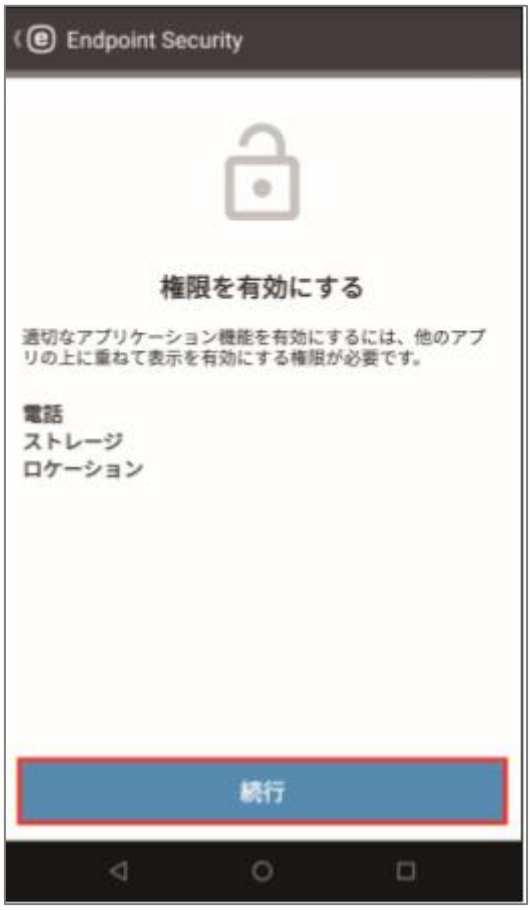
2. セキュリティの警告画面が表示されたときは、［詳細設定］をタップして、［https:// <ESMC サーバーの IP アドレス>:9980/enrollment にアクセスする］をタップします。

3. Google Play Store に移動するので、［インストール］ボタンをタップします。
※インストール後に表示される［開く］ボタンはタップしないでください。



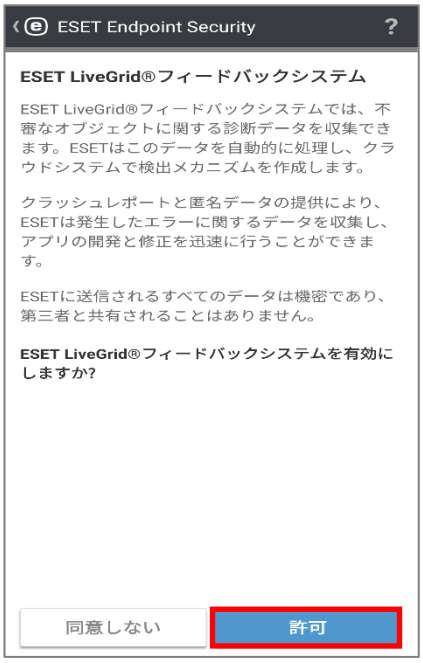
4. クラウドオプションから受信したメールに記載の登録リンクを再度タップします。
［接続］ボタンをタップします。
ESET Endpoint Security for Android の初期設定が始まります。

5. ［続行］ボタンをタップします。



6. ［許可］ボタンを 3 回タップします。

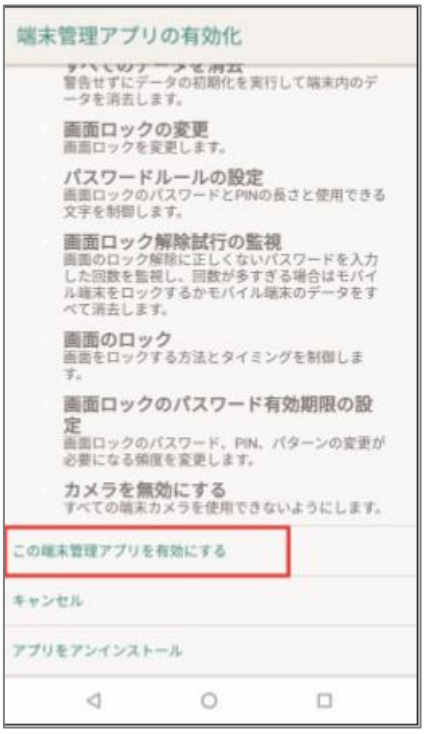
7. ［ESET LiveGrid フィードバックシステム］の設定画面が表示されます。内容を確認して、［許可］ボタンをタップします。



