

Kaspersky Security for Virtualization  
Light Agent 5.x  
簡単インストールガイド

VMware vSphere &  
Horizon 編

2020/11/24  
株式会社カスペルスキー  
セールスエンジニアリング部  
Ver. 1.0

はじめに .....	3
前提条件 .....	3
手順概要 .....	4
必要なパッケージ .....	5
1. KSV Light Agent 本体のインストール .....	6
1.1. インストール .....	6
1.2. インストール後の KSC 初期設定 .....	9
1.3. インターフェースの設定 .....	15
1.4. グループの作成 .....	17
1.5. デフォルトポリシーの作成 .....	18
1.6. デフォルトタスクの作成 .....	31
2. SVM (Protection Server コンポーネント) の導入 .....	32
2.1. SVM の導入 .....	32
2.2. SVM のライセンスアクティベーション .....	47
3. Light Agent for Windows のインストール .....	55
3.1. VDI 用ネットワークエージェントの準備 .....	55
3.2. マスター仮想マシンへのインストール (ローカルインストール方式) .....	63
4. マスター仮想マシンのクローン .....	73
4.1. 仮想マシンのクローン .....	73

---

### 前提条件

---

本書では、Kaspersky Security for Virtualization Light Agent（以下 KSV LA）を VMware vSphere 環境にインストールし、設定する手順を示しています。

前提条件として、以下の仮想環境が構築されているものとします。

- VMware ESXi ハイパーバイザー
- VMware vCenter Server

前提条件として、以下のカスペルスキー製品が構築されているものとします。

- Kaspersky Security Center (KSC)

KSC のインストールは以下の手順をご参照ください。

[https://kasperskylabs.jp/biz/kesksc/InstallGuide\\_KSC12\\_v1.0.pdf](https://kasperskylabs.jp/biz/kesksc/InstallGuide_KSC12_v1.0.pdf)

最新のシステム要件については、カスペルスキー製品 WEB ページより、最新の情報をご確認ください。

- Kaspersky Security for Virtualization Light Agent (KSV LA)

<https://support.kaspersky.co.jp/ksv5la#requirements>

- Kaspersky Security Center (KSC)

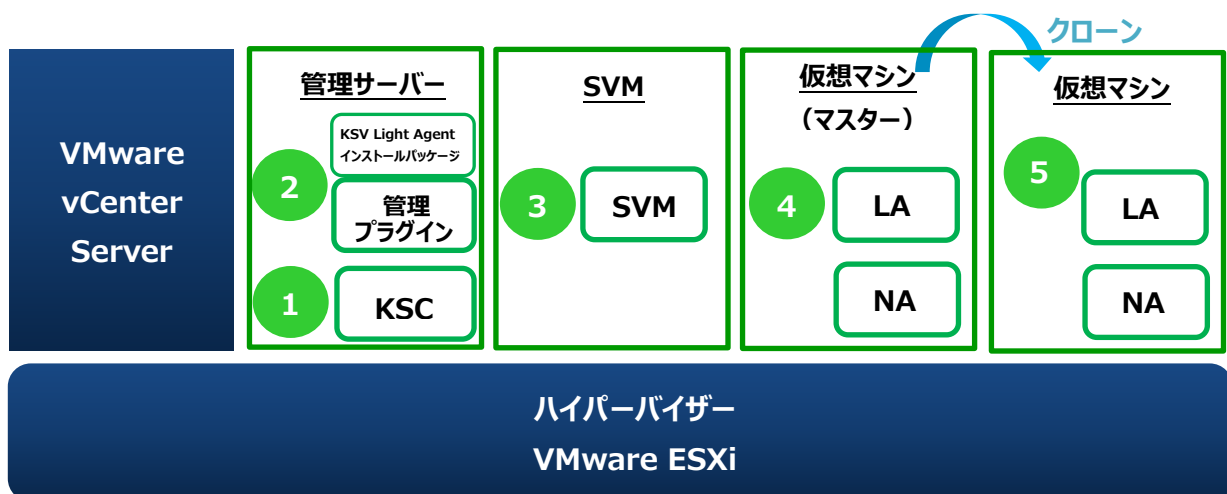
<https://support.kaspersky.co.jp/ksc12#requirements>

Kaspersky Security for Virtualization Light Agent のインストール手順は以下の通りです。

<b>Step.1</b>	Kaspersky Security Center(KSC)のインストール	
<b>Step.2</b>	KSV Light Agent 管理プラグインのインストール KSV Light Agent インストールパッケージの取り込み <u>KSCにインストール</u>	… P 6
<b>Step.3</b>	SVM (Protection Server コンポーネント) のインストール <u>ハイパーバイザー上にインストール</u>	… P32
<b>Step.4</b>	KSV Light Agent (LA) のインストール <u>仮想マシン (VM) にインストール</u>	… P55
<b>Step.5</b>	マスター仮想マシンのクローン 仮想化製品機能でクローン作成	… P73

導入後の構成イメージは下図の通りです。

下記①～⑥はそれぞれ上記 Step.1～Step.6 での作業対象機器を示しています。



Kaspersky Security Virtualization Light Agent を構成するために必要なインストールパッケージは、先を以下からダウンロードしてください。

<https://support.kaspersky.co.jp/ksv5la#downloads>

※ パッケージファイル名は、2020 年 11 月現在の最新バージョンを記載しておりますが、製品バージョンアップにより、パッケージファイル名は異なる場合がございます。

下記 URL より実際にダウンロードされたパッケージをご利用ください。

### 1. Kaspersky Security Virtualization 本体

Integration Server、管理プラグインを KSC にインストールし、KSV LA（Windows 用、LINUX 用）インストールパッケージを KSC に取り込みます。

✓ ファイル名 : **ksvla-components\_5.1.2.273\_mlg.exe**

### 2. SVM (Protection Server コンポーネント) 、

VMware ESXi 用パッケージ。セキュア仮想マシン SVM は KSV LA で保護された仮想マシンのスキャンを行います。

✓ ファイル名 : **ksvla-svm\_vmware-vsphere\_5.1.44.295\_mlg.zip**

### 3. ネットワークエージェント (NA)

KSV LA と KSC 間の通信を行うプログラムです。ポリシーとタスクなどの管理情報やプログラムの更新情報などをやりとりするほか、KSC 経由でクライアントに KSV LA をリモートインストールする際にも使用できます。

※ パッケージは KSC にバンドルされているため、別途ダウンロードは不要です。

## 1. KSV Light Agent 本体のインストール

---

### 1.1. インストール

---

- ① **ksvla-components\_5.1.2.273\_mlg.exe** を起動します。

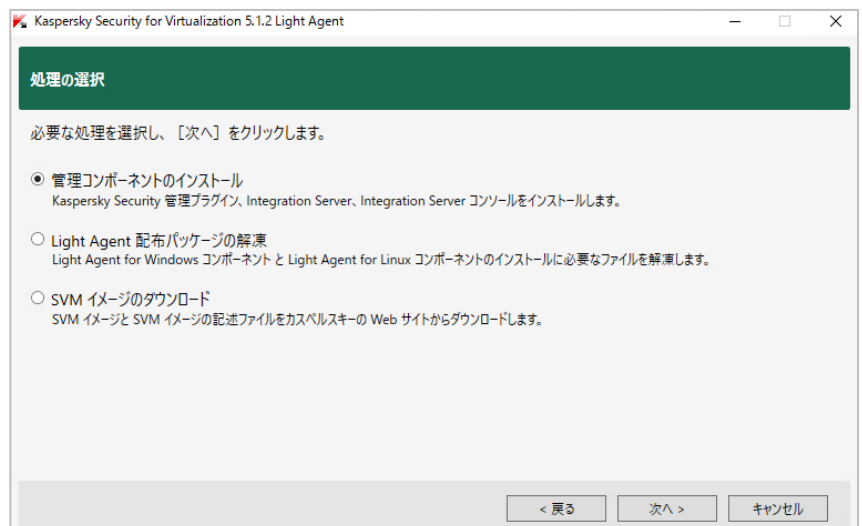


- ② セットアップウィザードが起動します。

使用する言語を選択し、「次へ」をクリックします。



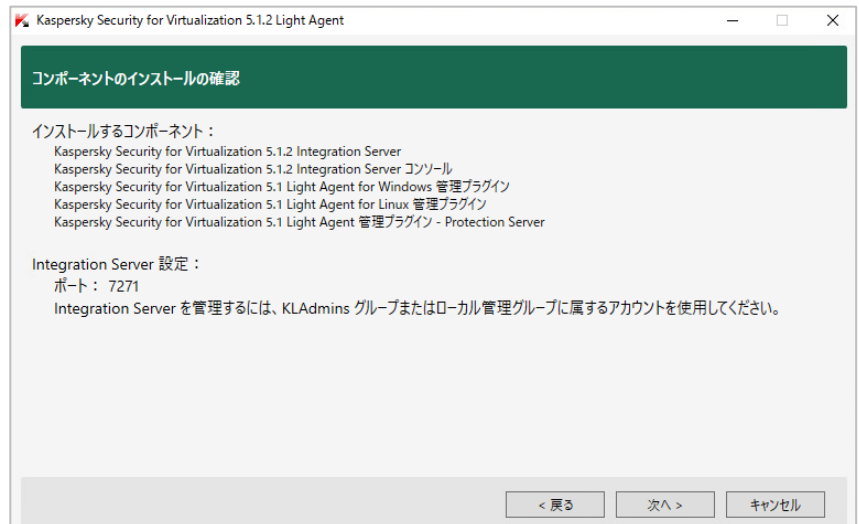
- ③ 「次へ」をクリックします。



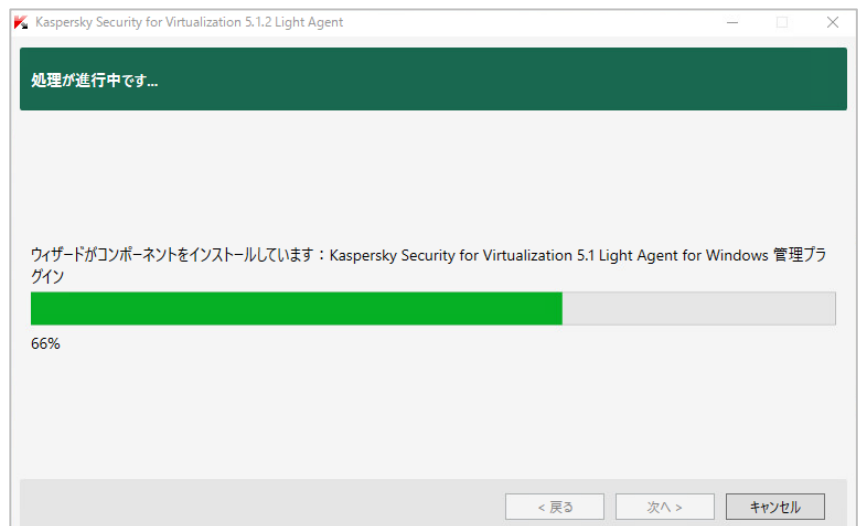
- ④ 「使用許諾契約書」と「プライバシーポリシー」が表示されるので、内容を確認し、チェックボックスをオンにして「次へ」をクリックします。



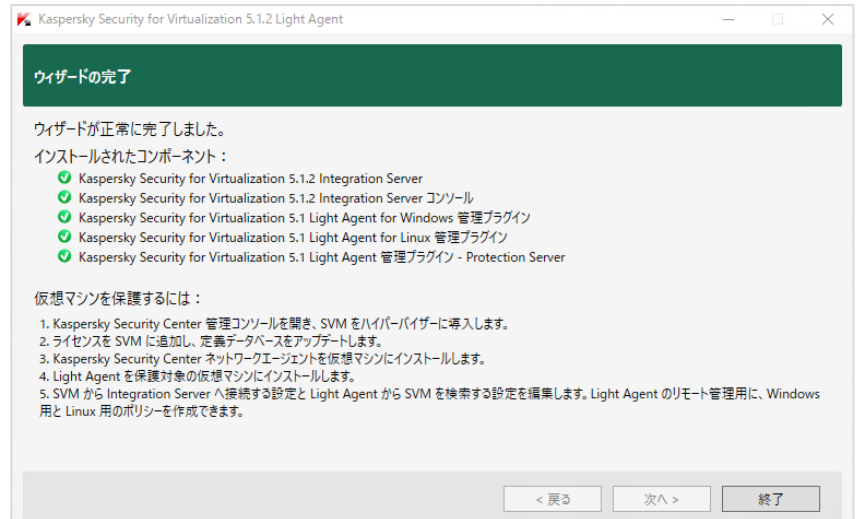
- ⑤ 「次へ」をクリックします。



- ⑥ 完了まで待ちます。



- ⑦ ウィザードが正常に完了したことを確認し、「終了」をクリックします。





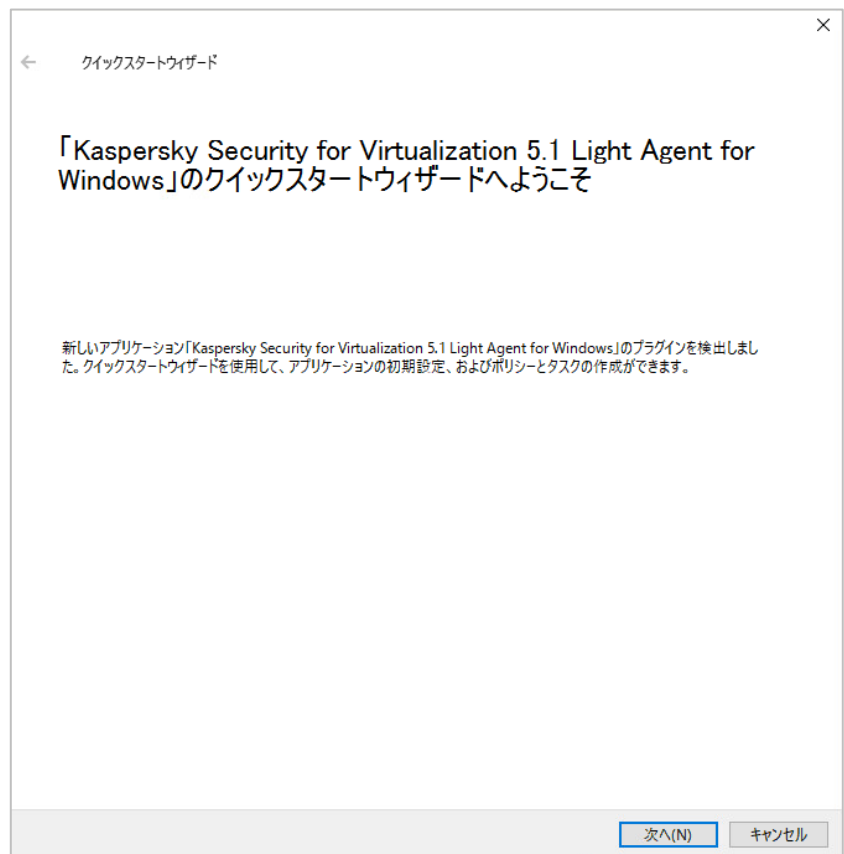
## 1.2. インストール後の KSC 初期設定

---

続いて、KSC の初期設定を行います。

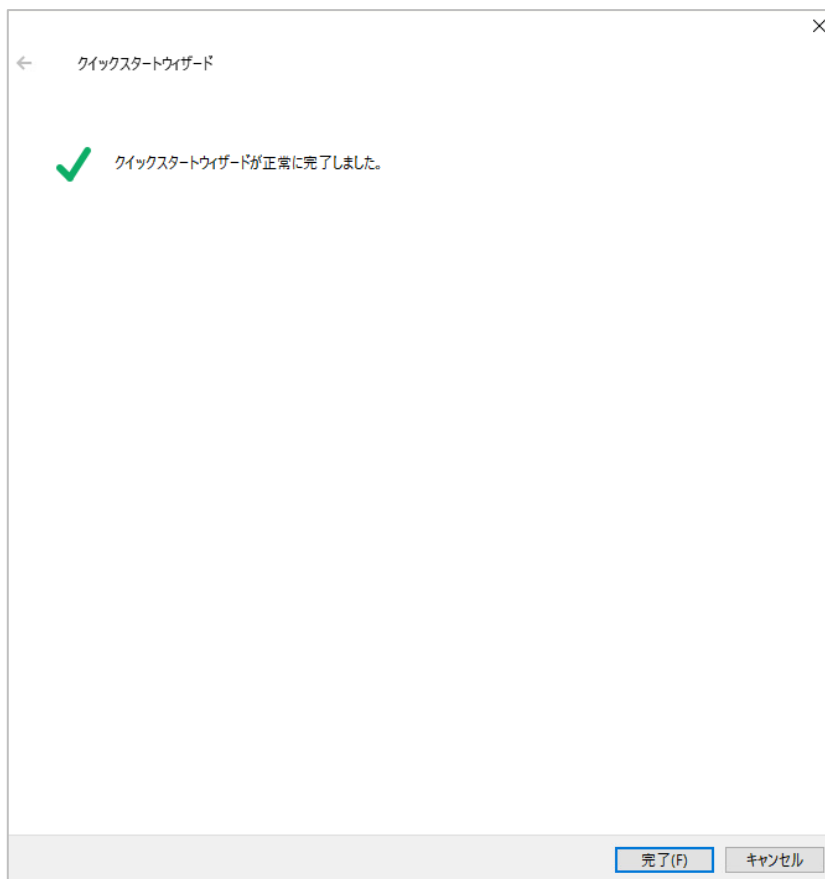
Windows のメニューから Kaspersky Security Center アプリを起動してください。

- ① Windows のメニューから Kaspersky Security Center アプリを起動します。既に起動している場合は、いったん終了し、起動してください。
- ② 続いて、Kaspersky Security for Virtualization Light Agent for Windows のクイックスタートウィザードが表示されます。「次へ」をクリックします。



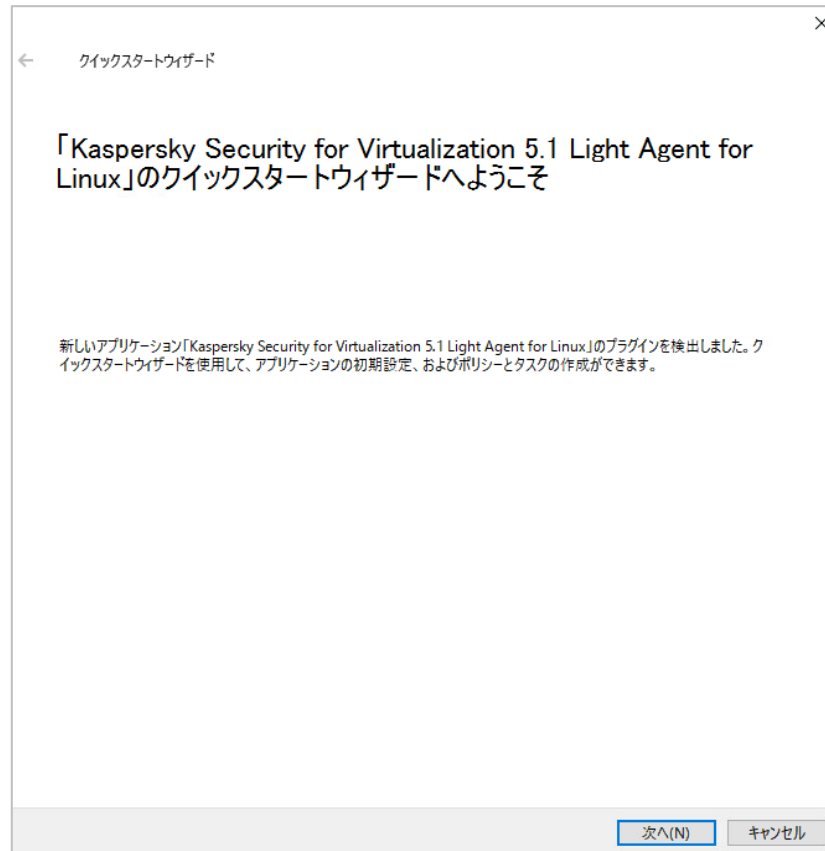
③ クイックスタートウィザードが正常に完了したら、「完了」をクリックします。

※ 本クイックウィザード中に Light Agent (Windows) コンポーネントに関連するタスクが自動的に作成されます。



④ 引き続き、Kaspersky Security for Virtualization Light Agent for Linux のクイックスタートウィザードが表示されます。

「次へ」をクリックします。

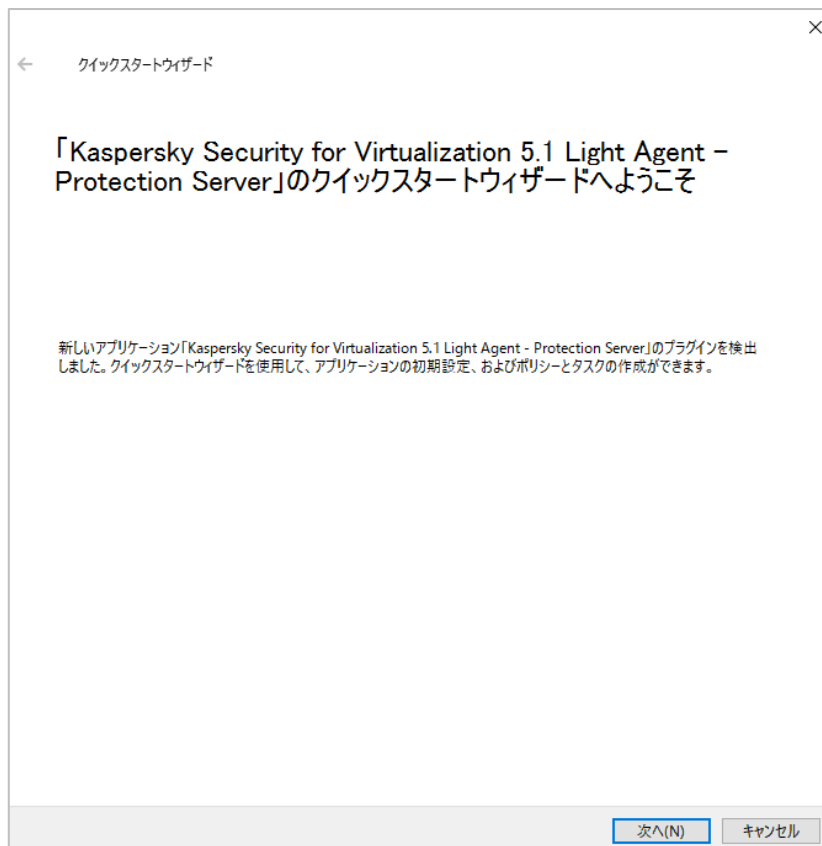
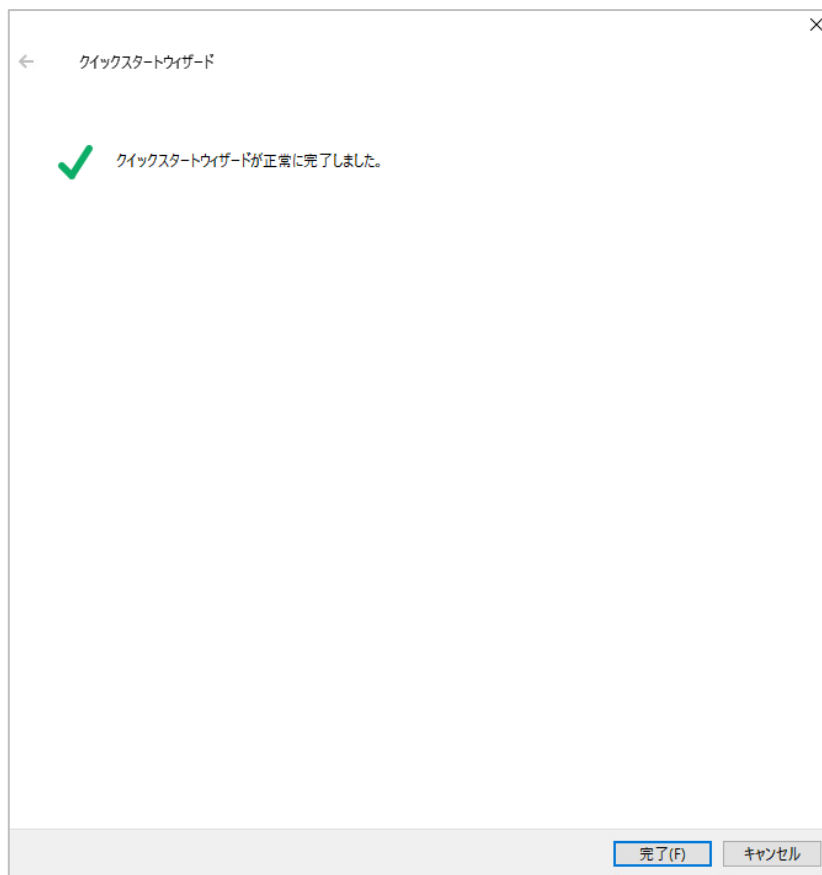


⑤ クイックスタートウィザードが正常に完了しましたら、「完了」をクリックします。

※ 本クイックウィザード中に Light Agent (Linux) コンポーネントに関連するタスクが自動的に作成されます。

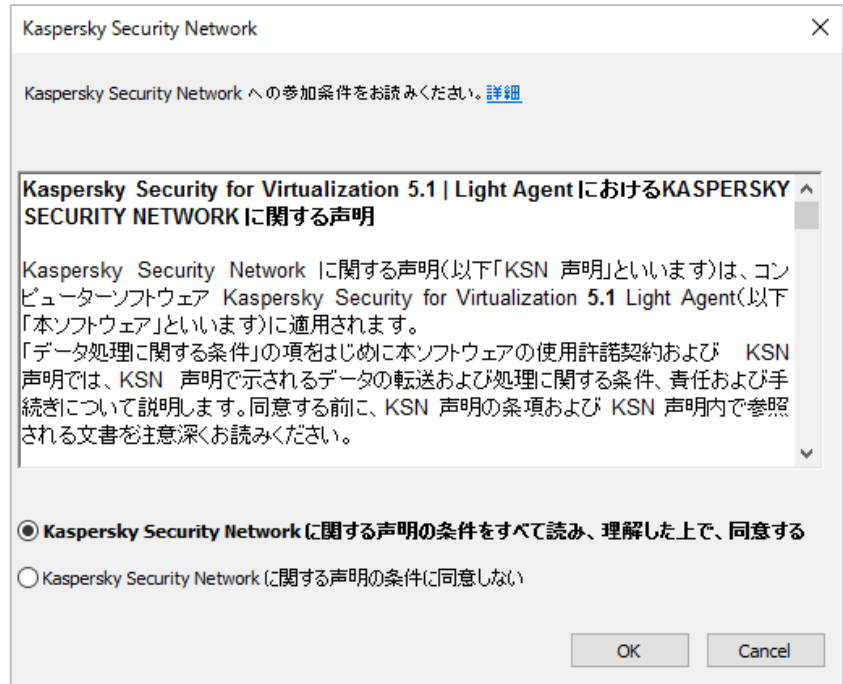
⑥ Kaspersky Security for Virtualization Light Agent Protection Server のクイックスタートウィザードが表示されます。

「次へ」をクリックします。



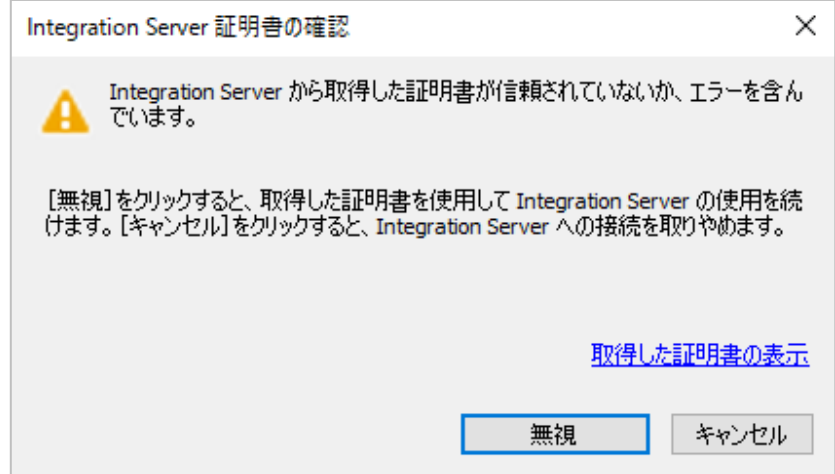
## ⑦ Kaspersky Security

Network に関する声明が表示されます。同意し、OK をクリックします。



## ⑧ Integration Server 証明書

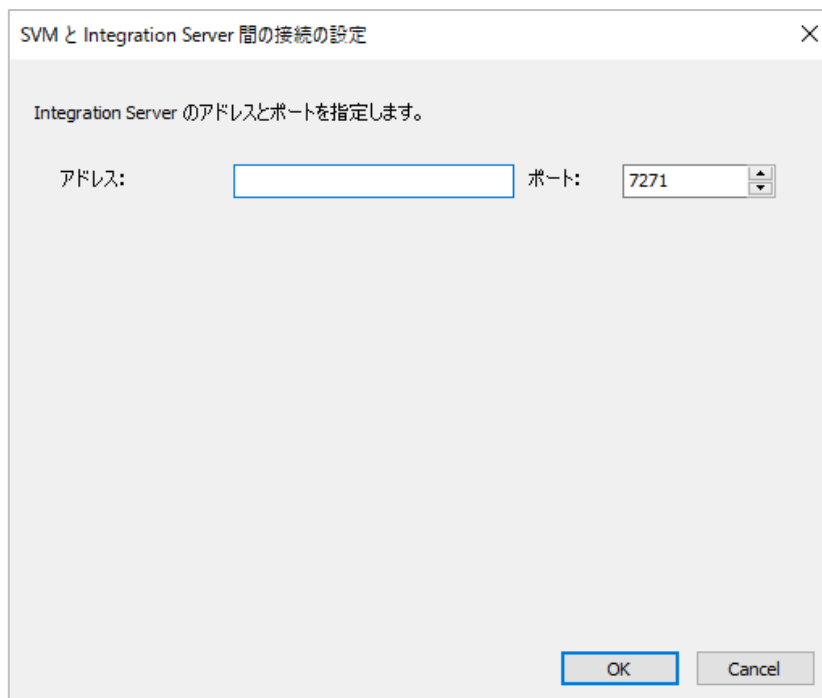
の確認が表示されます。デフォルトでは自己証明書を使用するために出ているエラーです。「無視」をクリックします。



⑨ Integration Server のアドレスを入力します。

Integration Server は KSC と同じサーバーにインストールされました。FQDN か、IP アドレスを入力します。

VMware の前提条件や Linux での使用のため、名前解決できる環境（一般的には DNS が整備された環境）を用意する必要があります。



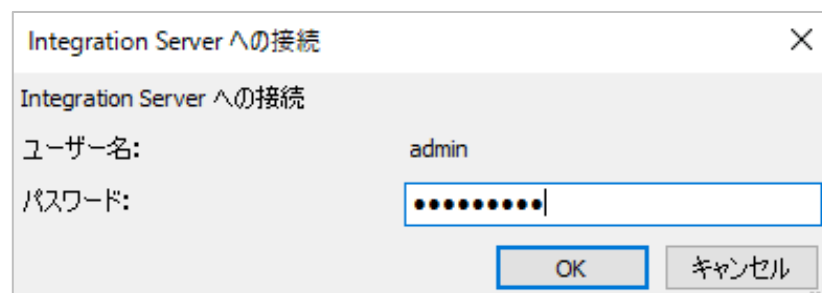
SVM と Integration Server 間の接続の設定

Integration Server のアドレスとポートを指定します。

アドレス:  ポート:

OK Cancel

⑩ KSC で使用しているパスワードを入力します。



Integration Server への接続

Integration Server への接続

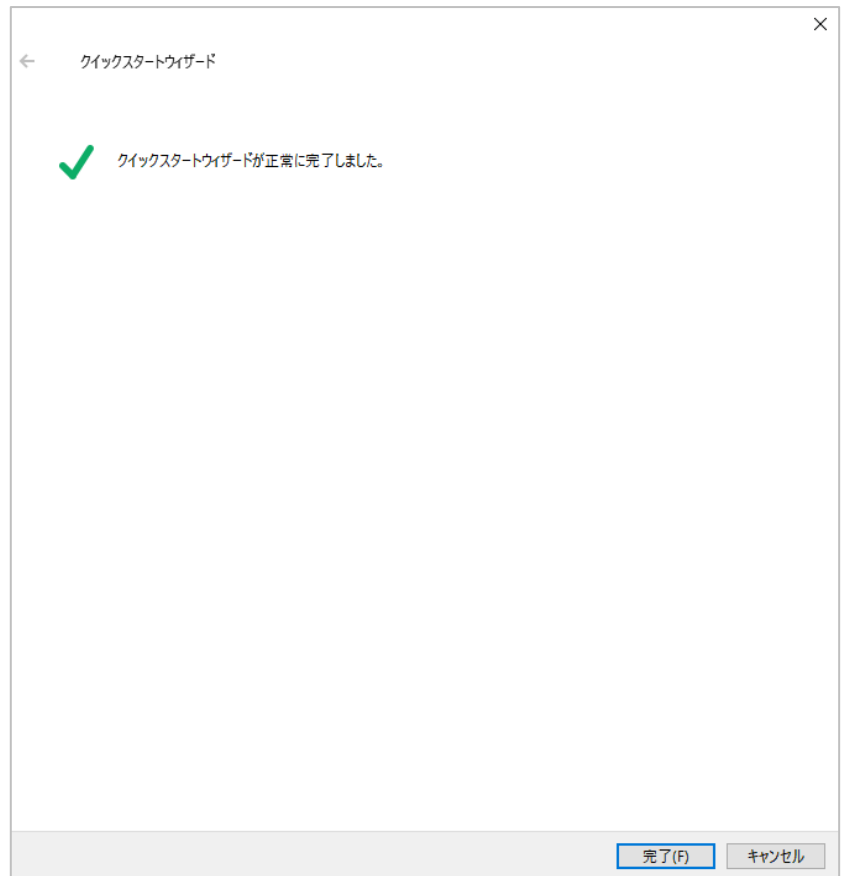
ユーザー名: admin

パスワード:

OK キャンセル

# kaspersky

- ⑪ クイックスタートウィザードが正常に完了しましたら、「完了」をクリックします。



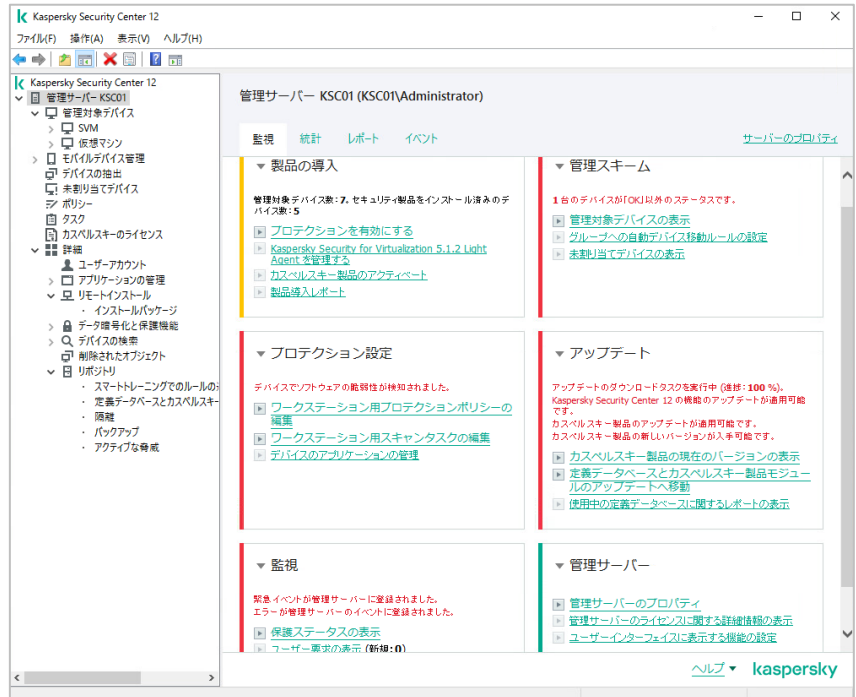
## 1.3. インターフェースの設定

KSC のインターフェース設定を行います。

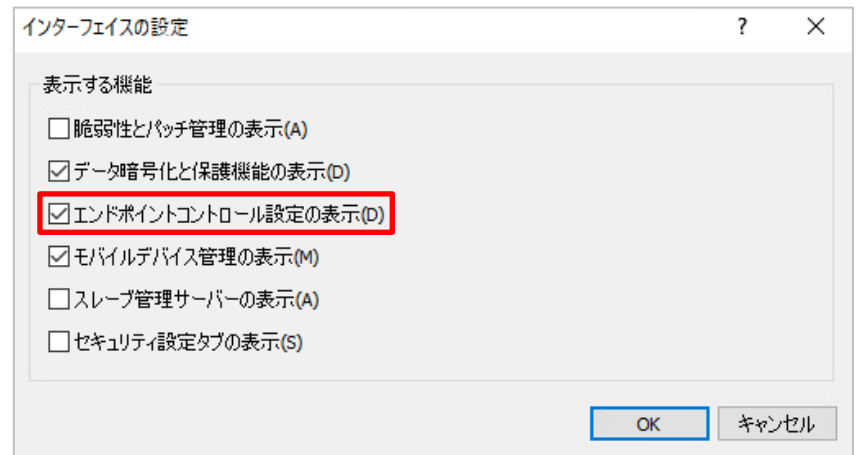
適用したライセンスで利用できる機能に応じて、KSC に表示できる機能を設定します。

KSV Light Agent では、エンドポイントコントロール設定の表示を追加する必要があります。

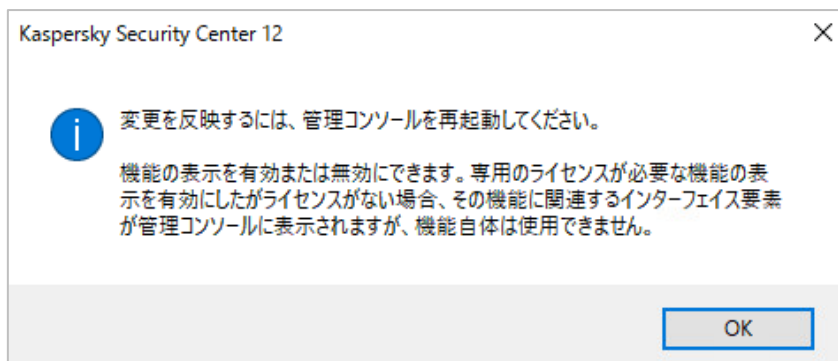
- ⑫ KSC の左メニューで、「管理サーバー」を選択します。  
表示メニュー内の「インターフェースの設定」をクリックします。



- ⑬ 「エンドポイントコントロール設定の表示」にチェックが入っていない場合は、チェックを入れ、「OK」をクリックします。



- ⑭ 管理コンソールの再起動を促すメッセージが表示されます。  
「OK」をクリックします。



- ⑮ 右上の「×」をクリックし、管理コンソールを終了させます。



- ⑯ 再度、KSC 管理コンソールを立ち上げます。



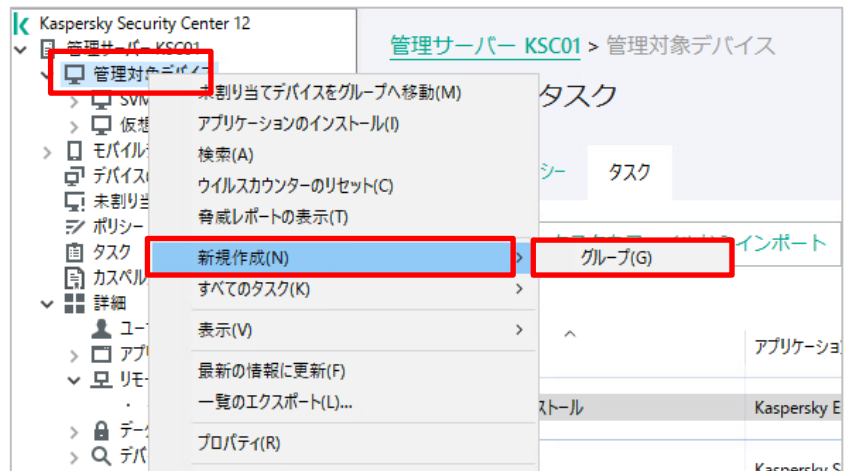
## 1.4. グループの作成

KSC は管理端末を任意のグループに分けて、それぞれに、異なるポリシーやタスクを割り当てることができます。そのため、本書では「SVM」、「仮想マシン」のグループを作成します。実際の導入時は、管理要件に従い、任意のグループを作成ください。

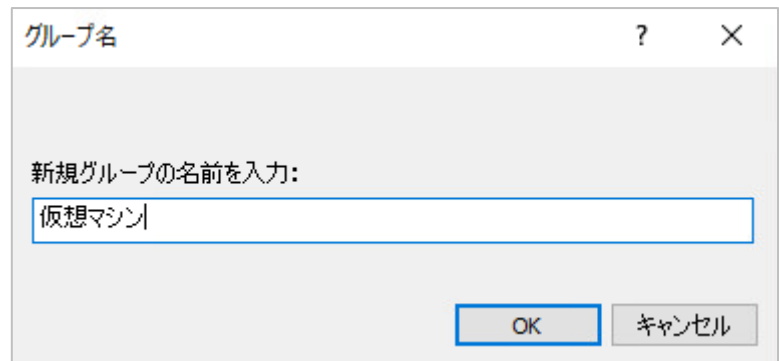
- ① KSC 左メニューの△マークをクリックし、メニューを展開させます。

- ② 「管理対象デバイス」を右クリックし、メニューを開きます。新規作成項目から、「グループ」を選択します。

本手順では、SVM、仮想マシングループを作成します。

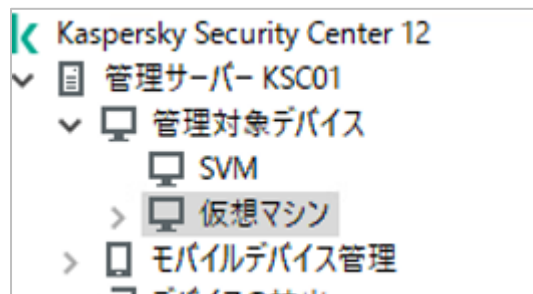


- ③ 新規グループの名前入力で、グループ名を入力します。



- ④ 同様の手順で、SVM 用のグループを作成します。

その他のグループは、環境に応じて作成してください。



## 1.5. デフォルトポリシーの作成

前項で作成したグループにポリシーを割り当てます。割り当てるポリシーの種類は下記のとおりです。SVM グループのみ SVM (Protection Server) 用ポリシーを適用しますので、ご注意ください。

- ・ SVM グループ・・・KSV LA Protection Server ポリシー
- ・ 仮想マシン グループ・・・KSV LA ポリシー

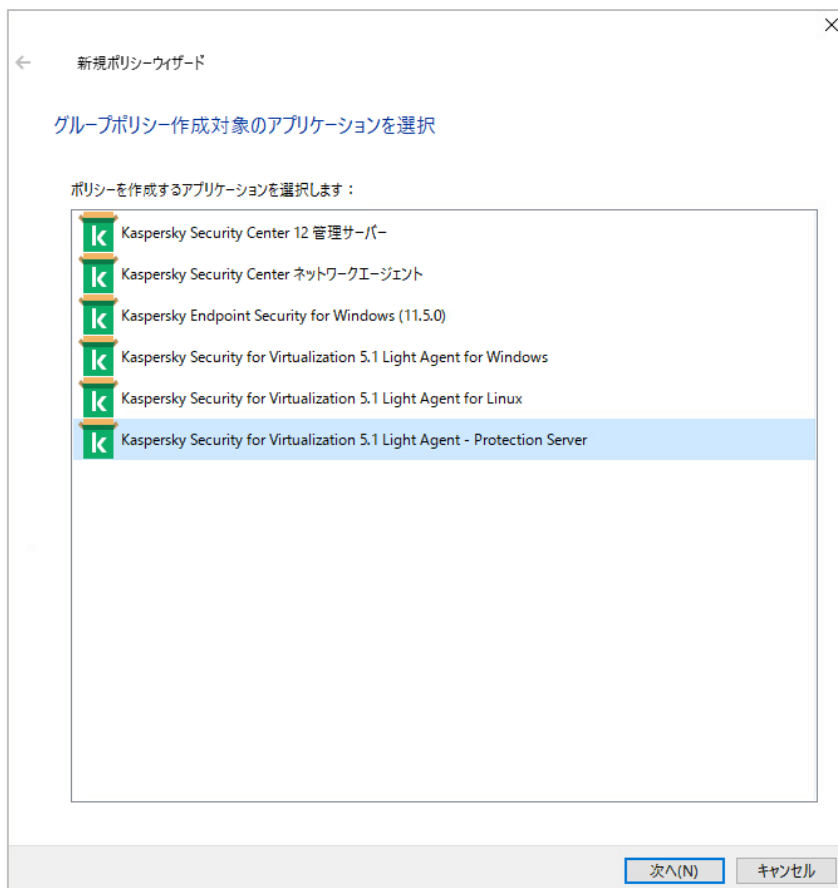
本書では、KSV LA に必要なデフォルトポリシー設定を行います。

ポリシー設定の詳細については、別紙「ポリシータスク設定ガイド」を参照ください。

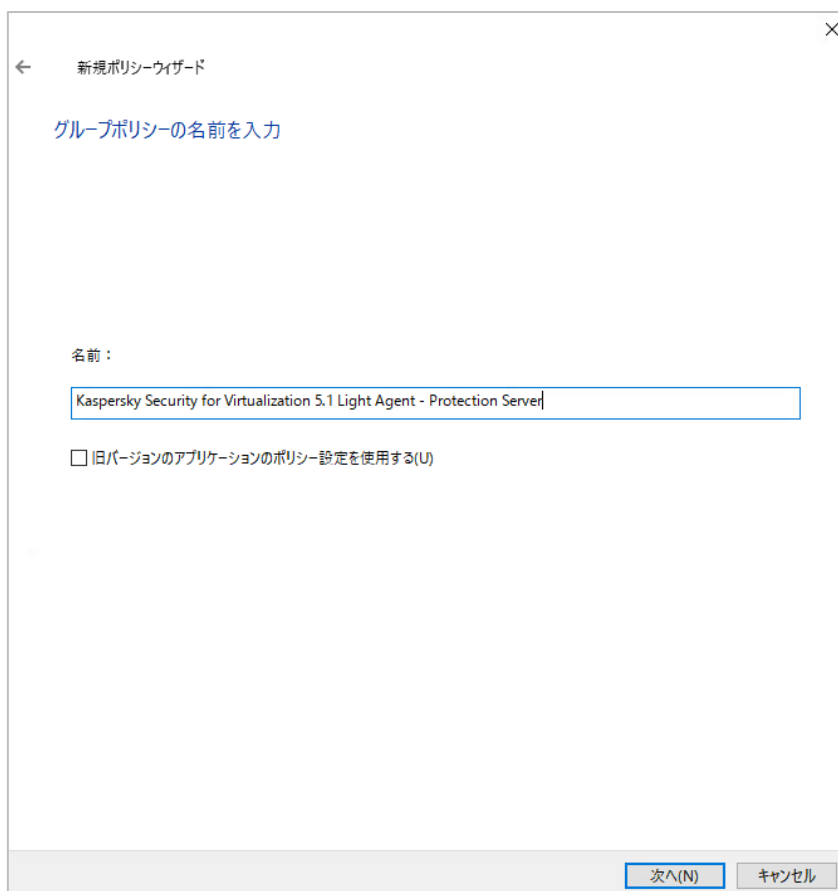
- ① KSC メニューから「SVM」グループを選択し、「ポリシーの作成」をクリックします。