8. 名前の入力画面が表示されます。必要に応じて名前の修正を行い、［保存］ボタンをタップします。

9. ［有効］ボタンをタップします。

10. ［この端末管理アプリを有効にする］をタップします。



11. ［続行］をタップします。

12. ［OK］をタップします。

13. ［ESET Endpoint Security］をタップし、［使用状況へのアクセスを許可］の右側にあるスライドバーをタップします。

14. ［設定が正常に完了しました］と表示されます。［終了］をタップします。

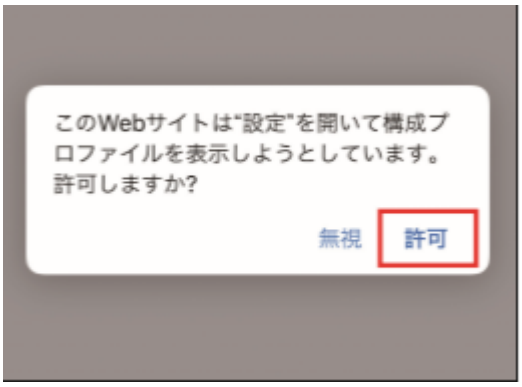
以上で、Android OS デバイスへ「ESET Endpoint Security for Android」の展開は完了です。

iOS デバイスの管理を実施しない場合は、「C-5.管理者パスワード適用ポリシーの作成」を実施してください。

E）iOS デバイスへ「ESET iOS Management Profile」の展開

1. クラウドオプションから受信したメールに記載された登録リンクをタップします。

2. ダイアログが表示されます。[許可]をタップします。



3. プロファイルのインストール画面が表示されますので、［インストール］をタップします。

4. ［インストール］をタップします。

5. ［信頼］をタップすると、プロファイルのインストールが行われます。

6. インストールが完了したら、[完了] をタップします。

以上で、クライアント用プログラムの展開は完了です。
続いて「7. クラウドオプションで管理ができていることを確認」に進んでください。

なお、しばらくしても、モバイルデバイスのアクティベーションが行われない場合は、以下をご参考のうえアクティベーションを実施してください。

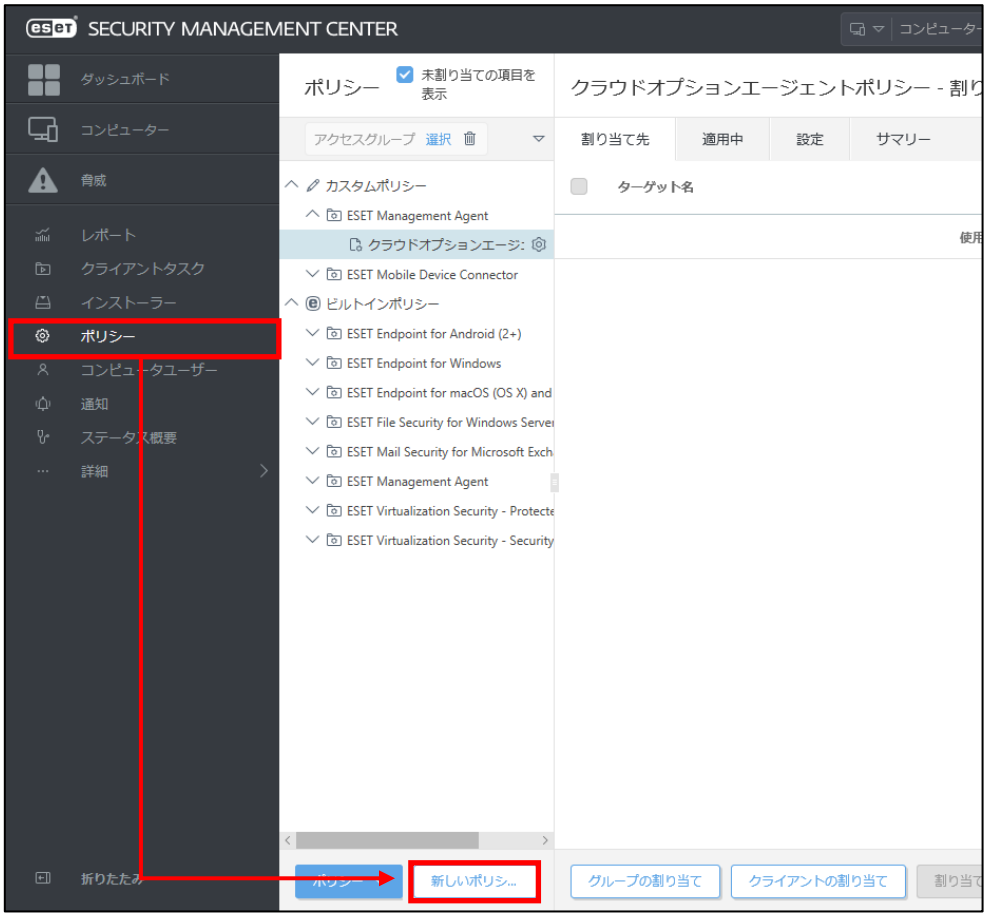
◆ESET Security Management Center V7.0 ユーザーズマニュアルの［8.8.2　新しいクライアントタスクの作成（P400)］
※タスク作成時に、[基本]→[タスク]→[タスク]には、[製品のアクティベーション]を選択してください。