- ② 「Kaspersky Security for Virtualization Light Agent –Protection Server」を選択し、「次へ」をクリックします。



- ③ 任意のポリシー名を入力し、「次へ」をクリックします。

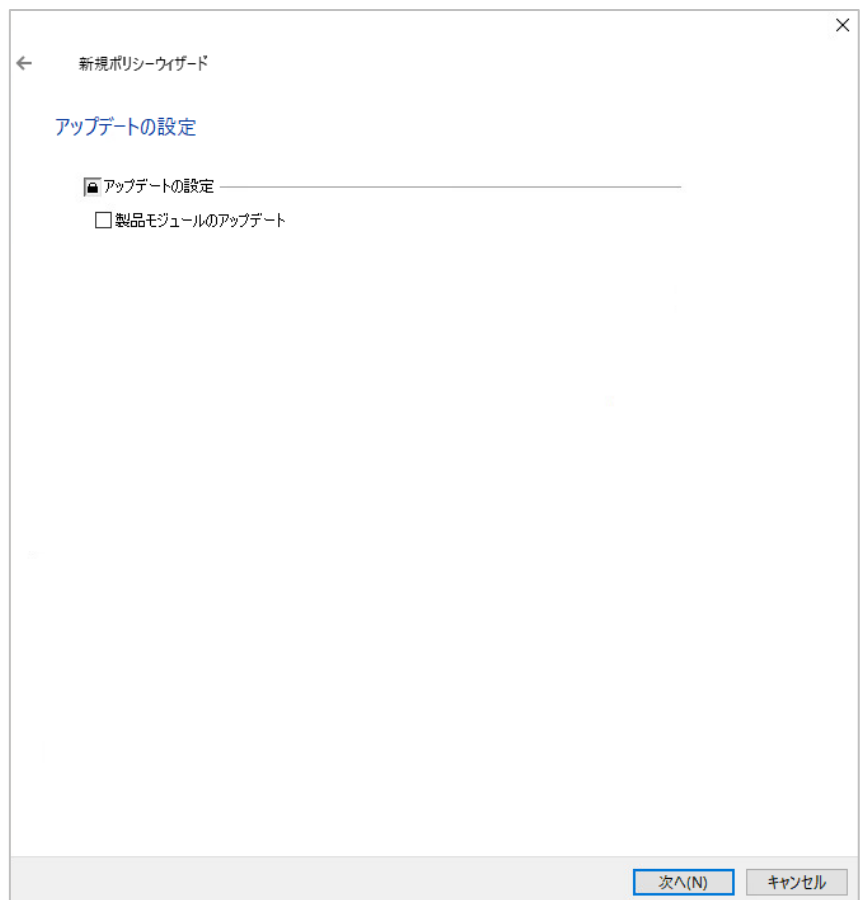


- ④ 「KSN 声明および参加条件に同意する」をチェックします。また、コンポーネントで使用する項目にもチェックし、「次へ」をクリックします

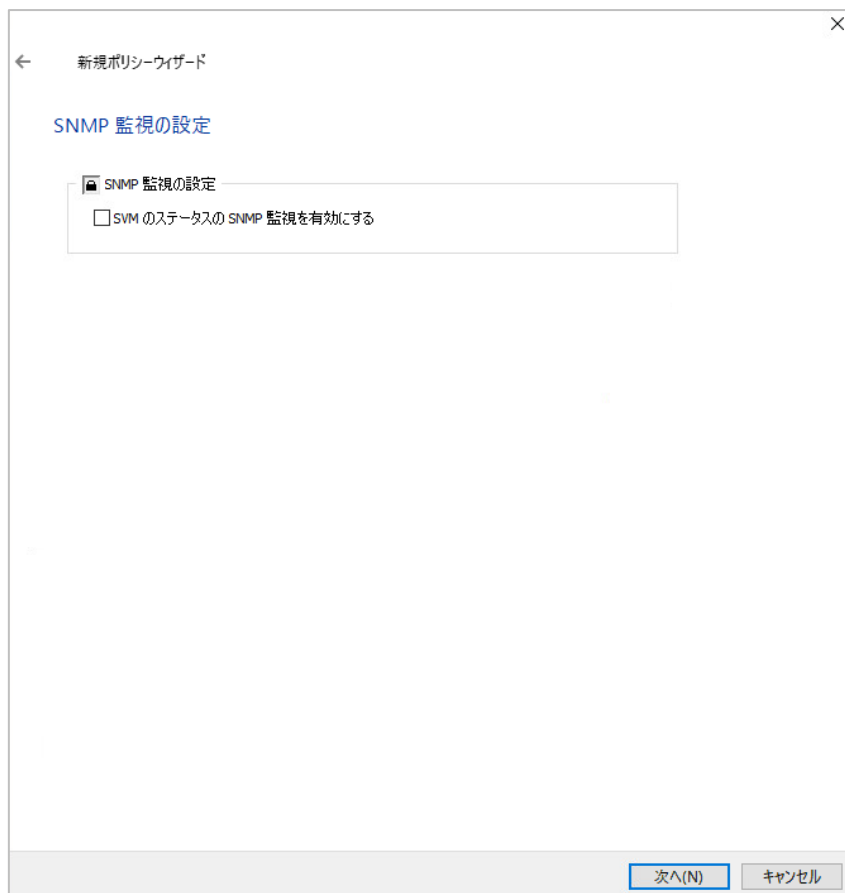


- ⑤ 「次へ」をクリックします。

製品のアップデートを自動で実施したい場合は、「製品モジュールのアップデート」のチェックを付けます。

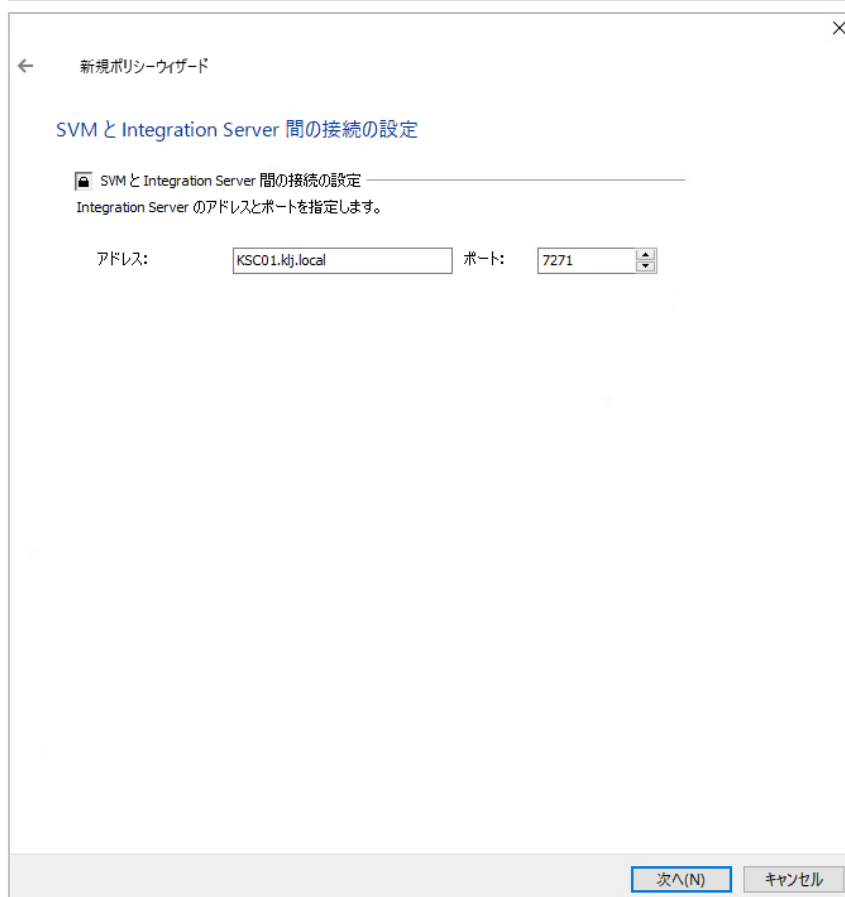


⑥

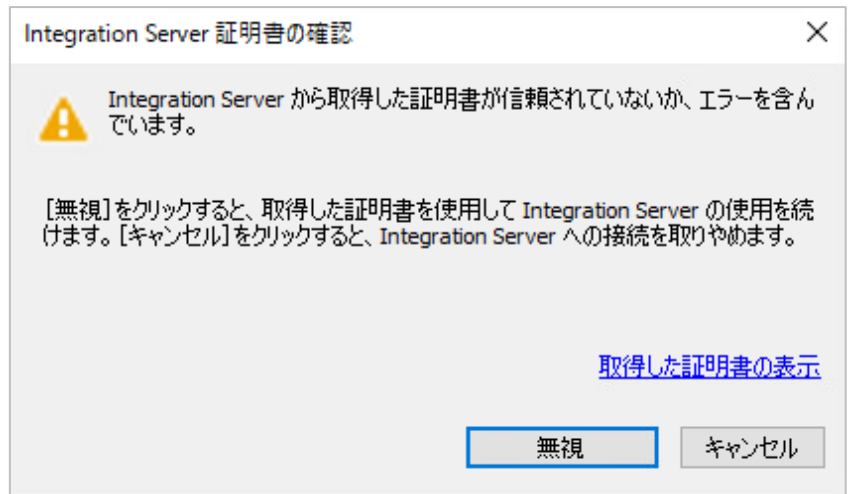


⑦ SVM の検出設定を行います。

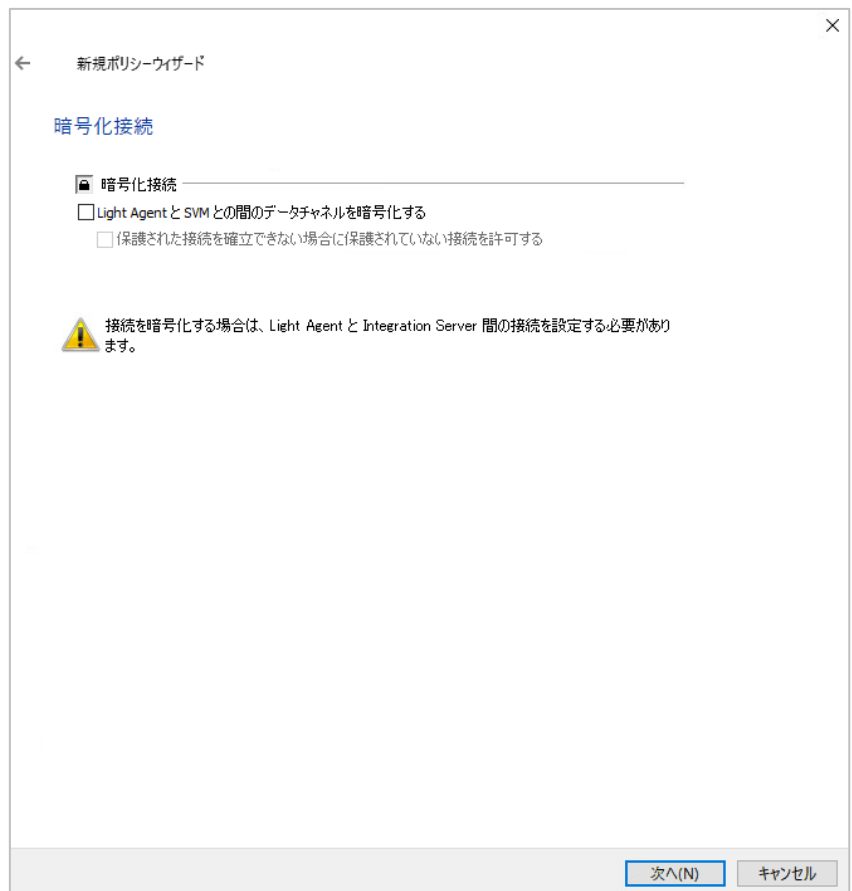
Integration Server のアドレスは、IP アドレスまたは FQDN で指定します。FQDN で設定する場合は、VM が Integration Server の名前解決ができる必要があります。



⑧ 無視をクリックします。



⑨ 「次へ」をクリックします。



⑩ 「次へ」をクリックします。

新規ポリシーウィザード

接続タグ

接続タグ

指定したタグを使用した Light Agent の接続を許可する:

例: tag1

この機能が使用できるのは、本製品を Enterprise ライセンスで使用する場合のみです。

次へ(N) キャンセル

⑪ アクティブポリシーが選択されていることを確認し、「完了」をクリックします。

新規ポリシーウィザード

アプリケーションのグループポリシーを作成

[終了] をクリックし、「Kaspersky Security for Virtualization 5.1 Light Agent - Protection Server」の作成処理を完了し、ウィザードを閉じます。

ポリシーのステータス:

アクティブポリシー

非アクティブポリシー

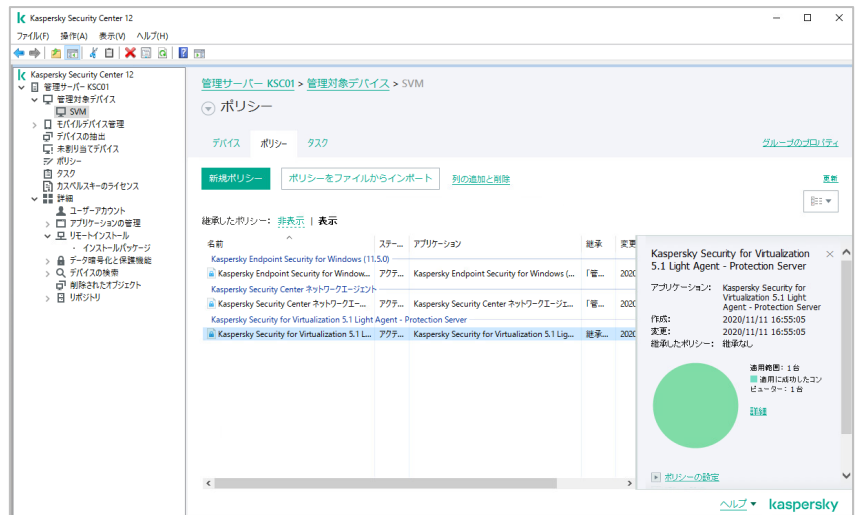
ポリシーの作成後すぐにプロパティを開く

完了(F) キャンセル

## ⑫ 「Kaspersky Security for Virtualization Light Agent Protection Server」

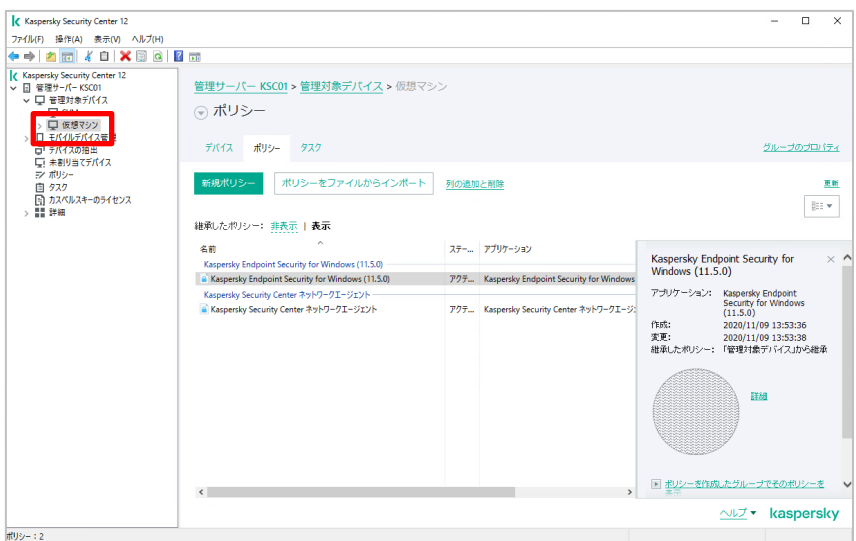
ポリシーが作成されていることを確認します。

**未だ、SVM をインストールしていないため、管理対象はありません。**



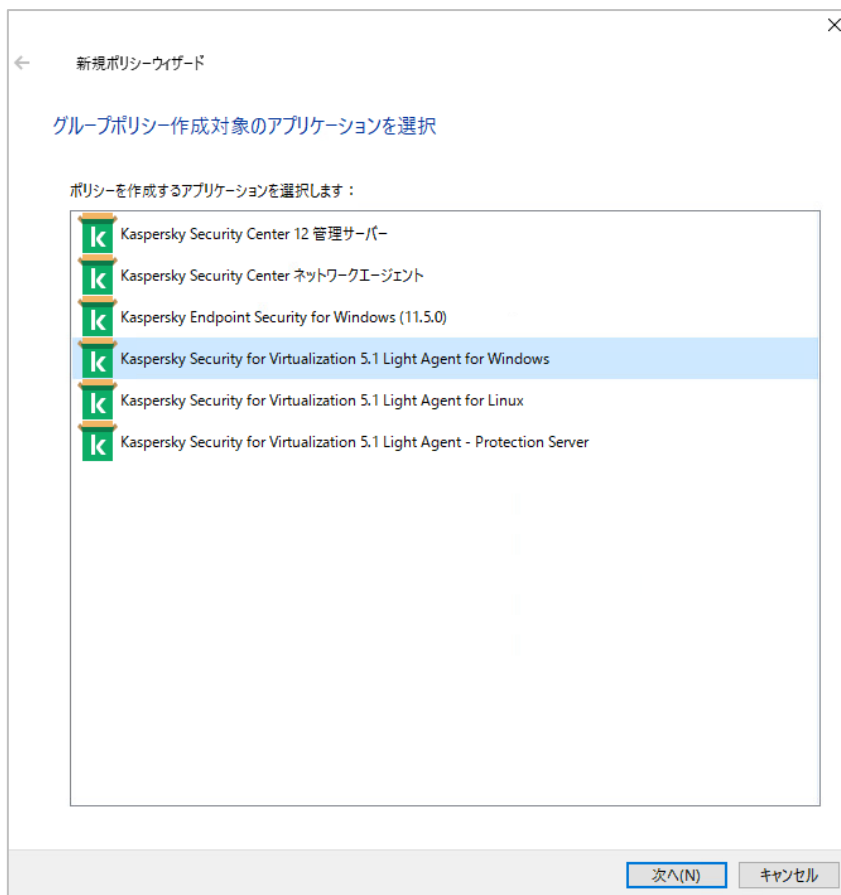
## ⑬ 引き続き、KSV LA のデフォルトポリシーを作成します。

「仮想マシン」グループを選択し、「ポリシーの作成」をクリックします。

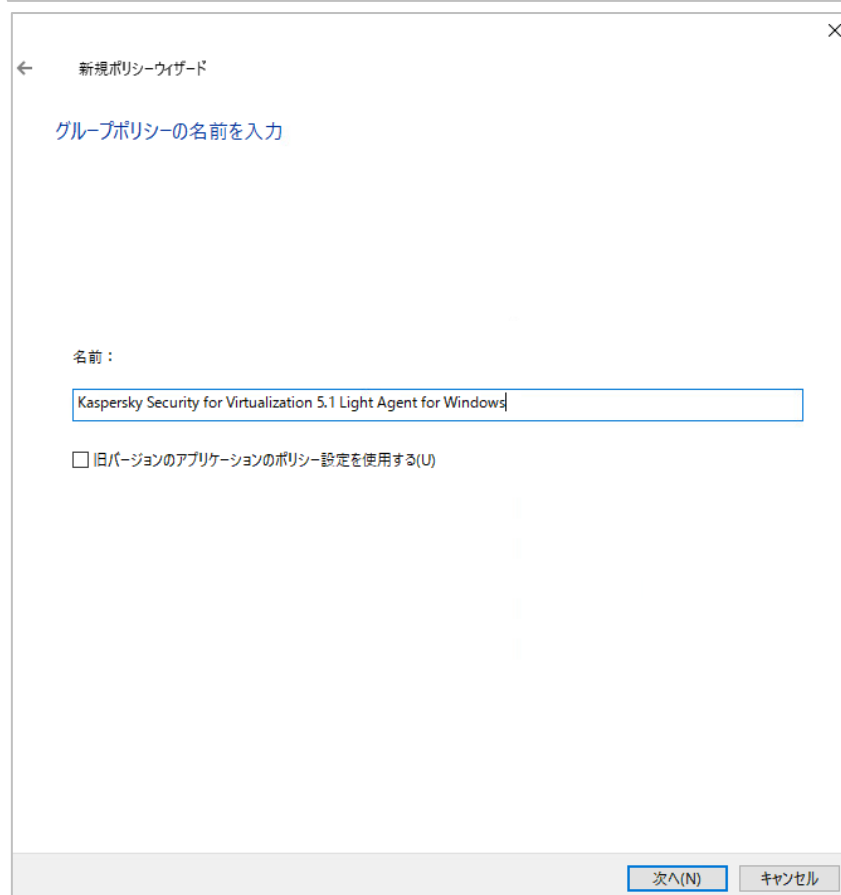




- ⑭ 「Kaspersky Security for Virtualization Light Agent for Windows」を選択し、「次へ」をクリックします。

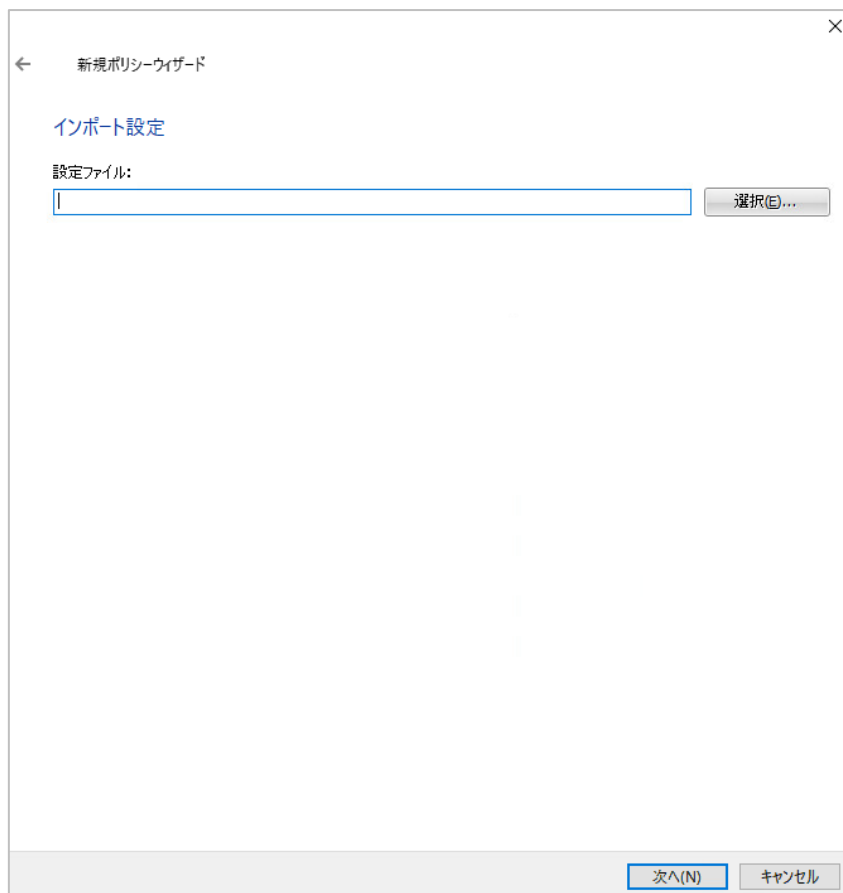


- ⑮ 任意のポリシー名を設定し、「次へ」をクリックします。



⑩ 「次へ」をクリックします。

※ インポート設定は、別途エクスポートしたポリシー設定ファイルを使用したい場合を選択します。

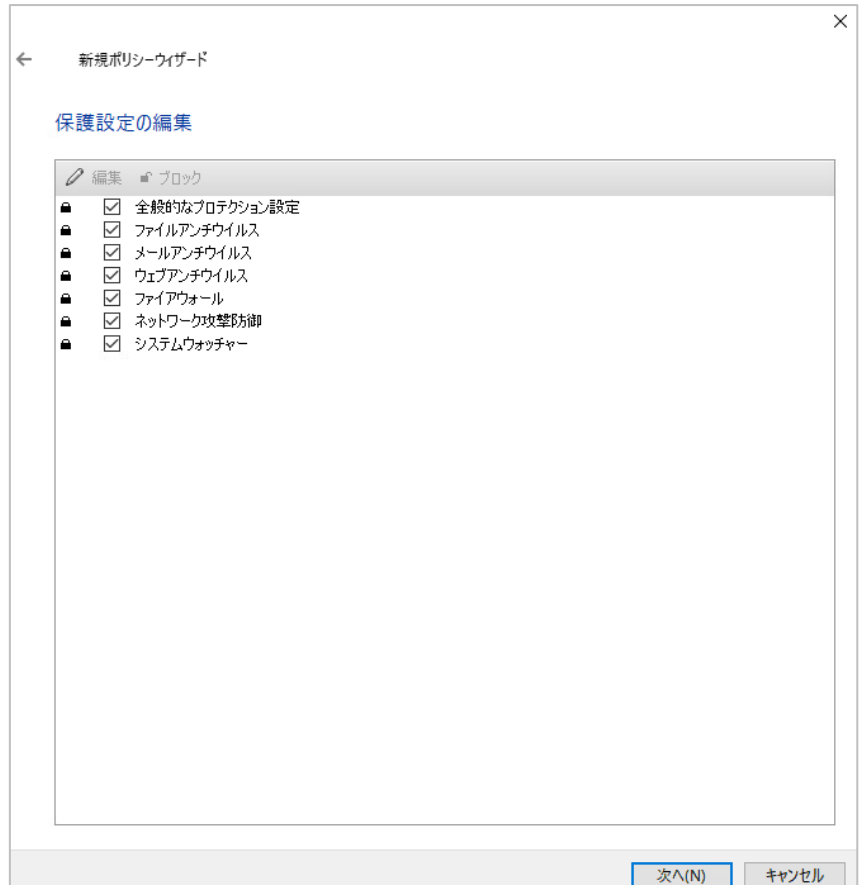


⑪ 利用するコントロール機能にチェックがあることを確認して、「次へ」をクリックします。

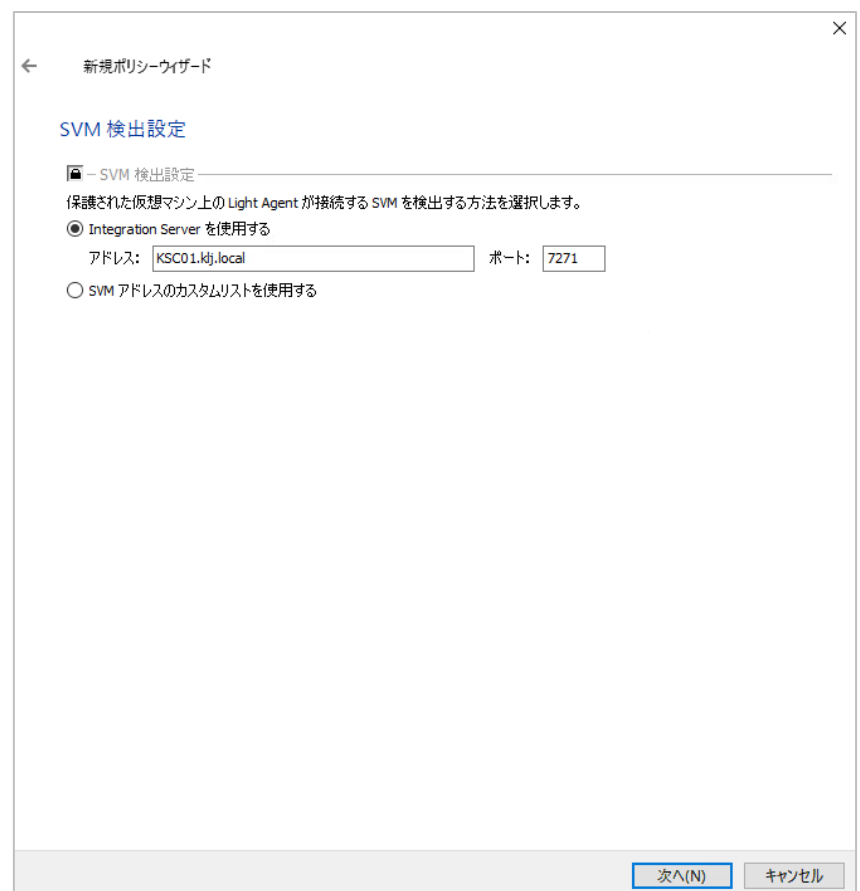
ポリシーは後から変更出来ます。



- ⑱ 利用するマルウェア保護機能にチェックがあることを確認して、「次へ」をクリックします。



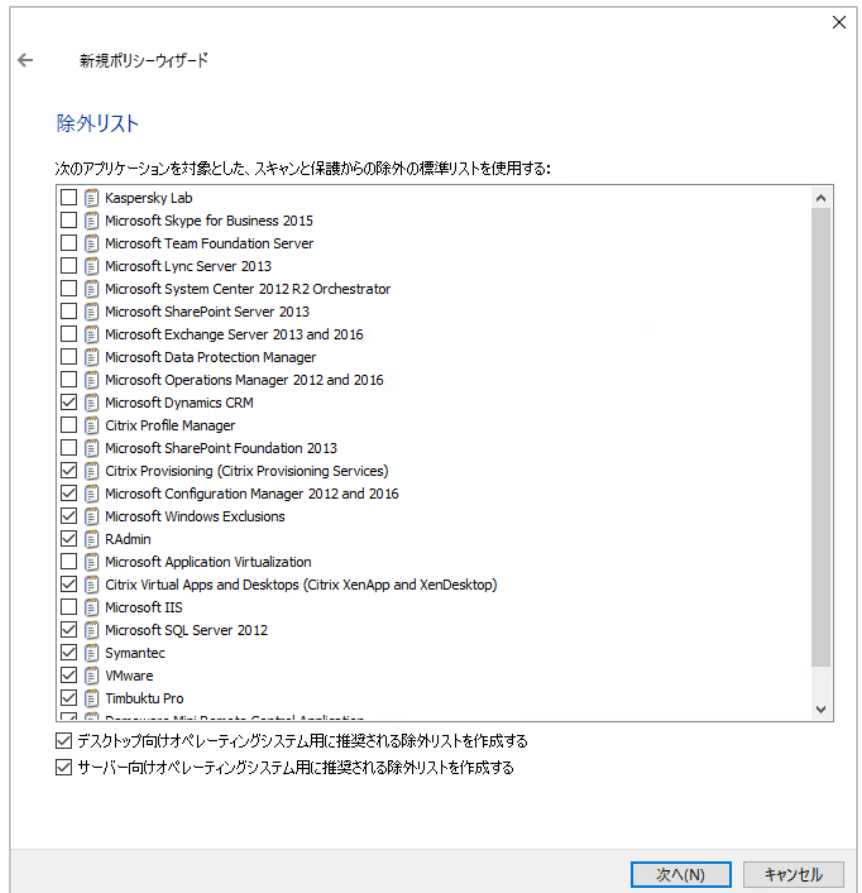
- ⑲ SVM 検索設定を実施します。通常は「マルチキャストを使用する」を選択し、「次へ」をクリックします。



⑳



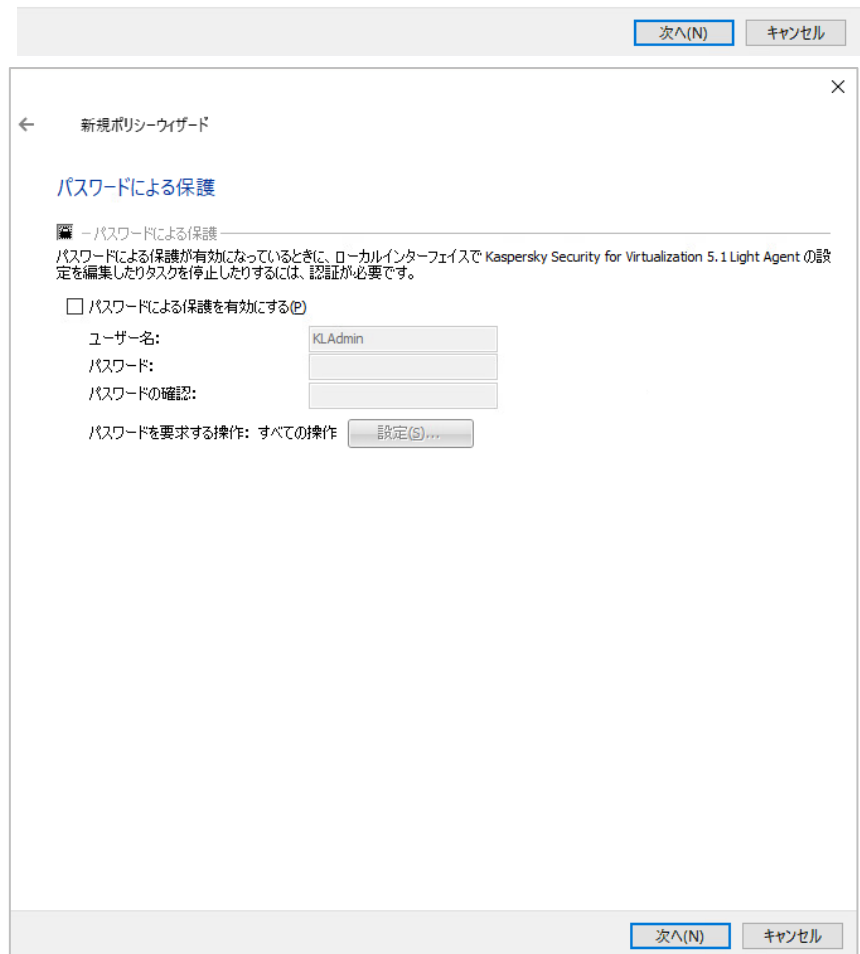
21「次へ」をクリックします。



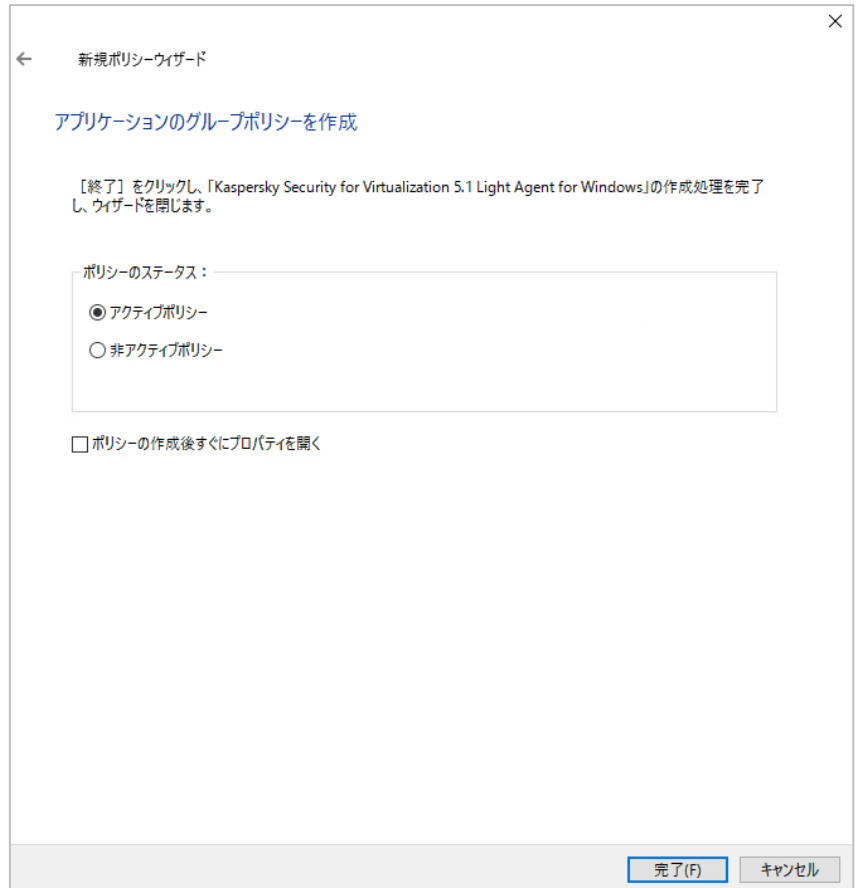
22「次へ」をクリックします。



23 ユーザーによる Light Agent の設定編集やタスク停止を禁止する場合は、パスワード設定を行います。



24 「アクティブポリシー」を選択し、「完了」をクリックします。



25 「Kaspersky Security for Virtualization Light Agent for Windows」ポリシーが作成されていることを確認します。

**未だ、Light Agent for Windows をインストールしていないため、管理対象はありません。**

## 1.6. デフォルトタスクの作成

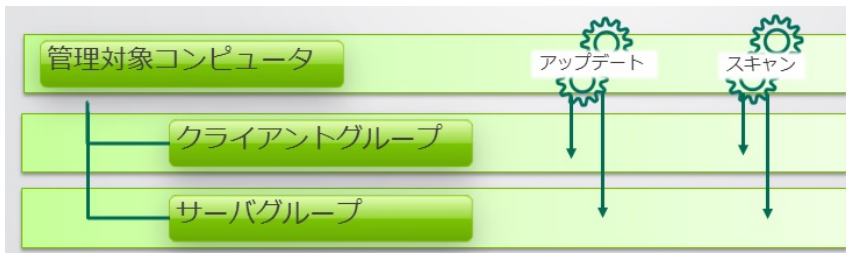
KSC から管理端末にスキャンやアップデートの指示をする際に「タスク」という概念を使用します。

クイックスタートウィザード時にデフォルトタスクが自動的に作成されています。

デフォルトタスクは KSC 左メニューの管理対象コンピューター（ルートグループ）に割り当てられており、デフォルトでは、そのタスク設定が配下のグループに強制的に継承される仕組みになります。

継承除外のグループを設定することで、グループごとに柔軟なスケジュール設定が可能となります。

### ■グループへのタスク継承イメージ図



### ■KSV Light Agent の必須タスク説明

タスク名	タスク実行コンポーネント	タスクの役割
リポジトリへのアップデートのダウンロード	Kaspersky Security Center 12 管理サーバー	インターネット上のカスペルスキー定義 DB 配信サーバーから、定義 DB を管理サーバーのリポジトリにダウンロードします。 デフォルトでは、1 時間に 1 回ダウンロードを行う設定になっています。
定義データベースのアップデートタスク	Kaspersky Security for Virtualization Light Agent - Protection Server	管理サーバーのリポジトリにダウンロードされた定義 DB を SVM に配信します。 デフォルトでは、新しい定義 DB がリポジトリにダウンロードされ次第配信する設定になっています。
ウイルススキャン	Kaspersky Security for Virtualization Light Agent for Windows または Linux	各仮想マシンのウイルススキャンを実施します。 デフォルトでは、手動実行する設定になっています。

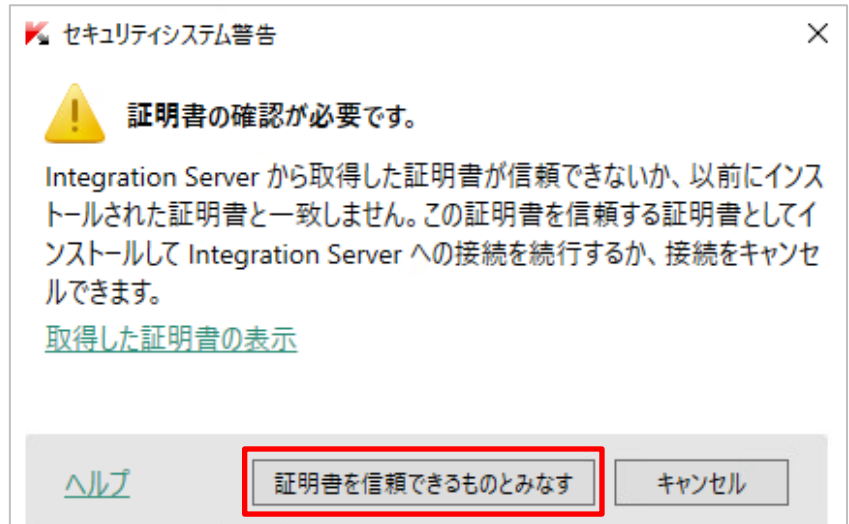
## 2. SVM (Protection Server コンポーネント) の導入

### 2.1. SVM の導入

- ① 「Kaspersky Security for Virtualization Light Agent を管理する」をクリックします。



- ② 「証明書を信頼できるものとみなす」をクリックします。

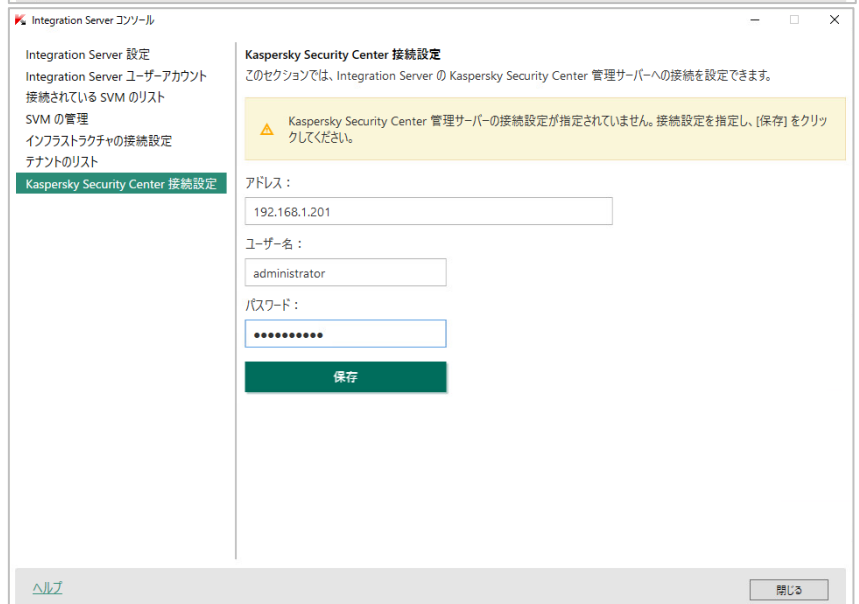
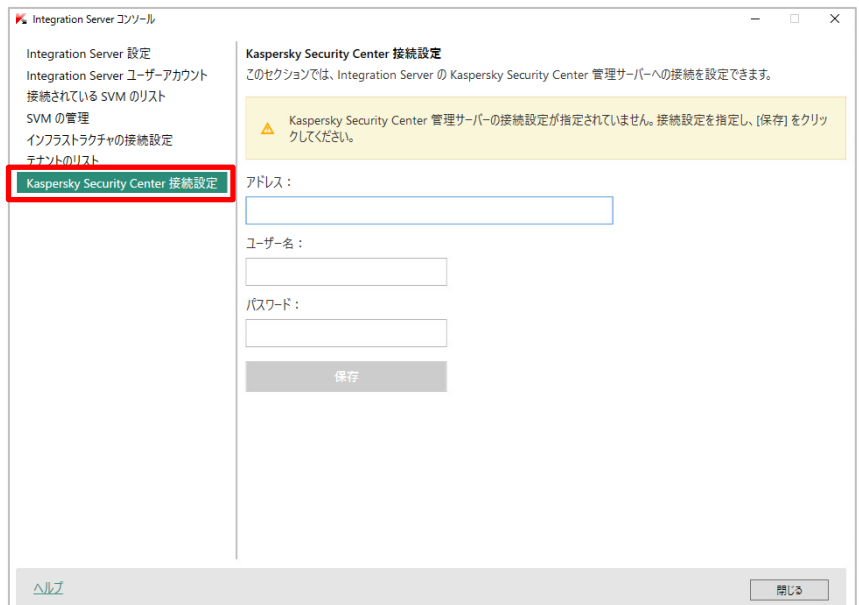




③ 画面が切り替わります。



④ Kaspersky Security Center 接続設定をクリックします。Kaspersky Security Center のアドレス、管理者アカウント、パスワードを入力します。