C-5. 管理者パスワード適用ポリシーの作成【管理者側作業】

各 Android OS のモバイルデバイスに管理者パスワードを設定します。
iOS のモバイルデバイスに対して、本作業を行う必要はございません。

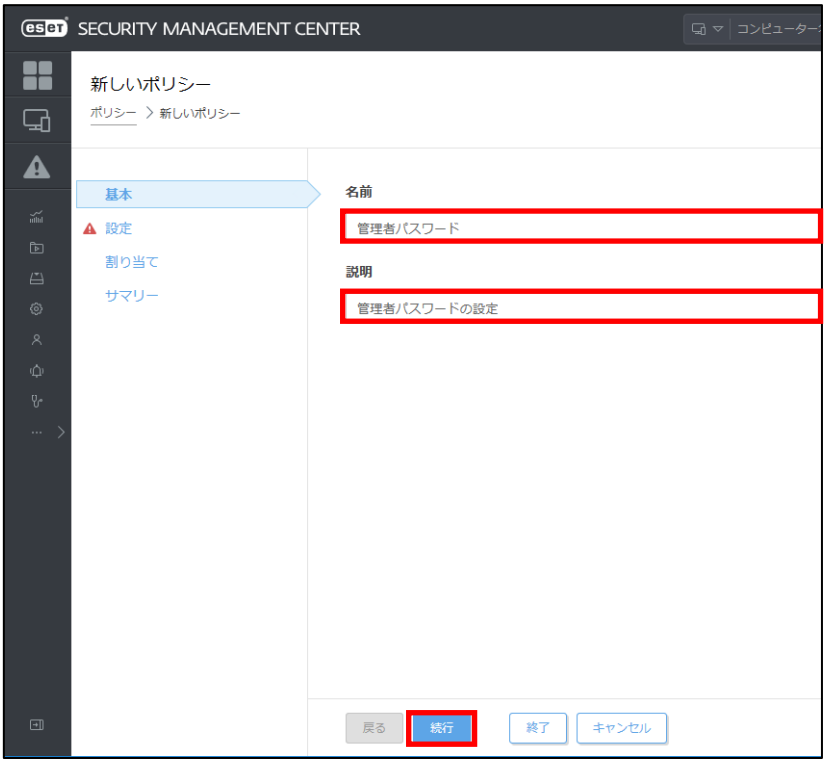
以下の手順を参照し、管理者パスワードの設定を行ってください。