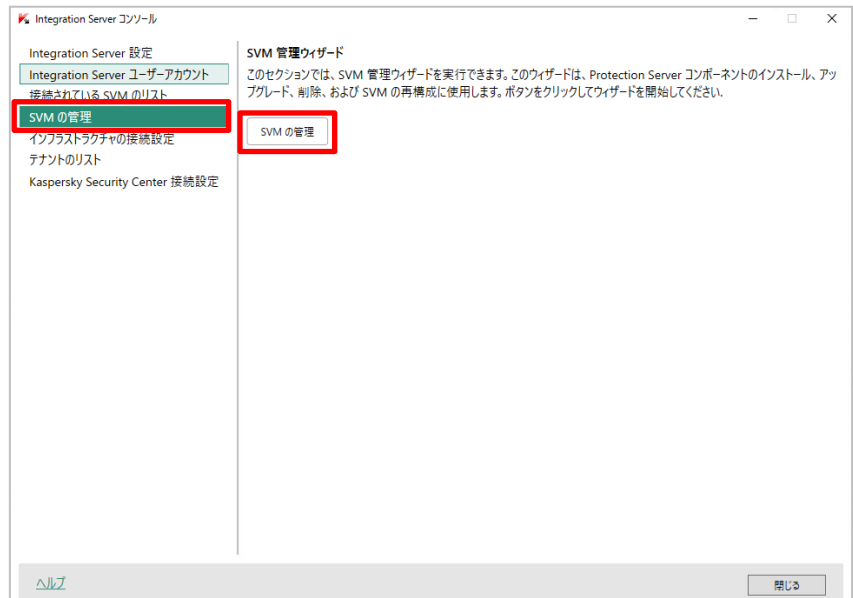
- ⑤ 「証明書をインストール」をクリックします。



- ⑥ 「保存」をクリックします。



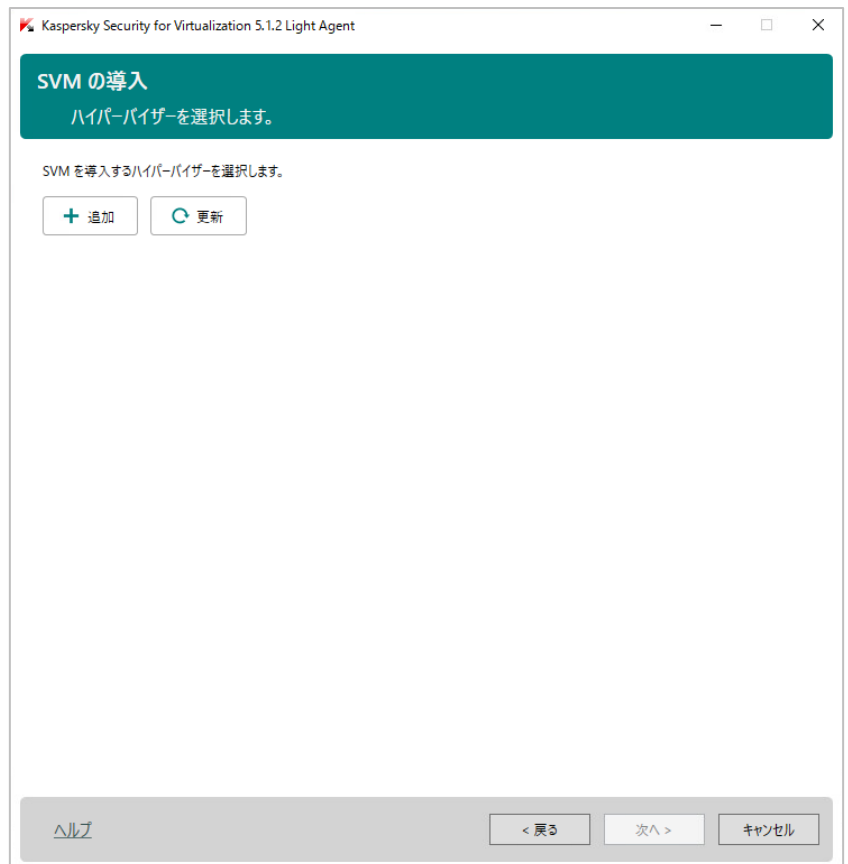
- ⑦ SVM の管理をクリックし、「SVM の管理」ボタンをクリックします。



- ⑧ 「SVM の導入」を選択し、「次へ」をクリックします。



- ⑨ 「追加」をクリックします。



- ⑩ ハイパーバイザーの種別を選択します。

仮想インフラストラクチャの接続設定

### 仮想インフラストラクチャ

種別： VMware vCenter Server

アドレス：  
認識されたアドレスの数： 0

### 管理者アカウント

SVM の導入、削除、再設定に使用されるアカウント。

ユーザー名：  
パスワード：

読み取り専用権限を持つアカウント

Integration Server と仮想インフラストラクチャの接続に使用するアカウント。

[ヘルプ](#)      接続      キャンセル

種別： VMware vCenter Server

アドレス： VMware vCenter Server  
Windows Server Hyper-V (ハイパーバイザー / クラスター)  
Microsoft SCVMM  
Citrix Hypervisor (Citrix XenServer)  
KVM  
Proxmox VE  
Skala-R Management

管理者アカウント

SVM の導入、削除

ユーザー名： HUAWEI FusionCompute VRM  
Nutanix Prism

パスワード：

⑪ アドレスを入力します。

vCenter Server の IP アドレスまたは完全ドメイン名を入力してください。

vCenter Server のユーザー名とパスワードを入力し、「接続」をクリックします。

仮想インフラストラクチャの接続設定

仮想インフラストラクチャ

種別: VMware vCenter Server

アドレス: 192.168.1.61

認識されたアドレスの数: 1

管理者アカウント

SVM の導入、削除、再設定に使用されるアカウント。

ユーザー名: administrator@klj.local ✓

パスワード: ●●●●●●●●●● ✓

読み取り専用権限を持つアカウント

Integration Server と仮想インフラストラクチャの接続に使用するアカウント。

ヘルプ 接続 キャンセル

⑫ 「証明書が認証済みであるとみなす」をクリックします。。

セキュリティシステム警告

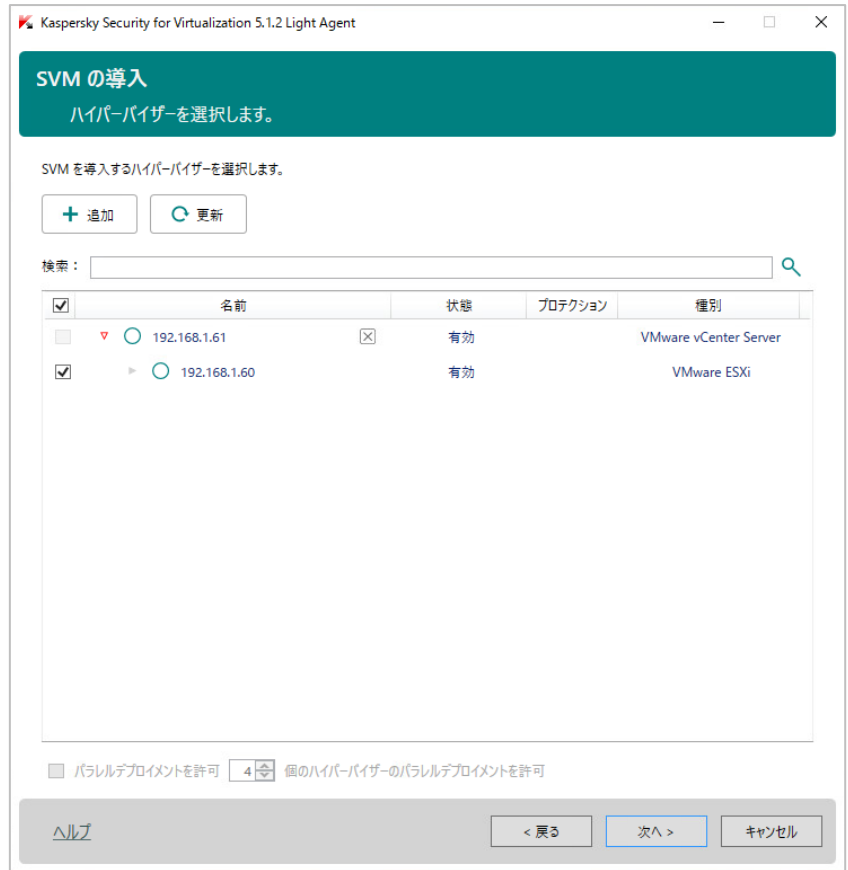
! 証明書の正当性の確認が必要です。

ハイパーバイザーまたは仮想インフラストラクチャ管理サーバー 192.168.1.61:443 から受け取った証明書が信頼されていないか、前回インストールした証明書と一致しません。証明書の正当性を確認し、接続を継続するか中止するかを選択してください。

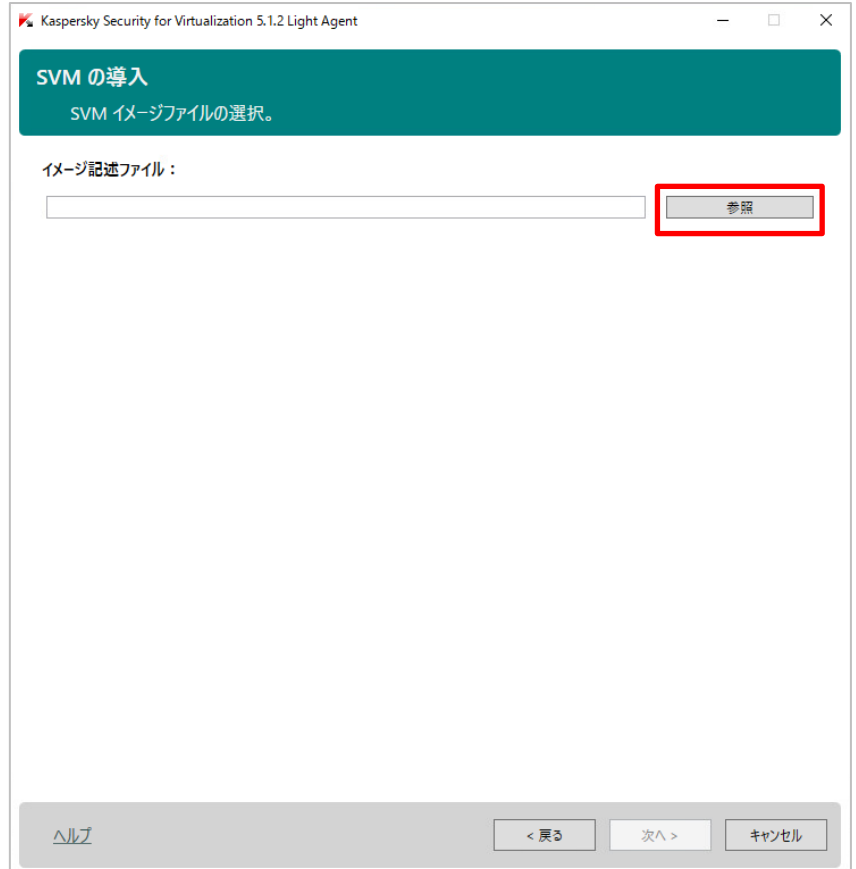
[取得した証明書の表示](#)

証明書が認証済みであるとみなす キャンセル

- ⑬ 接続に成功すると、vCenter および ESXi ハイパーバイザーの IP アドレスまたは完全ドメイン名が表示され、名前の左に緑色の「○」が表示されます。導入対象ハイパーバイザーをチェックし、「次へ」をクリックします。

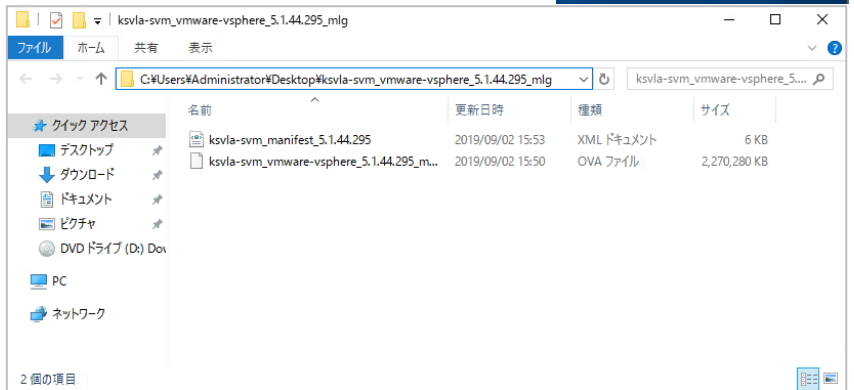
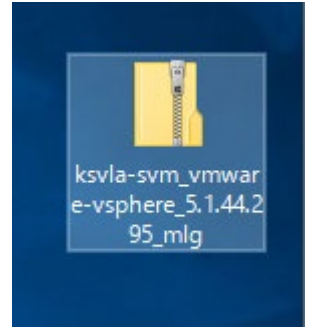


- ⑭ SVM イメージファイルの選択画面にて、「参照」をクリックします。

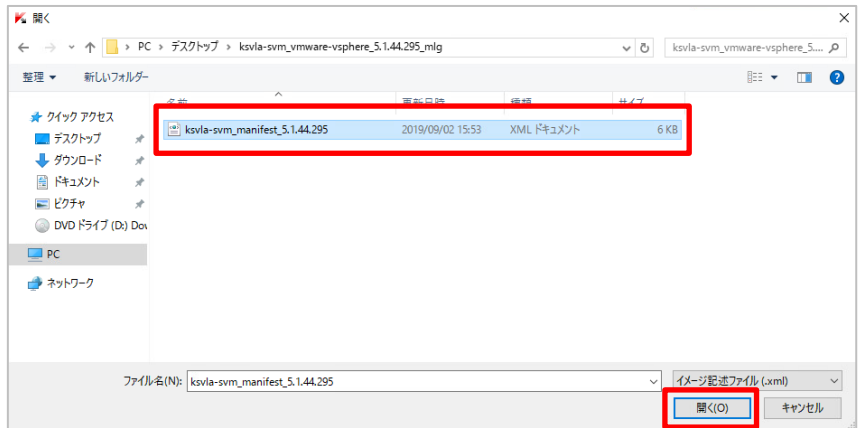


# kaspersky

イメージファイルは ZIP で提供されていますので、展開しておきます。



- ⑮ 展開しておいた SVM イメージファイルを選択し、「開く」をクリックします。



- ⑩ VMware vSphere のイメージの完全性項目で「検証」をクリックします。

VMware vSphere イメージの完全性が「検証済み」となったことを確認し、「次へ」をクリックします。





- ⑰ 任意の SVM 名、保管領域  
(データストア名)、  
ネットワーク名を設定し、  
「次へ」をクリックします。

保護対象の仮想マシンが分散  
スイッチを使用している場合は、  
SVM を分散スイッチに配置する  
など、適切に設定します。後に  
vCenter から変更することも可  
能です。



- ⑱ SVM ネットワーク設定を  
行います。



- ⑱ IP アドレス、サブネットマスク、ゲートウェイ、DNS、代替 DNS を入力し、「次へ」をクリックします。



- ⑳ SVM が接続する Kaspersky Security Center の FQDN(IP アドレス)、ポート番号、SSL ポート番号を設定します。



21 SVM の設定パスワードと  
ルートアカウントパスワードを  
設定します。

任意で、SSH 接続の  
許可設定を実施します。

※ 設定パスワードは「SVM」の  
再設定時に入力するパスワード  
です。

ルートアカウントパスワードは、  
SSHなどで、SVMに直接  
アクセスする際の「root」  
アカウントパスワードです。

22 「次へ」をクリックします。

Kaspersky Security for Virtualization 5.1.2 Light Agent

### SVM の導入

SVM でのアカウントの設定。

klconfig アカウント

klconfig アカウントのパスワードを作成します (設定パスワード)。  
この設定パスワードは、SVM 設定を変更する際に必要になります。

パスワード:

確認:

ルートアカウント

ルートアカウントパスワードを作成します。  
このルートアカウントは、SVM ログおよび Kaspersky Security ログでオペレーティングシステムにアクセスする際に使用されます。

パスワード:

確認:

リモートルートアカウントアクセス

ルートアカウントに対して SSH を使用したリモートアクセスを許可する

< 戻る    次へ >    キャンセル

Kaspersky Security for Virtualization 5.1.2 Light Agent

### SVM の導入

導入の開始。

一般的な導入設定:

SVM イメージ記述ファイル: C:\Users\Administrator\Desktop\ksvla-svm\_vmware-vsphere\_5.1.44.295\_mlg\ksvla-svm\_manifest\_5.1.44.295.xml

SVM ネットワーク設定: 静的 IP アドレス割り当て

SSH を使用したリモートルートアカウントアクセス: 許可

Kaspersky Security Center 接続設定: ksc01.klj.local : 14000/13000

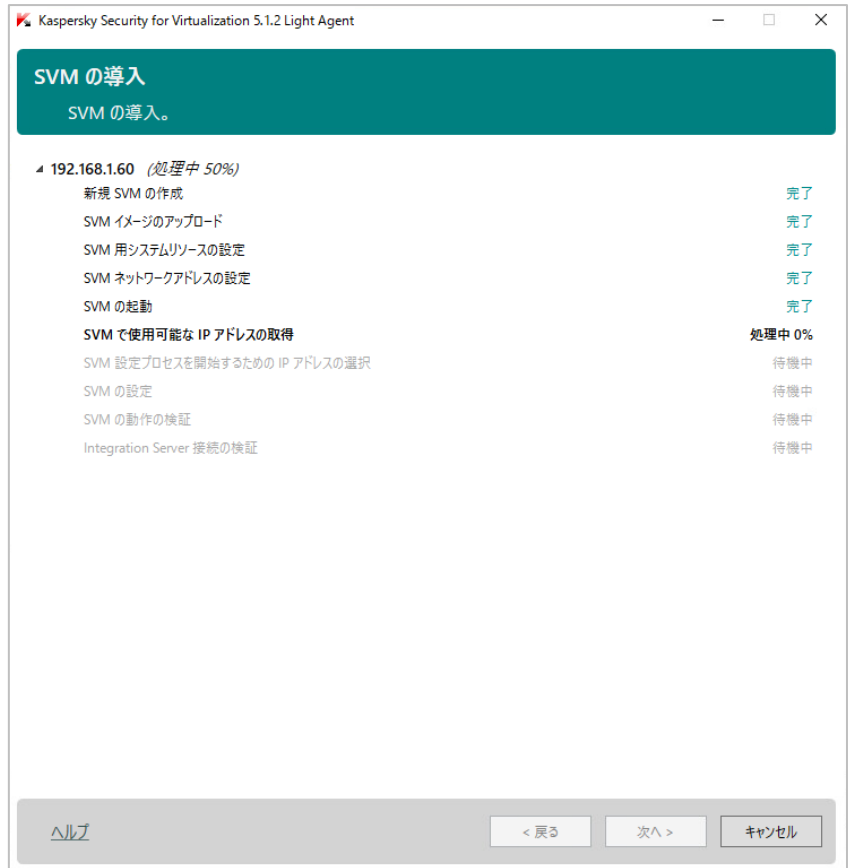
パラレルデプロイメント: 1

各ハイパーバイザー用の設定の詳細:

ハイパーバイザー	SVM 名	保管領域	ネットワーク名	IP アドレス	サブネットマ
192.168.1.60	la-svm-192-168-...	datastore1	VM Network	192.168.1.70	255.255.255

< 戻る    次へ >    キャンセル

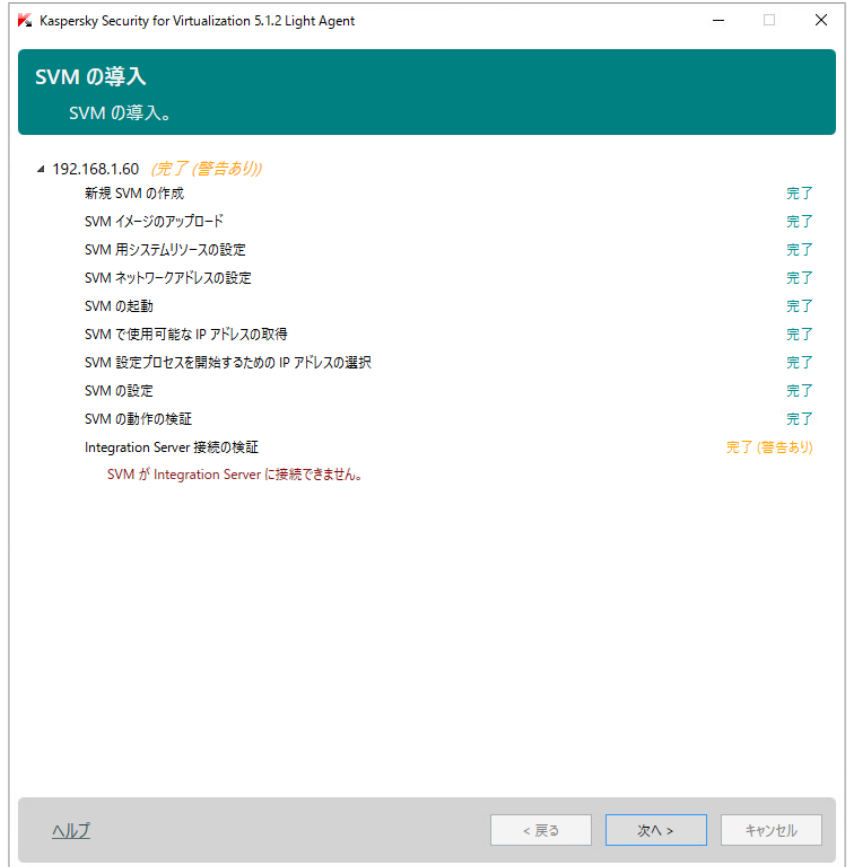
23 完了を待ちます。



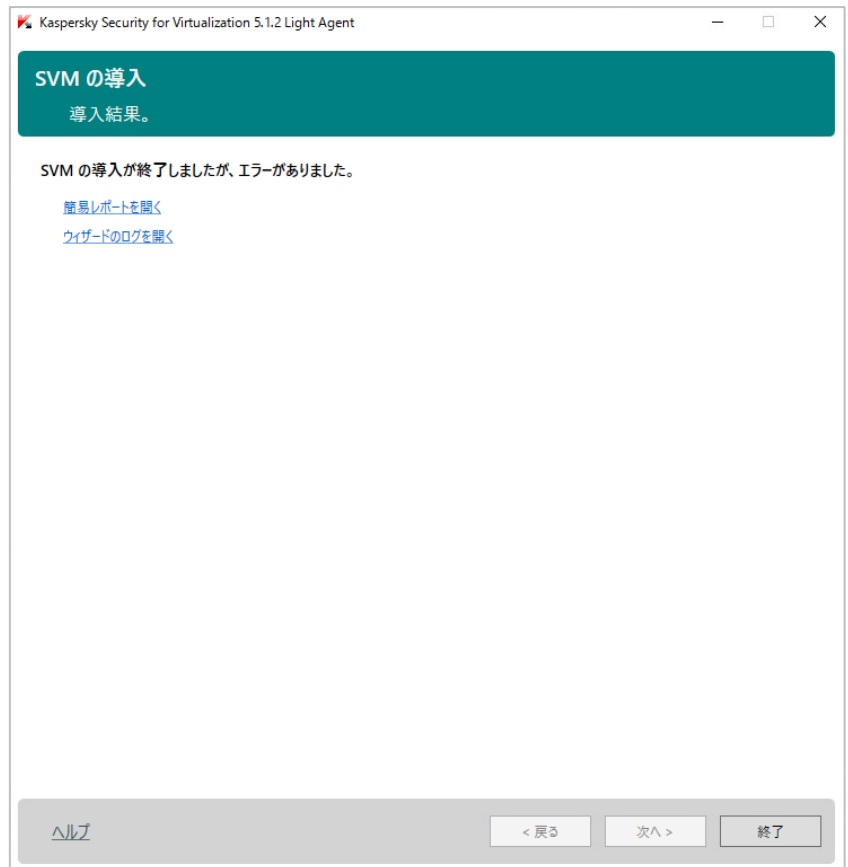
24 SVM のインストールが

完了ステータスになったことを  
確認し、「次へ」をクリックします。

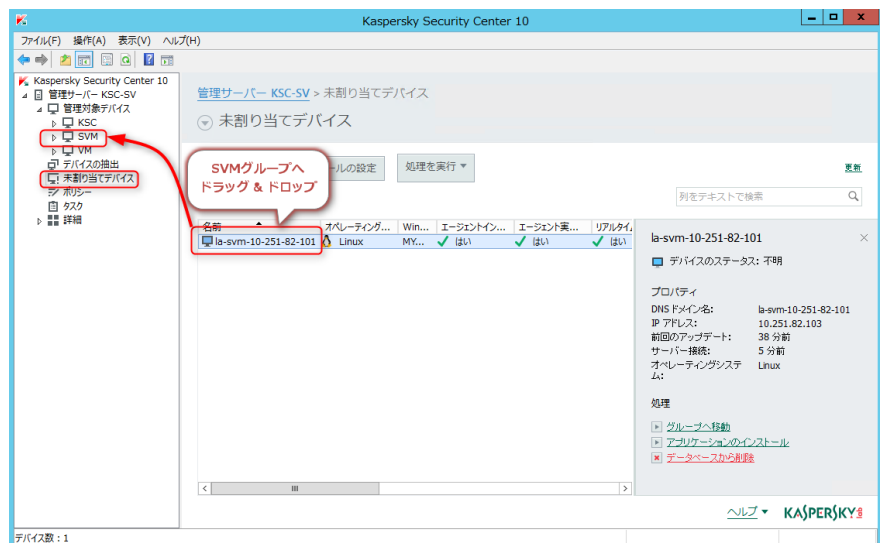
「SVM が Integration  
Server に接続できません」警  
告は無視して構いません。



25 SVM 導入が完了したことを確認し、「終了」をクリックします。



26 未割り当てグループ配置された SVM を SVM グループに配置します。



27 SVM グループに SVM が  
配置されたことを確認します。

The screenshot shows the Kaspersky management console interface. At the top, there are tabs for 'デバイス' (Devices), 'ポリシー' (Policies), and 'タスク' (Tasks). A 'グループのプロパティ' (Group Properties) link is visible in the top right. Below the tabs, there are buttons for 'デバイスをグループに移動' (Move devices to group), '新規グループ' (New group), '処理を実行' (Execute), and '列の追加と削除' (Add and remove columns). A search bar contains the text 'フィルターが指定されていません。レコードの合計: 1' (No filter specified. Total records: 1). Below the search bar, there are status indicators: '緊急: 0' (Critical: 0), '警告: 0' (Warning: 0), and 'OK: 1' (OK: 1). A table lists the devices with columns for '名前' (Name), '前回の管理サー...' (Last management server), 'ネットワークエジ...' (Network edge), 'リアル...' (Real-time), and '作成日' (Creation date). The first row shows a device named 'la-svm-192-168-1-60' with a status of 'はい' (Yes) and a creation date of '32 分前' (32 minutes ago). To the right of the table, a detailed view for the device 'la-svm-192-168-1-60' is shown, indicating that the device status is 'OK/可視' (OK/Visible) and the last connection to the management server was '1 分前' (1 minute ago). Below this, the 'プロパティ' (Properties) section lists: 'DNS ドメイン名: la-svm-192-168-1-60', 'IP アドレス: 192.168.1.70', '保護ステータス: 実行中 (推奨レベル)' (Protection status: In progress (Recommended level)), and 'スキャンからの保護ス...' (Protection from scan...).

名前	前回の管理サー...	ネットワークエジ...	リアル...	作成日
la-svm-192-168-1-60	1 分前	はい	実行中	32 分前

la-svm-192-168-1-60

- デバイスのステータス: OK/可視
- 前回の管理サーバーへの接続: 1 分前

プロパティ

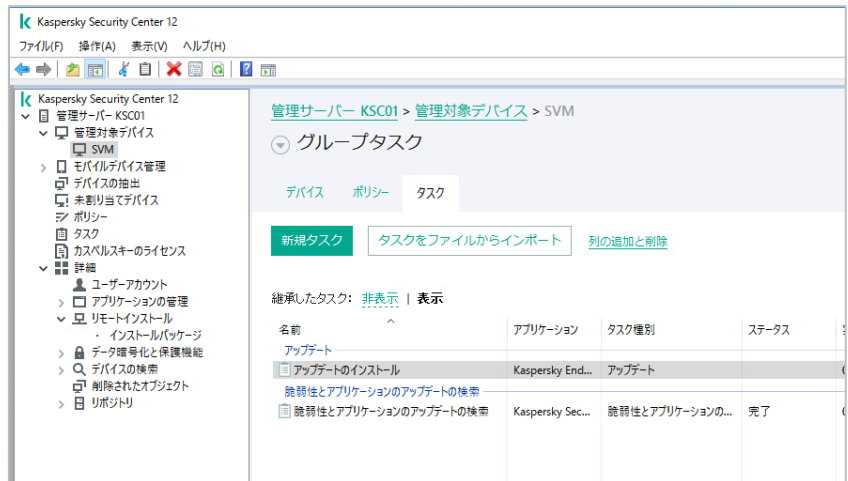
- DNS ドメイン名: la-svm-192-168-1-60
- IP アドレス: 192.168.1.70
- 保護ステータス: 実行中 (推奨レベル)
- スキャンからの保護ス... デバイスからのデータな...

## 2.2. SVM のライセンスアクティベーション

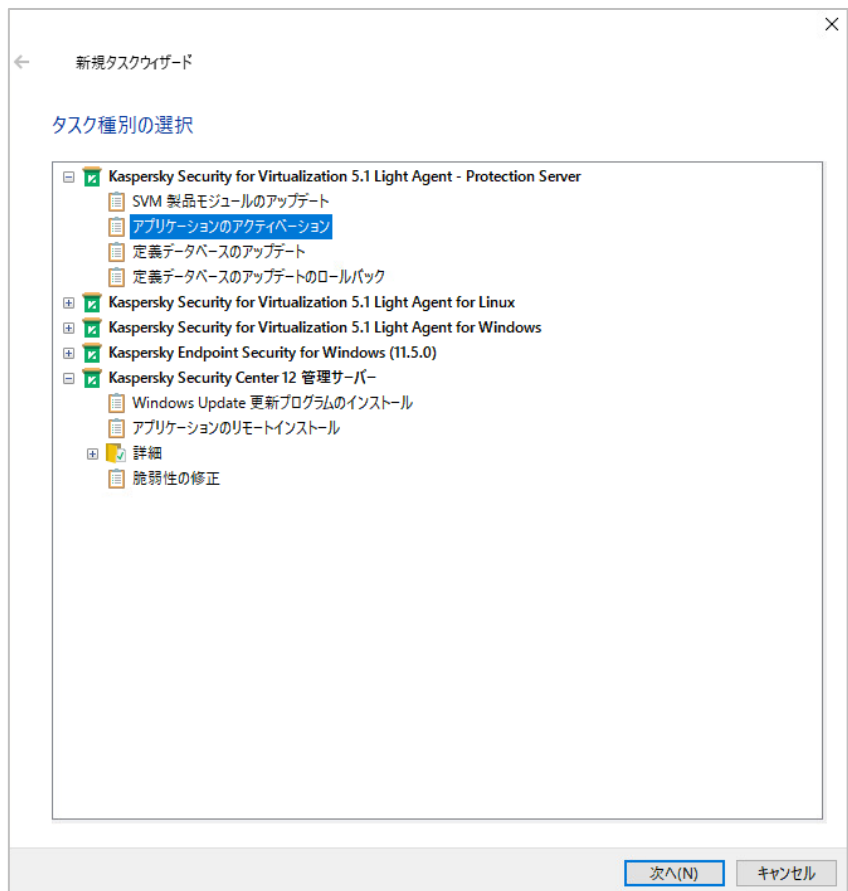
SVM に対して、ライセンスアクティベーションを行います。

各仮想マシンのライセンスは、SVM によって管理され、Light Agent がインストールされた際に自動的にアクティベーション処理が実施されます。仮想マシン（VM）に対してのライセンスアクティベーションは不要です。

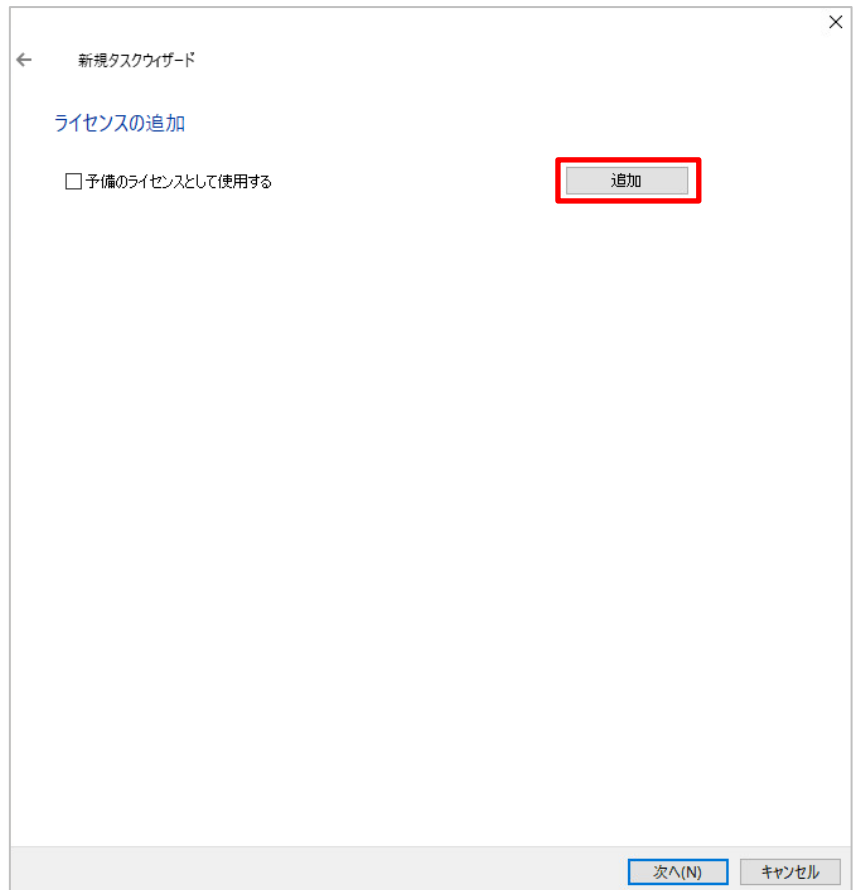
- ① KSC の管理画面を開きます。  
左メニューの「タスク」を選択し、右メニューの「タスクの作成」をクリックします。



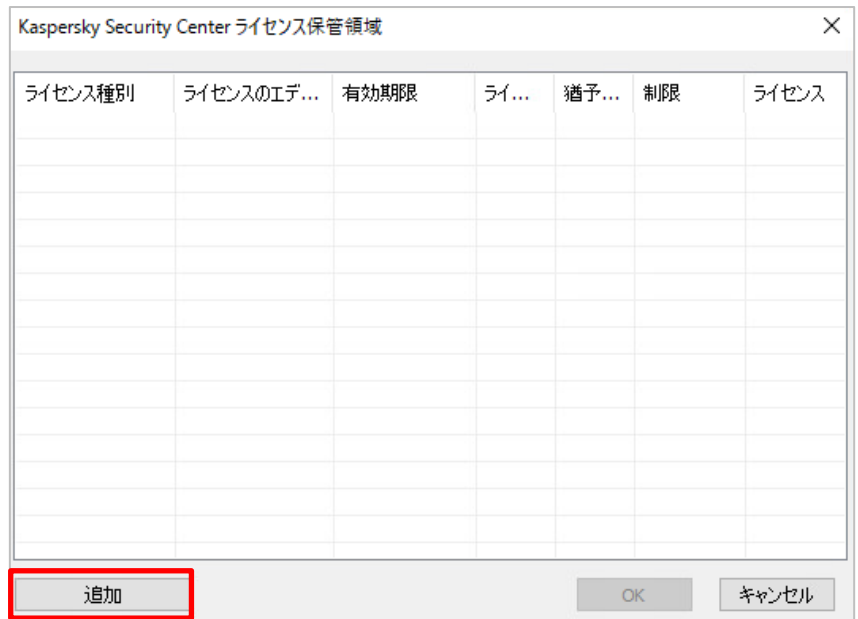
- ② Protection Server の「アプリケーションのアクティベーション」を選択し、「次へ」をクリックします。



② 新規タスクウィザードで「追加」をクリックします。



④ 「追加」をクリックします。



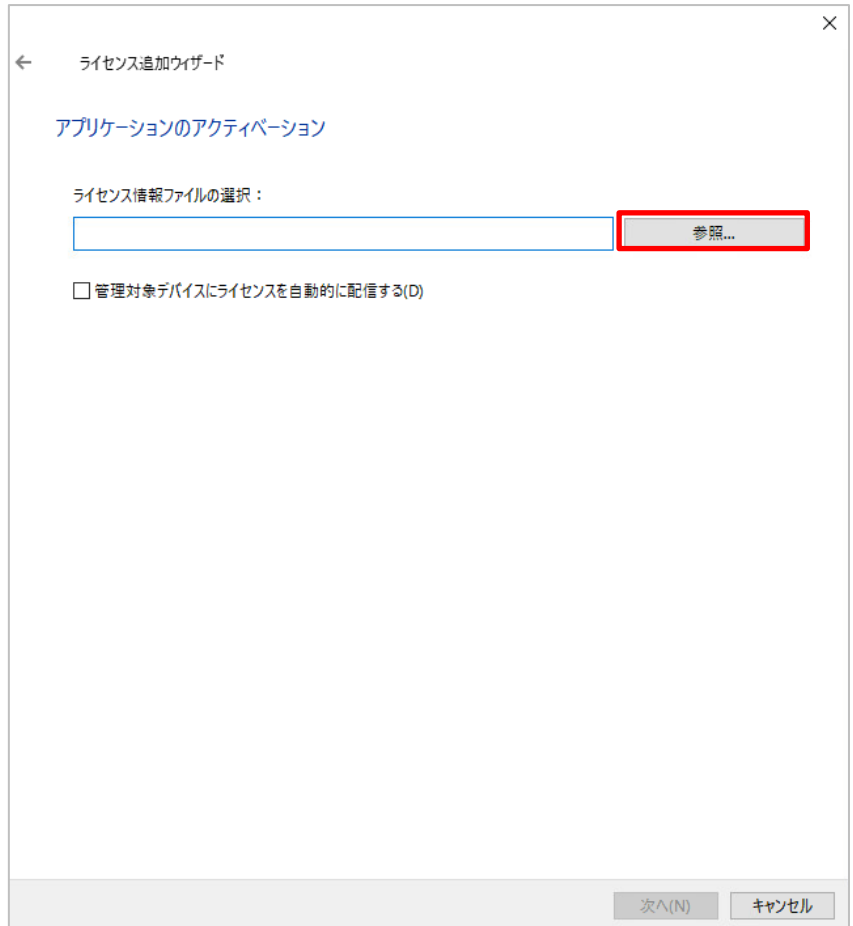


⑤ライセンス情報ファイルを入力するかアクティベーションコードを選択します。

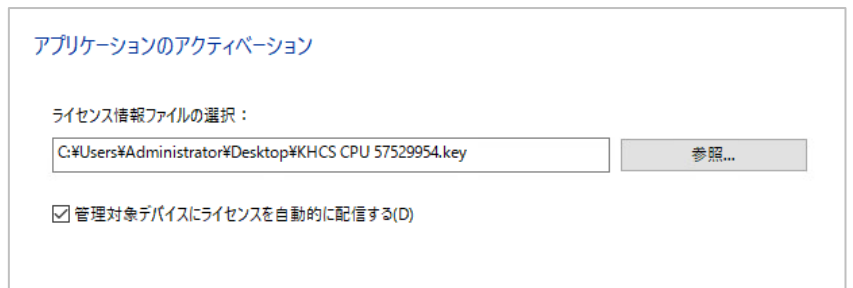
今回はライセンス情報ファイルを指定します。



⑥ 参照をクリックします。

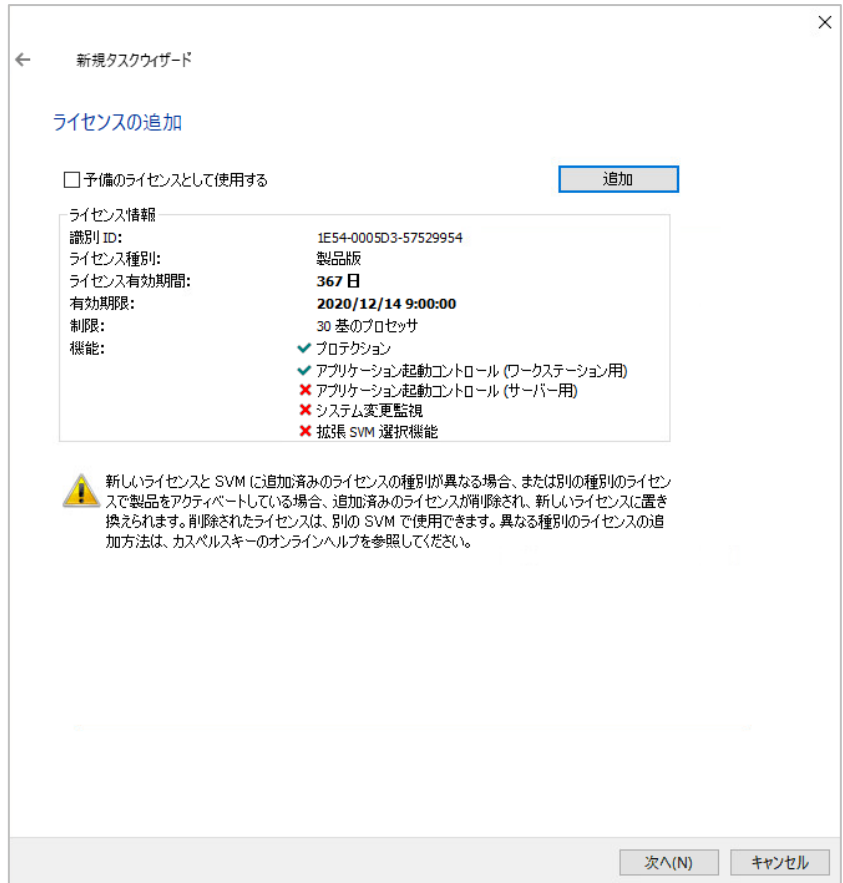


⑦ 納品されているライセンスファイルを KSC にコピーし、指定します。

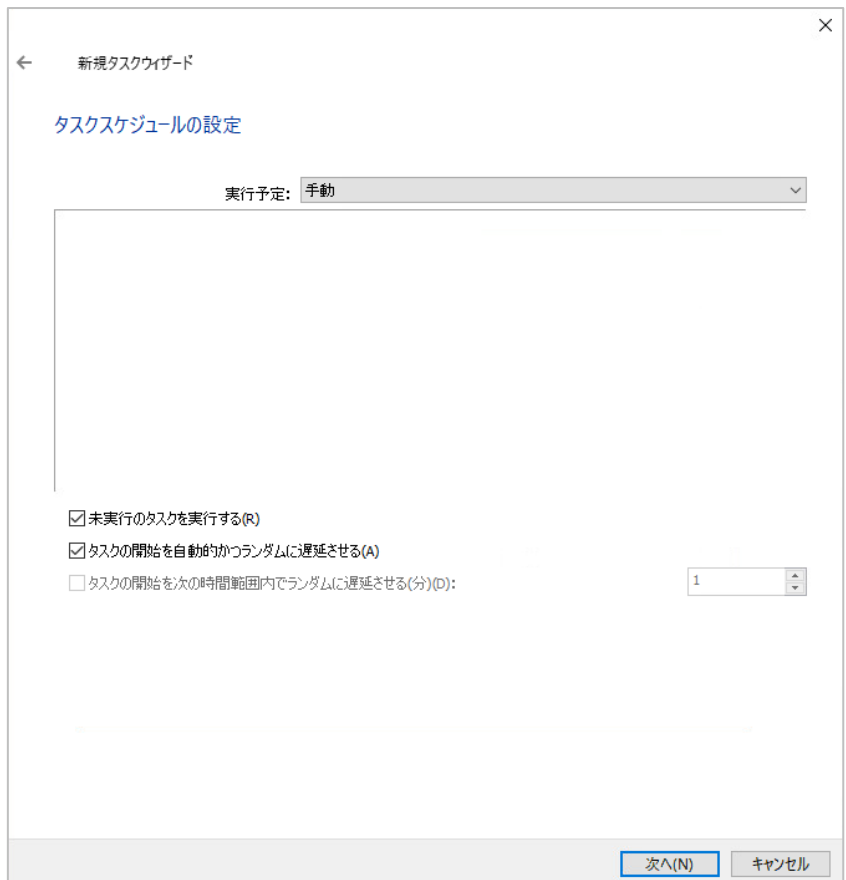




- ⑩ ライセンスが追加されたことを確認し、「次へ」をクリックします。



- ⑪ 実行予定を「手動」にし、「次へ」をクリックします。



- ⑫ 任意の「タスク名」を入力し、「次へ」をクリックします。

← 新規タスクウィザード

タスク名の定義

名前:

アプリケーションのアクティベーション

次へ(N) キャンセル

- ⑬ 「ウィザード完了後にタスクを実行する」を選択し、「完了」をクリックします。

← 新規タスクウィザード

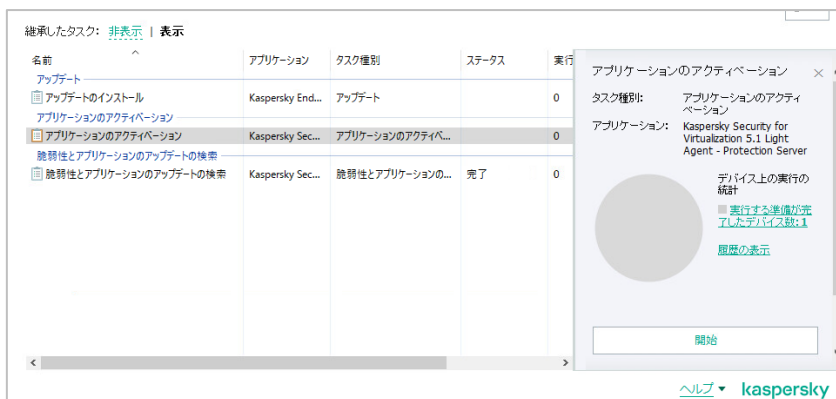
タスク作成の終了

【終了】をクリックし、「アプリケーションのアクティベーション」の作成処理を完了し、ウィザードを閉じます。

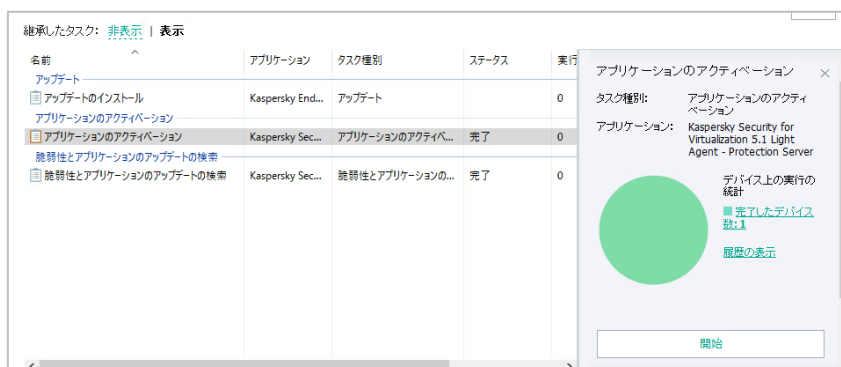
ウィザードの終了後にタスクを実行(R)