1. 「ポリシー」→「新しいポリシー」をクリックします。

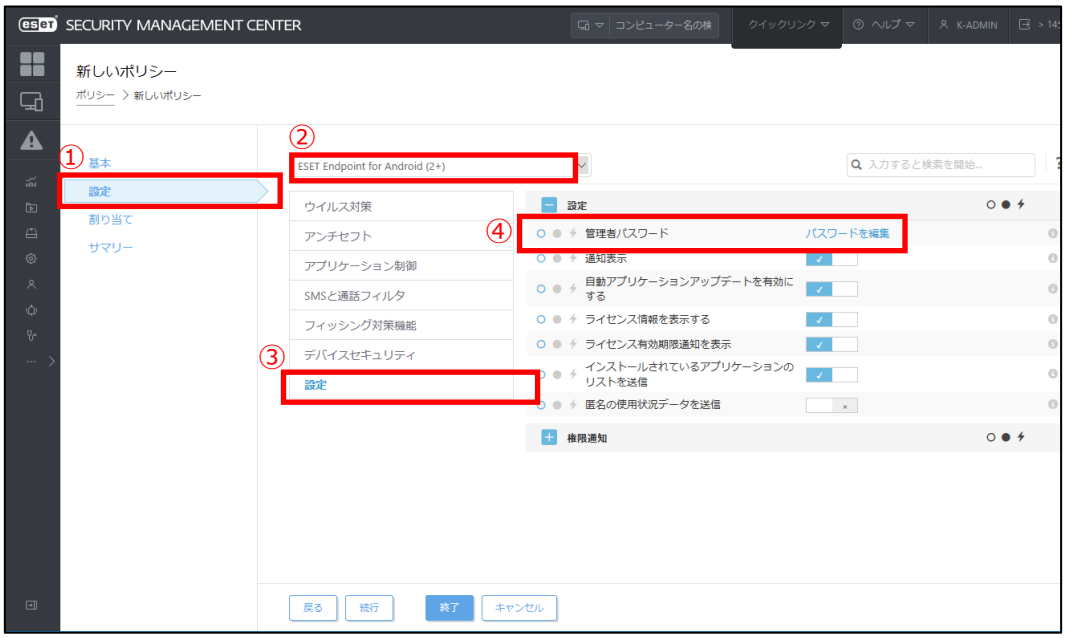


2. 下記の通り設定し、「続行」をクリックします。

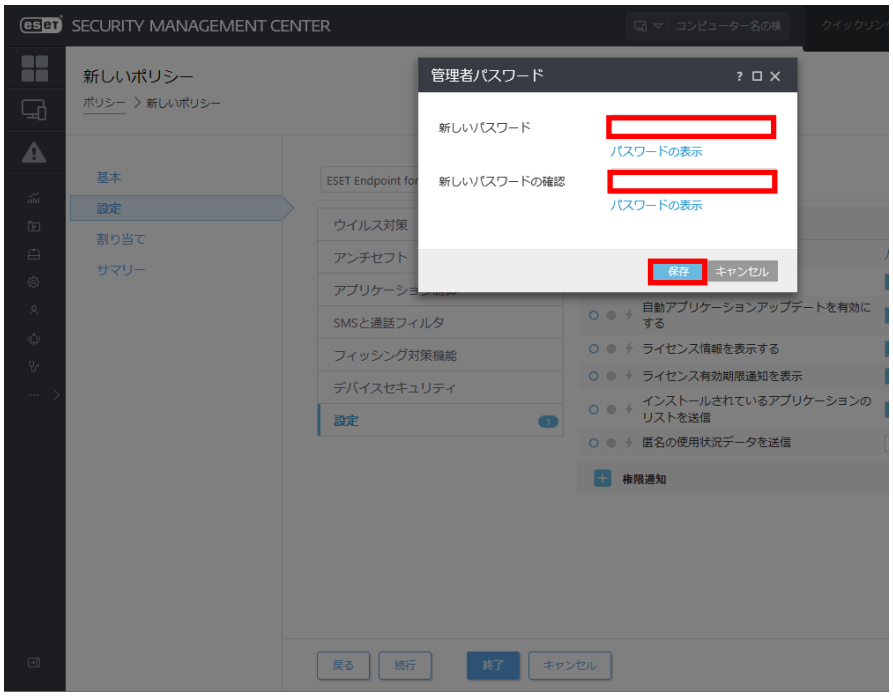
名前	任意のポリシー名 例「管理者パスワード」
説明	任意のポリシー説明 例「管理者パスワード設定」



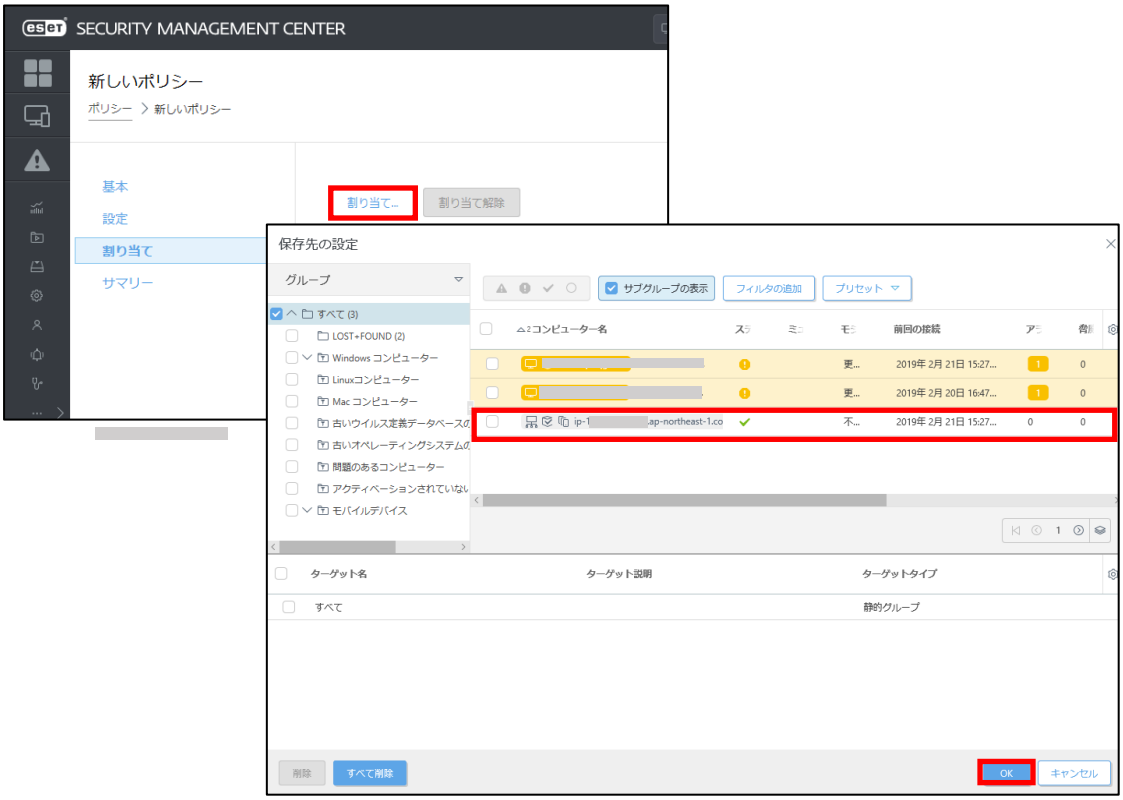
3. ［設定］→［ESET Security Product for Android(2+)］→［設定］→［パスワードの編集］をクリックします。