完了(F) キャンセル

⑭ タスクを選択し、開始をクリックします。



⑮ 「アプリケーションのアクティベーション」タスクが正常に完了したことを確認します。

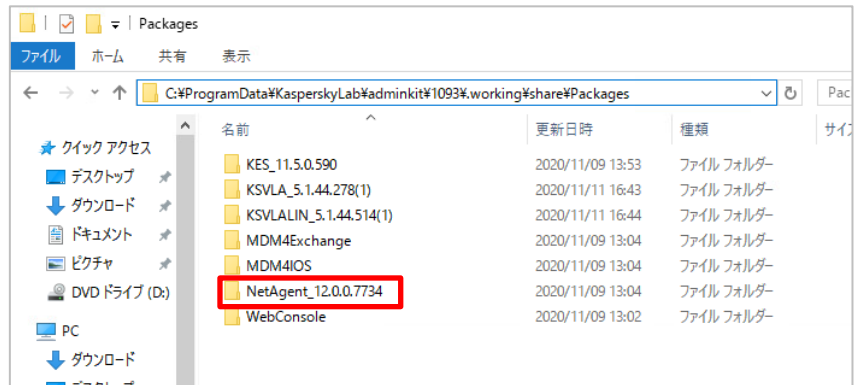


## 3. Light Agent for Windows のインストール

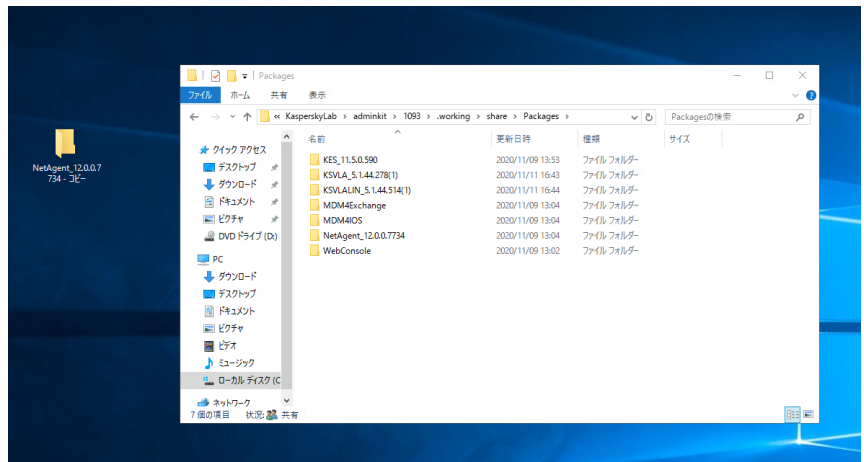
### 3.1. VDI 用ネットワークエージェントの準備

非永続型 VDI で使用するためのネットワークエージェントを準備します。

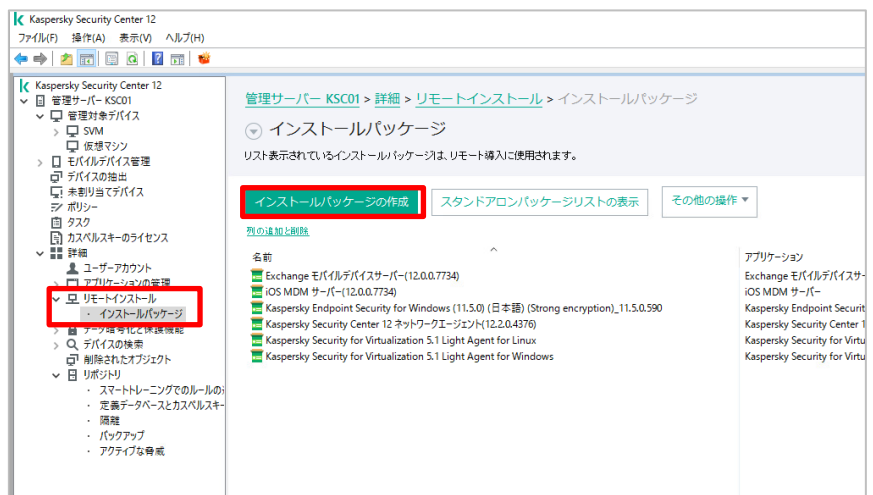
- ① C:\ProgramData\KasperskyLab\admindit\1093\working\share\Packages を開きます。



- ② ネットワークエージェントをデスクトップなどにコピーします。  
パッケージ作成が完了したら、このコピーは削除できます。



- ③ インストールパッケージの作成をクリックします。



- ④ カスペルスキー製品のインストールパッケージを作成するをクリックします。

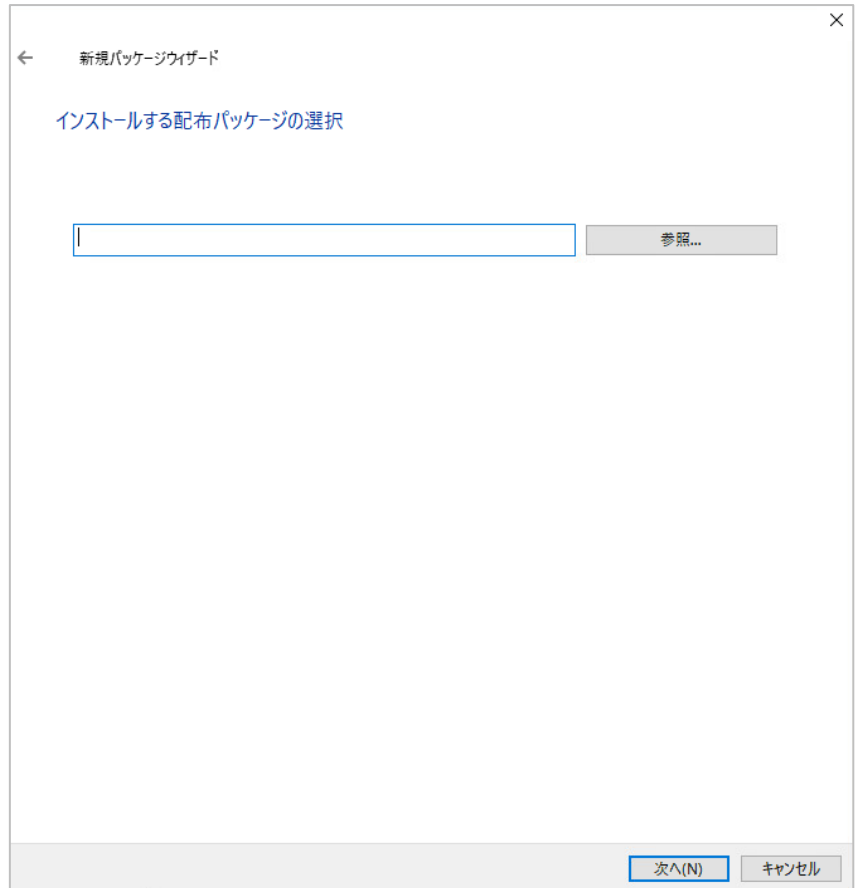


- ⑤ 判別しやすい名称を付け、「次へ」をクリックします。

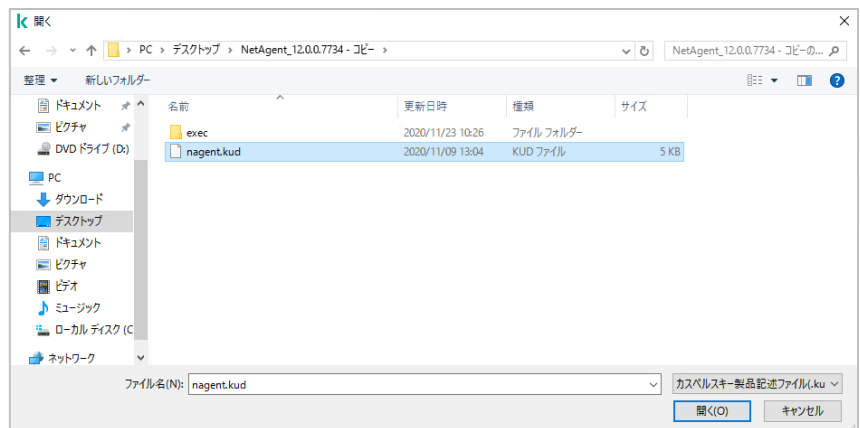




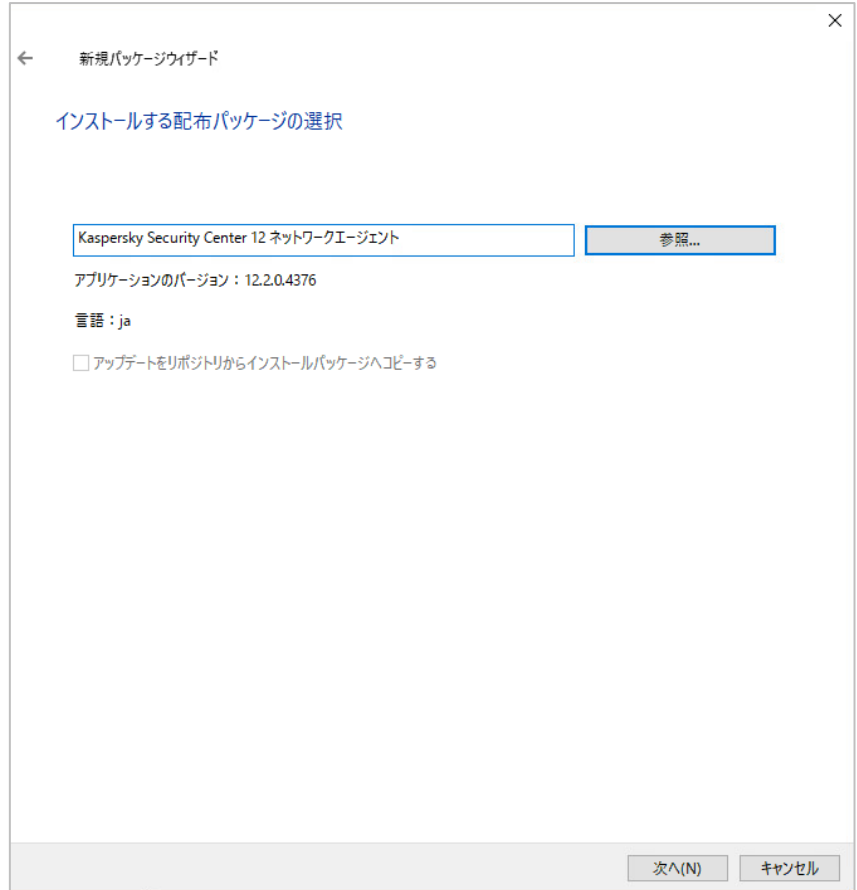
⑥ 「参照」をクリックします。



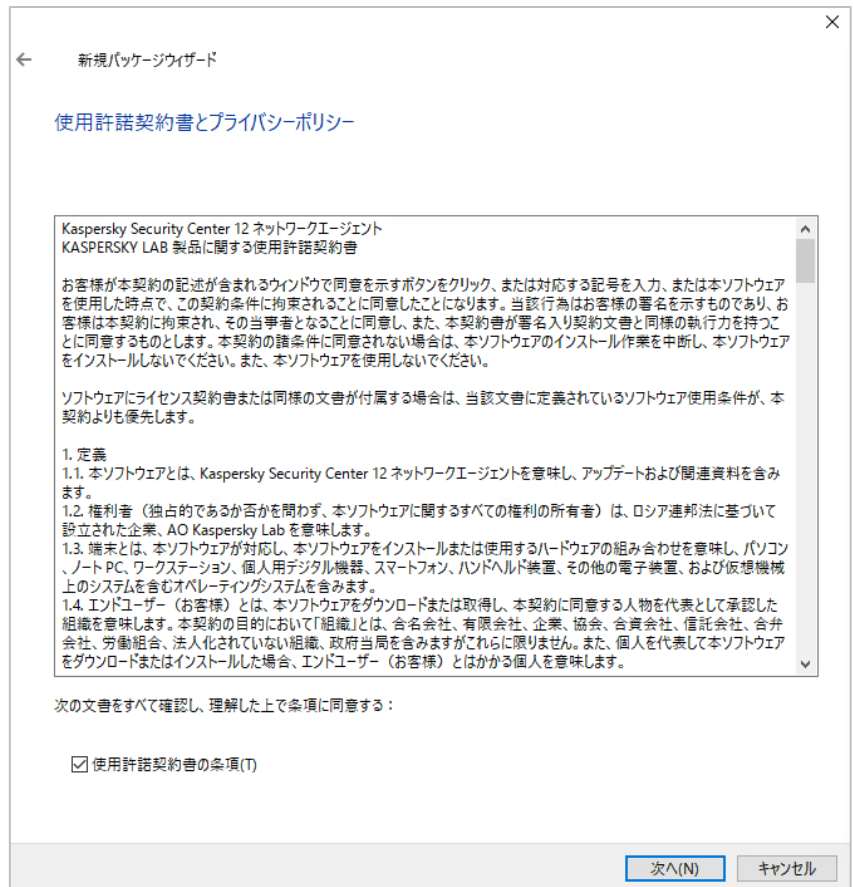
⑦ 先ほどコピーしたデスクトップのフォルダーを開き、拡張子 kud のファイルを指定します。