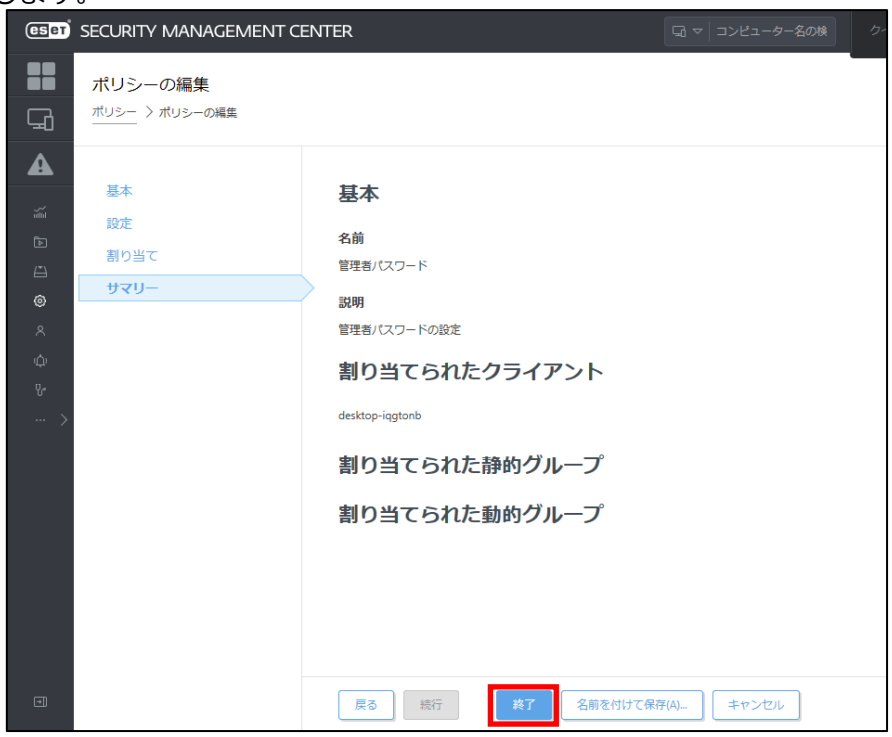
4. パスワードを入力し、［保存］をクリックします。
「続行」をクリックします。



5. ［割り当て…］をクリックし、［保存先の設定］画面が開いたら、対象の Android OS のモバイルデバイスを選択し、［OK］をクリックします。



6. サマリーより、入力した情報が正しいことを確認し、「終了」をクリックします。



以上で、管理者パスワード適用ポリシーの作成は完了です。

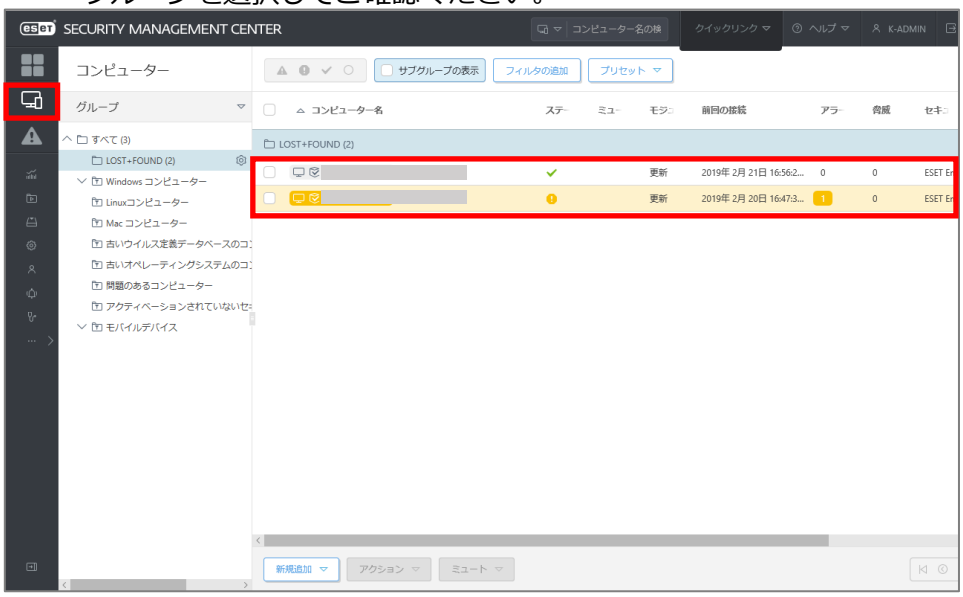
7. クラウドオプションで管理できていることを確認【管理サーバー側作業】

ESET Security Management Center でクライアント端末の管理ができていることを確認します。

以下に、クライアント管理の確認手順を記載します。

1. 「**3.6.ライセンス情報･ログイン情報の準備**」で確認した①「ESMC ログイン名」、②「ESMC ログインパスワード」を入力し、③「日本語」を選択して、④「ログイン」をクリックします。

2. 「コンピューター」のクライアントの一覧画面よりクライアントが表示されていることを確認してください。
   ※クライアント展開時に所属する静的グループを指定した場合は、そちらの各グループを選択してご確認ください。



3. 管理対象クライアント端末のステータスが黄色や赤色になっている場合、クライアント側でエラー（検出エンジンがアップデートされていない、アクティベーションされていない）が発生している可能性があります。
詳細を確認し、ご対応ください。

コンピューター名を実際のコンピューター名に変換する場合は、「サ―バータスク」の「コンピューター名の変更」タスクをご使用ください。
タスクのご使用方法は ESET Security Management Center V7.0 ユーザーズマニュアルより、「8.14.7.8 コンピューター名の変更」をご確認ください。

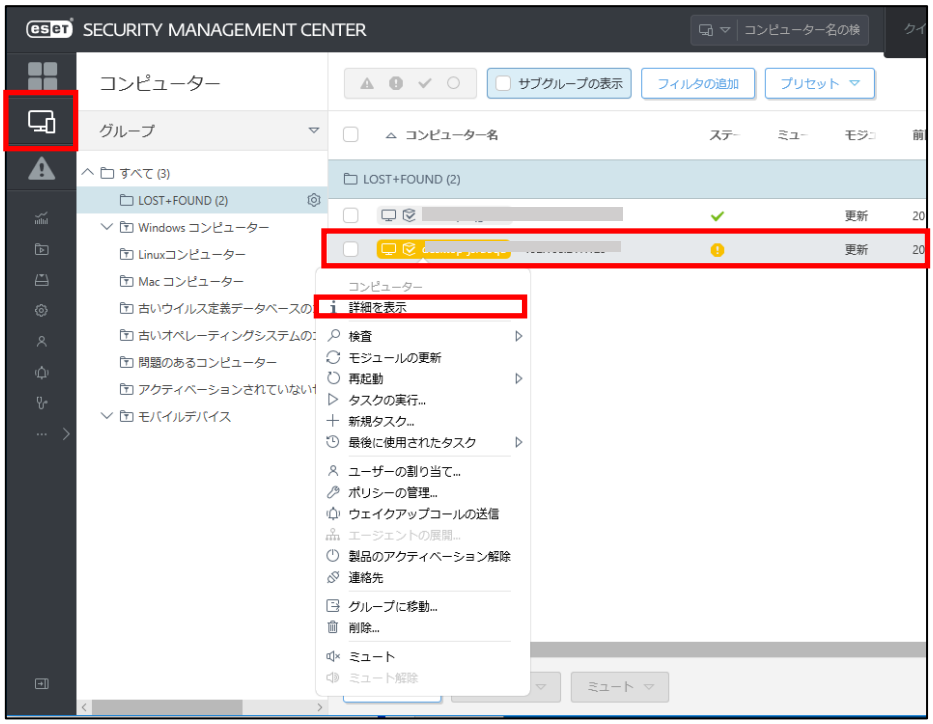
完了

以上でクラウドオプジョンでのクライアント端末の管理は完了です。

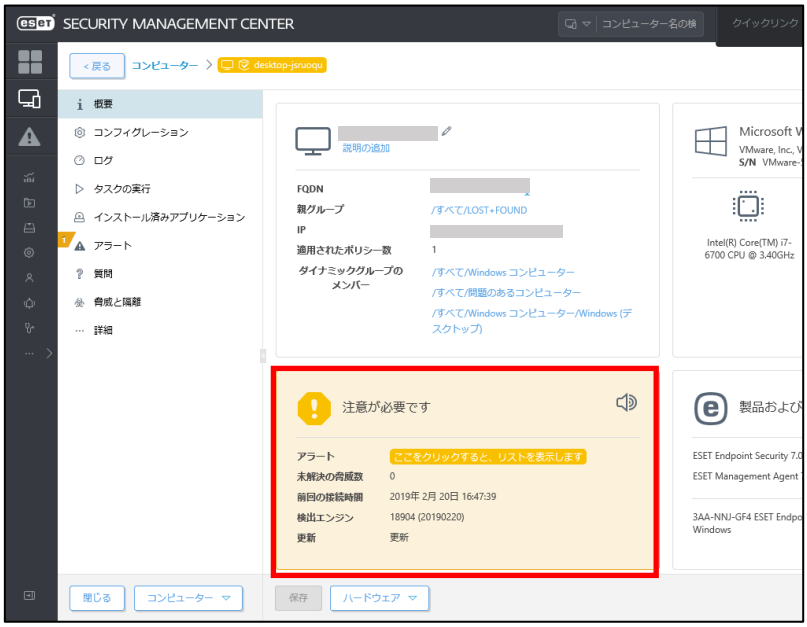
その他、ESET Security Management Center の操作方法につきましては、ESET Security Management Center V7.0 ユーザーズマニュアルを参照し、クラウドオプションをご利用ください。

【参考】クライアント端末の詳細情報確認

1. 「コンピューター」の一覧より、任意のクライアントコンピューターをクリックし、メニューから「詳細を表示」を選択します。



2. 該当クライアントの詳細情報が表示されます。こちらの画面で検出エンジンのバージョン、OS 情報、ESET 設定などが確認できます。
※モバイルデバイスの情報取得タイミングについて、初回のみ 1～2 日かかる場合がございます。



また、ユーザーズサイトでご提供している機能説明資料なども合わせてご参照いただき、クラウドオプションをご利用ください。

■ESET Endpoint Protection シリーズ ユーザーズサイト
https://canon-its.jp/product/eset/users/

※機能説明資料はユーザーズサイトの[プログラム/マニュアル] – [最新バージョンをダウンロード]の、10.製品説明資料・各種手順書より以下のファイルをダウンロードください。

・Windows / Windows Server 向けクライアント用プログラム（V7.x）機能紹介資料

・Mac 向けクライアント用プログラム（V6.x）新機能紹介資料

・Linux Desktop 向けクライアント用プログラム（V4.0）機能紹介資料

・Android 向けクライアント用プログラム（V2.x）新機能紹介資料

・Linux Server 向けクライアント用プログラム（V4.5）機能紹介資料

・ESET Security Management Center V7.x 新機能紹介資料

また、弊社 ESET サポート情報ページにて、製品機能・仕様・操作手順などの情報を公開していますので、ご利用ください。

■ESET サポート情報　法人向けサーバー・クライアント用製品
https://eset-support.canon-its.jp/?site_domain=business

ご不明な点などがございましたら、上記 Web ページをご確認いただくか、下記 Web ページより弊社サポートセンターまでお問い合わせください。

■お問い合わせ窓口（サポートセンター）
https://eset-support.canon-its.jp/faq/show/883?site_domain=business