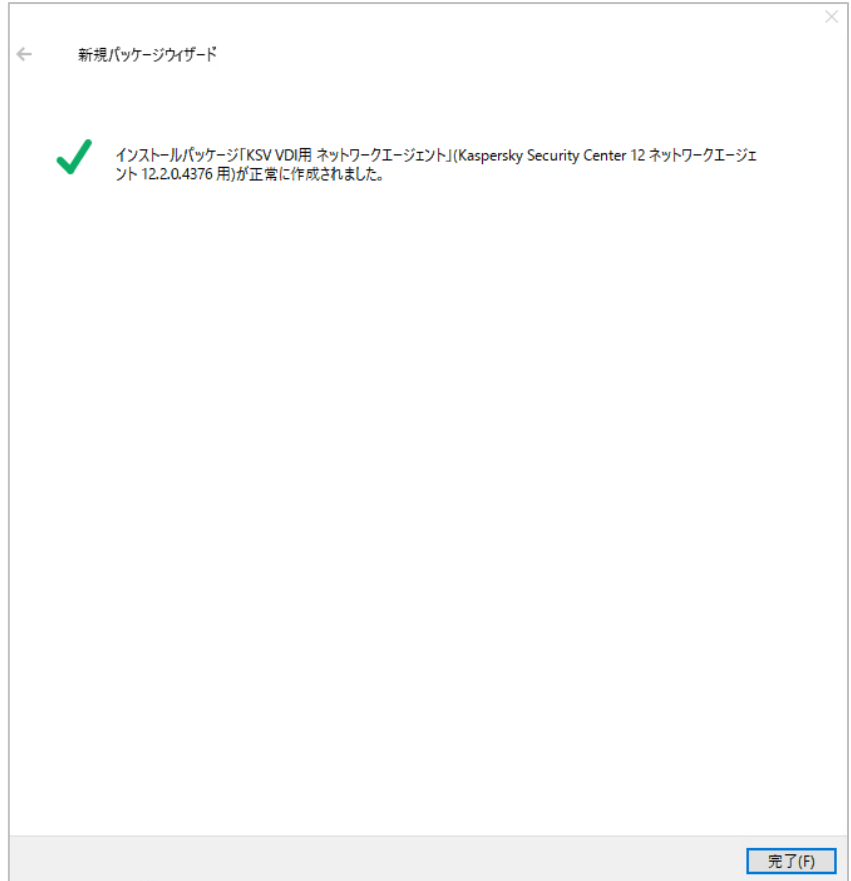
⑧ 「次へ」をクリックします。



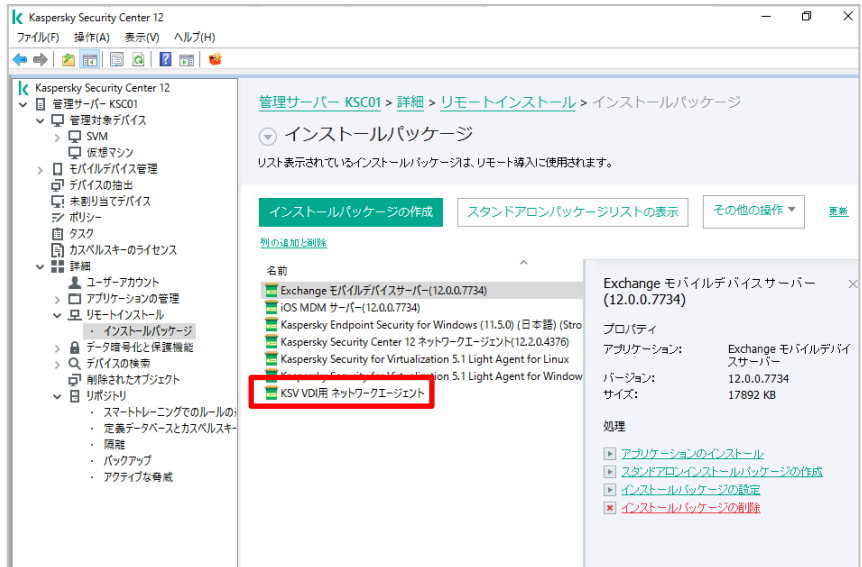
⑨ 使用許諾とプライバシーポリシーに同意します。



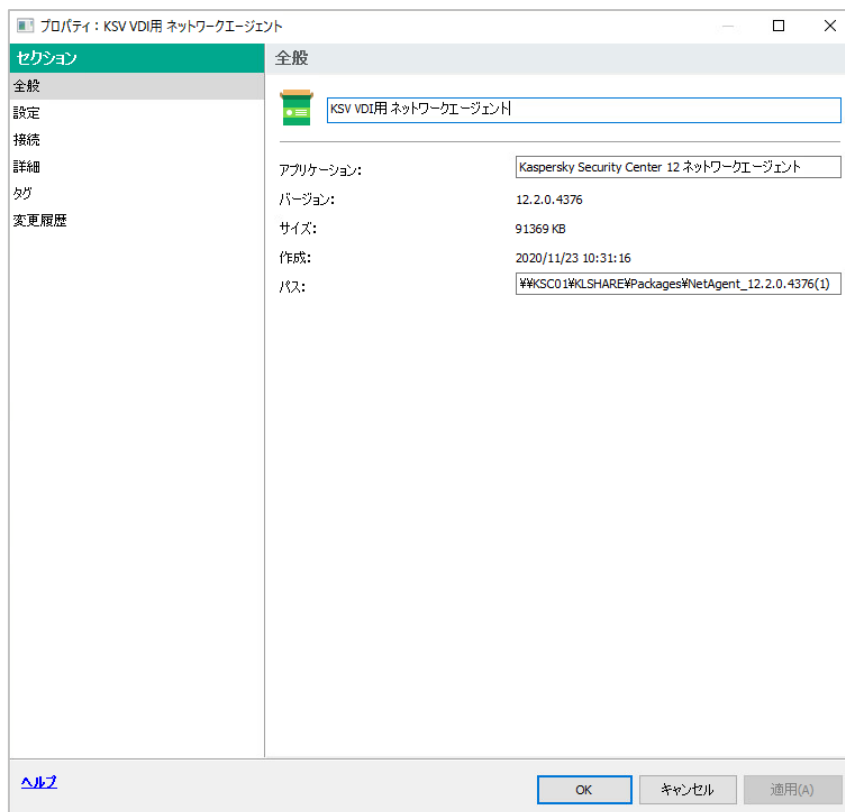
⑩ 「完了」をクリックします。



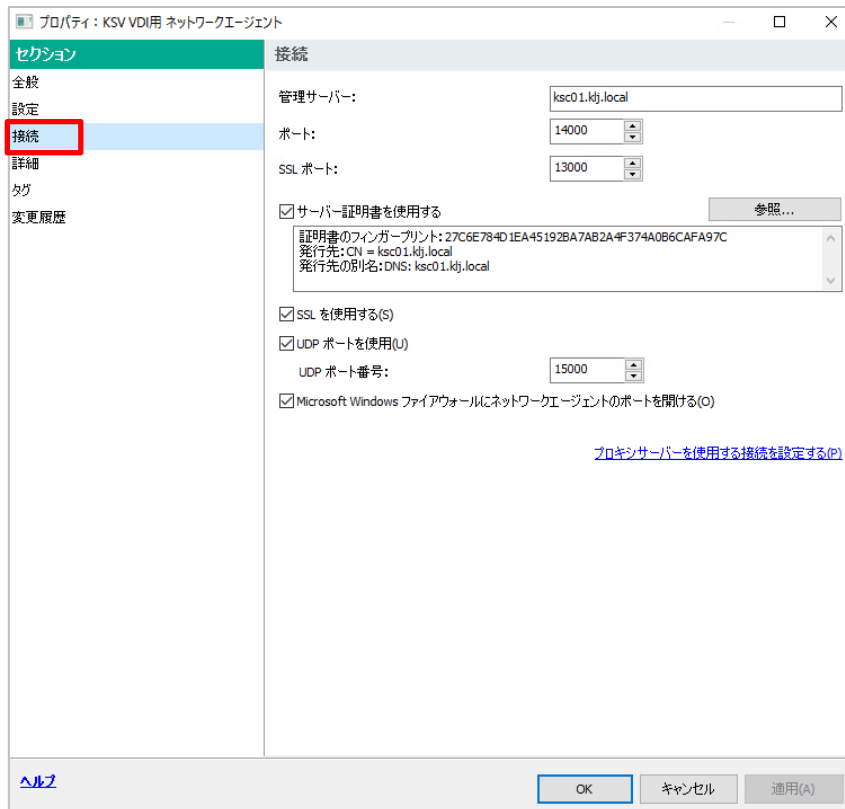
⑪ パッケージが作成されたことを確認し、ダブルクリックします。



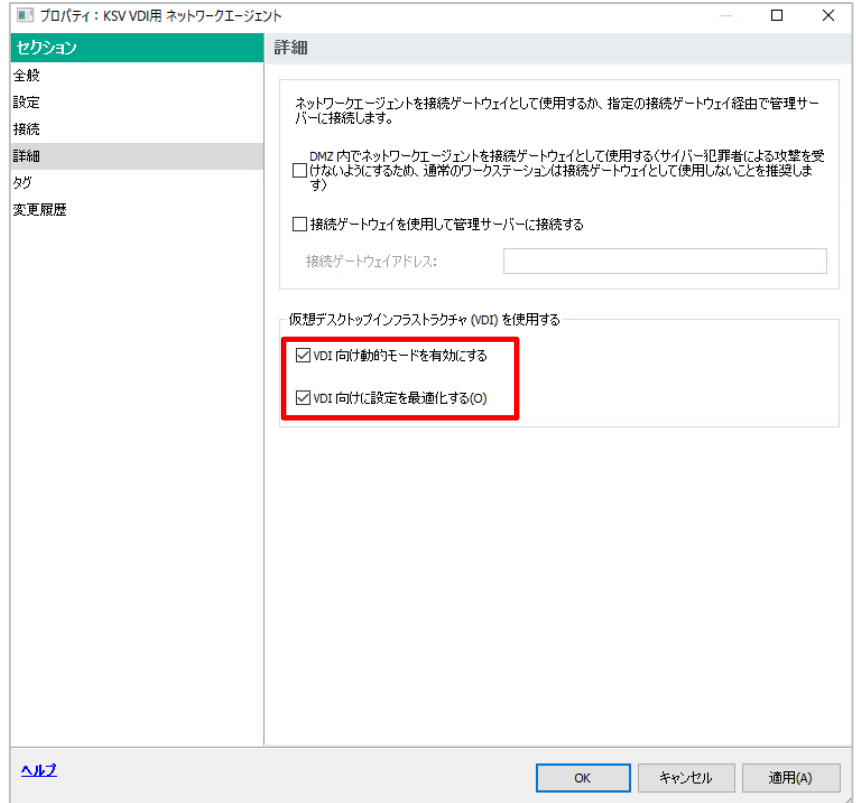
⑫ プロパティが開きます。



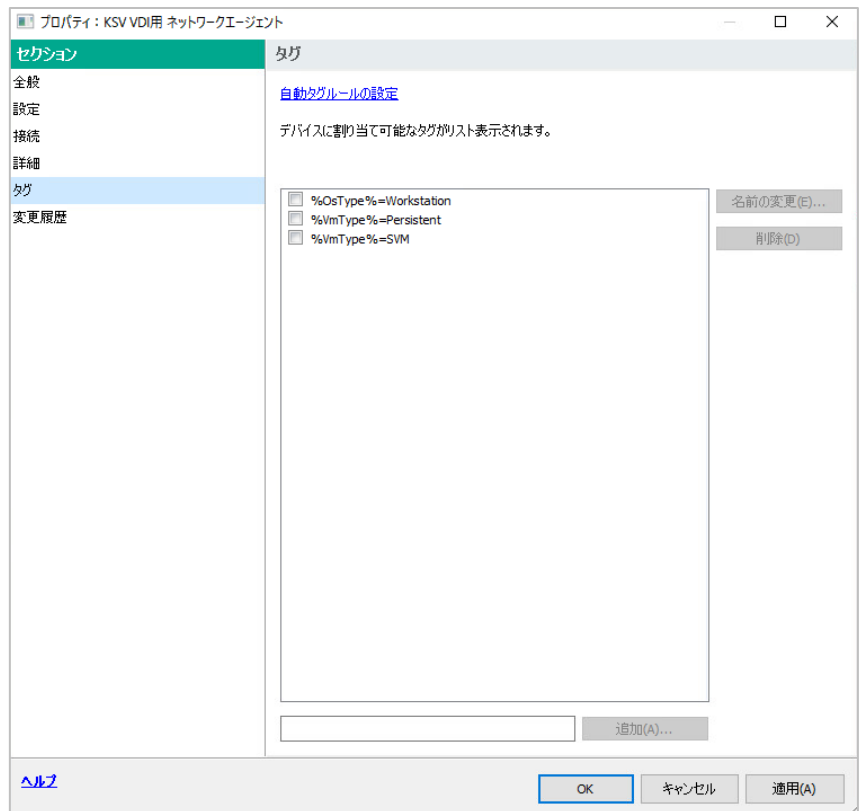
⑬ 接続セクションから、管理サーバーのアドレスが正しいことを確認します。



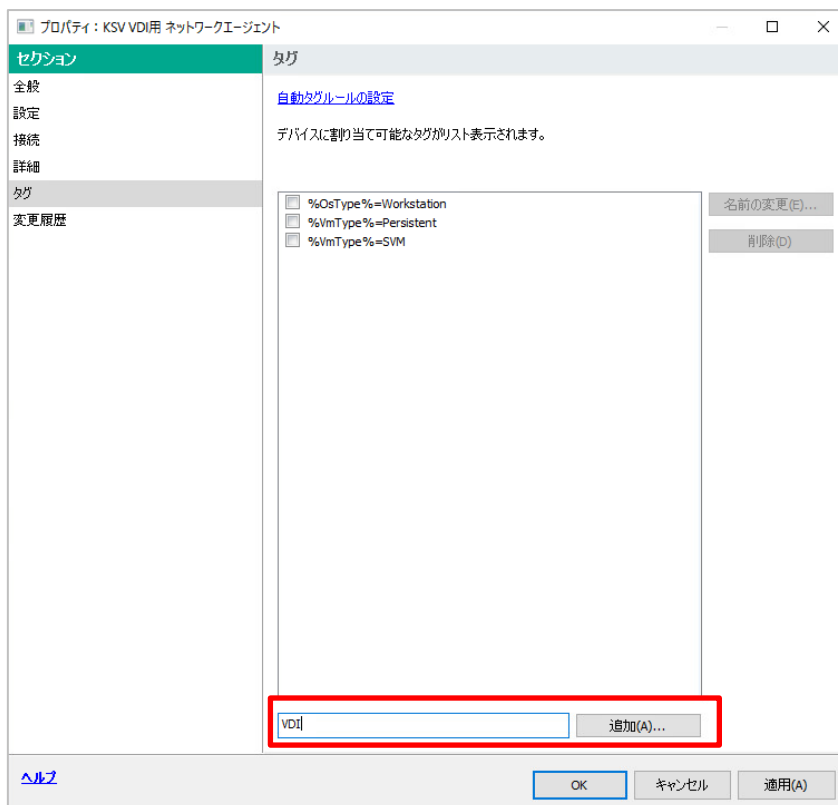
- ⑭ 「詳細」セクションから、「VDI 向けに動的モードを有効にする」、「VDI 向けに設定を最適化する」にチェックを入れます。



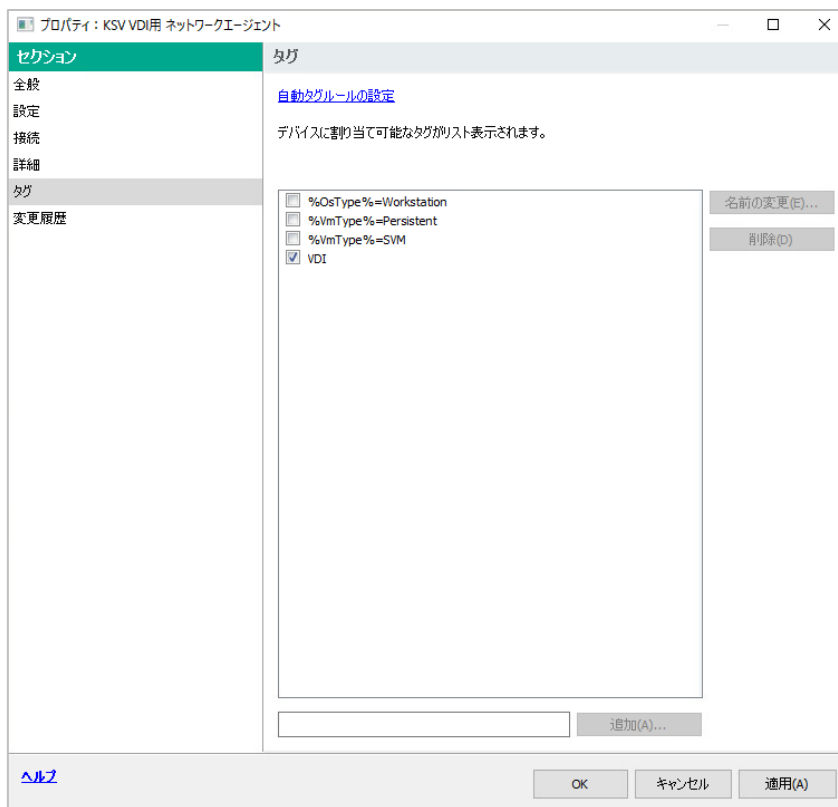
- ⑮ タグセクションを開きます。



- ⑩ VDIと入力し、追加をクリックします。

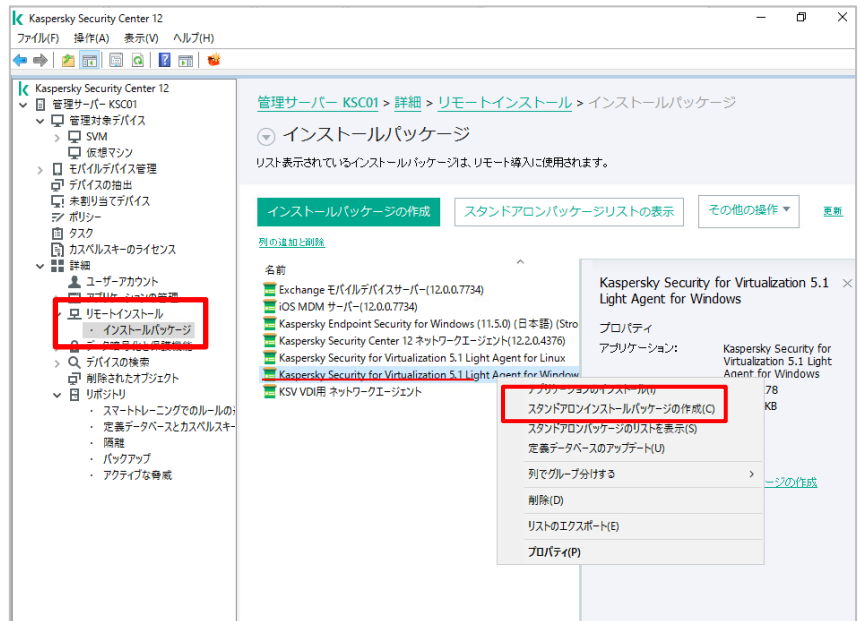


- ⑪ VDI タグにチェックが付いていることを確認し、「OK」をクリックします。



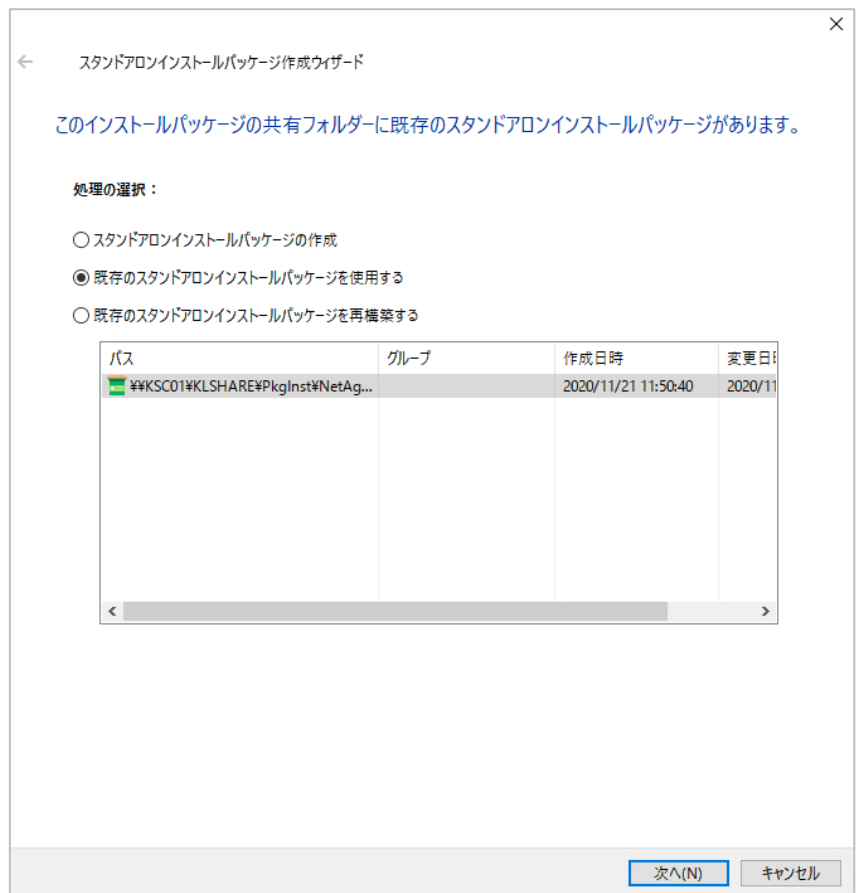
## 3.2. マスター仮想マシンへのインストール（ローカルインストール方式）

- ① Light Agent for Windows のインストールパッケージを右クリックし、「スタンドアロンインストールパッケージの作成」をクリックします。

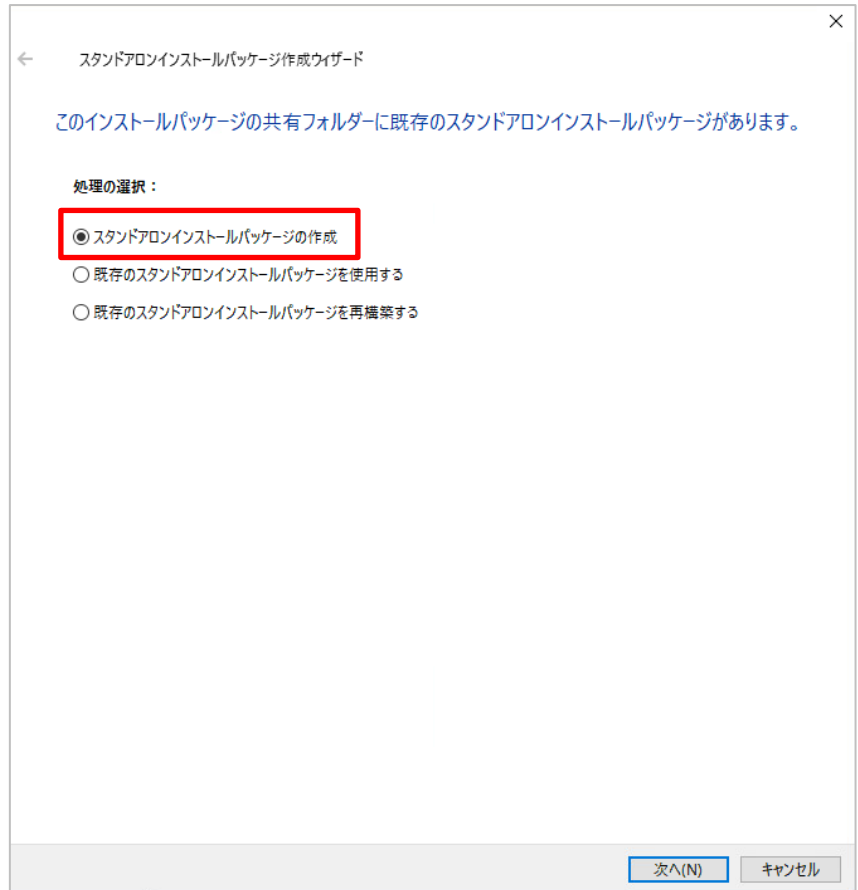


- ② 既にスタンドアロンインストールパッケージが存在する場合は、右のような画面になります。

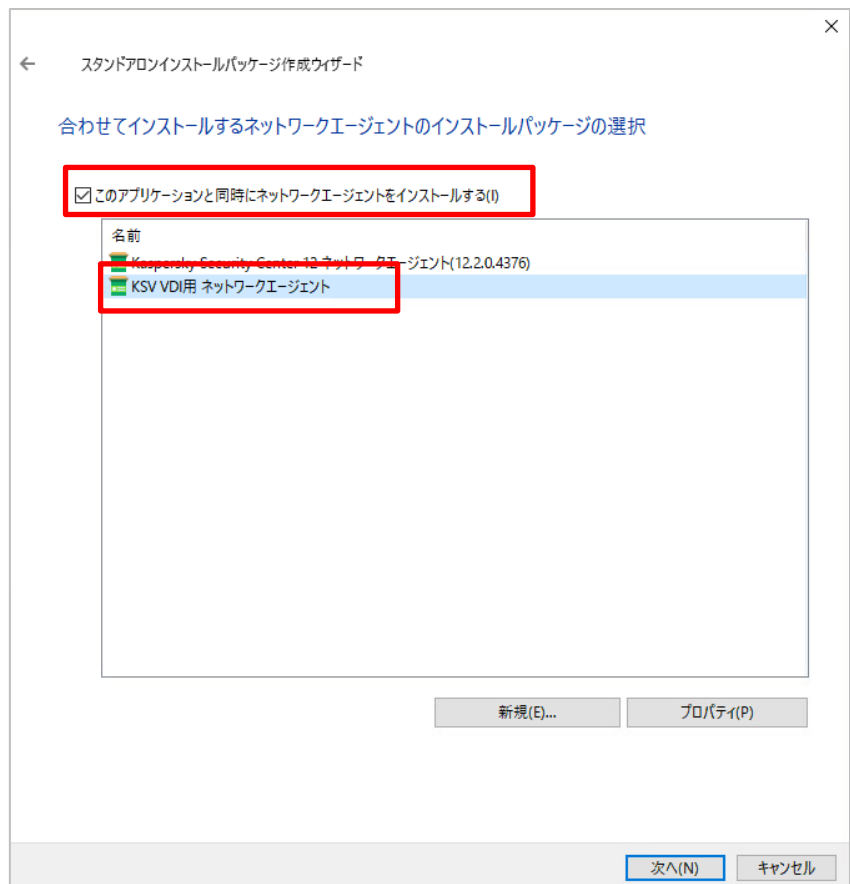
このメッセージが出ない場合は、4 の画面が出ます。



- ③ このメッセージが出る場合は一番上の、「スタンドアロンインストールパッケージの作成」に変更してください。

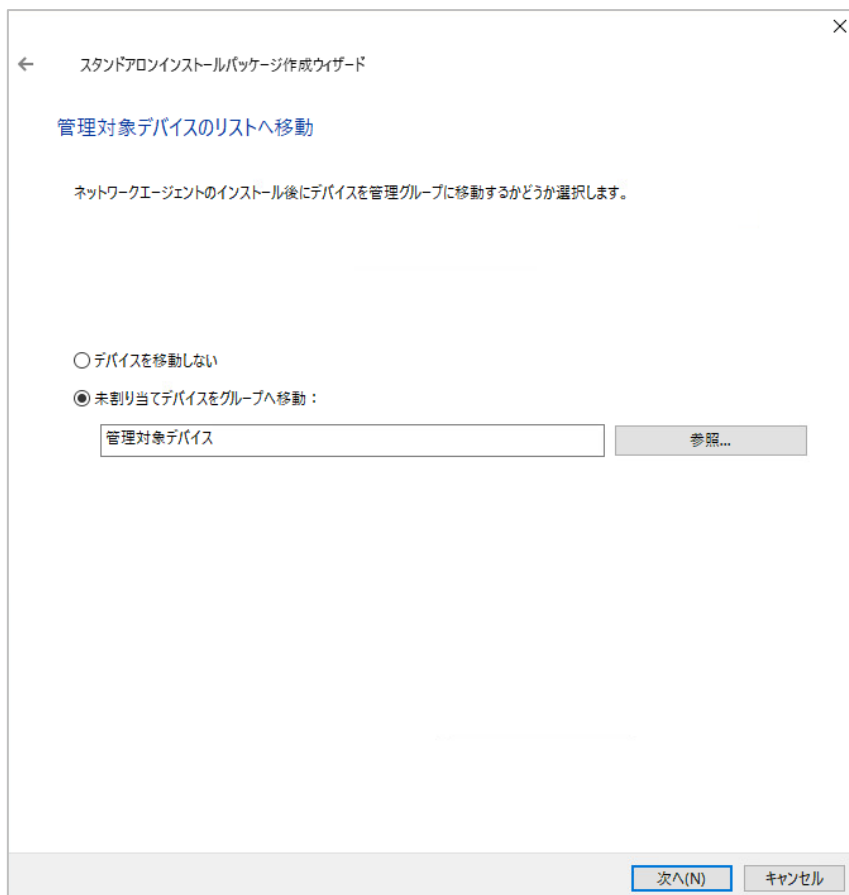


- ④ 先に作成した VDI 用ネットワークエージェントを選択し、「次へ」をクリックします。

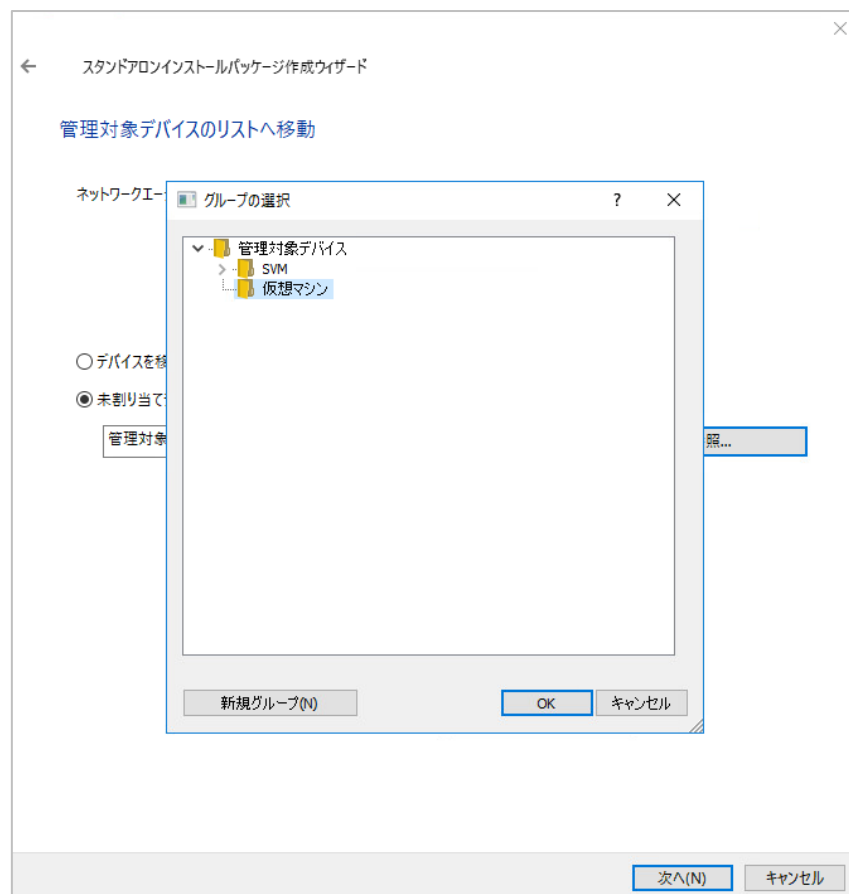




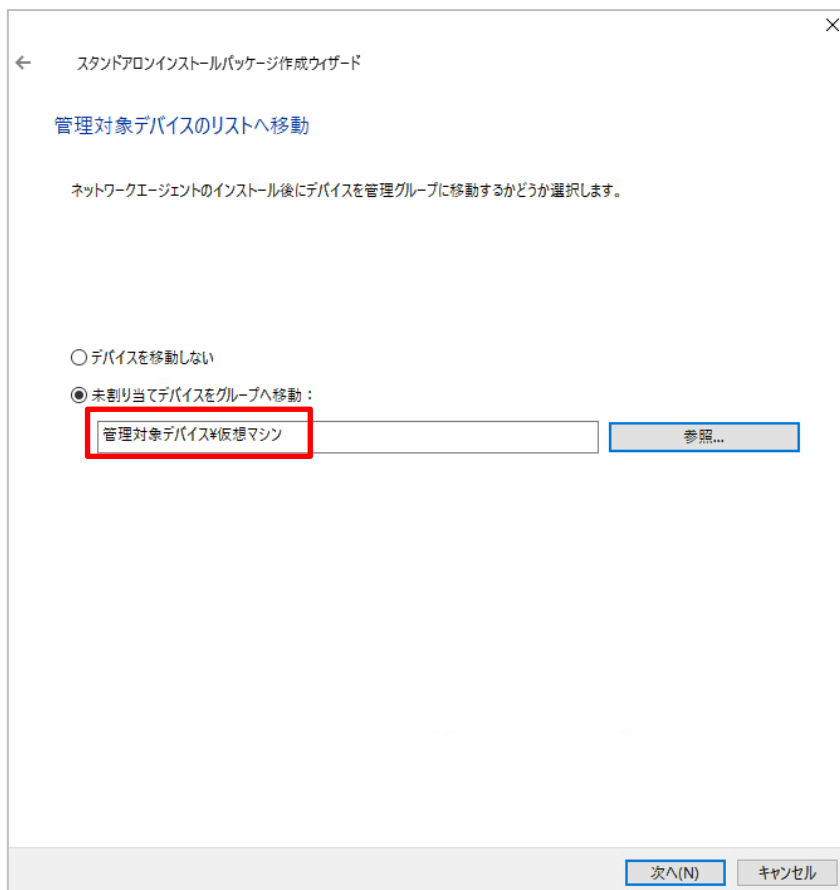
⑤ 参照をクリックし、クライアントにネットワークエージェントをインストールした際、自動的にどのグループに所属させるかを選択します。



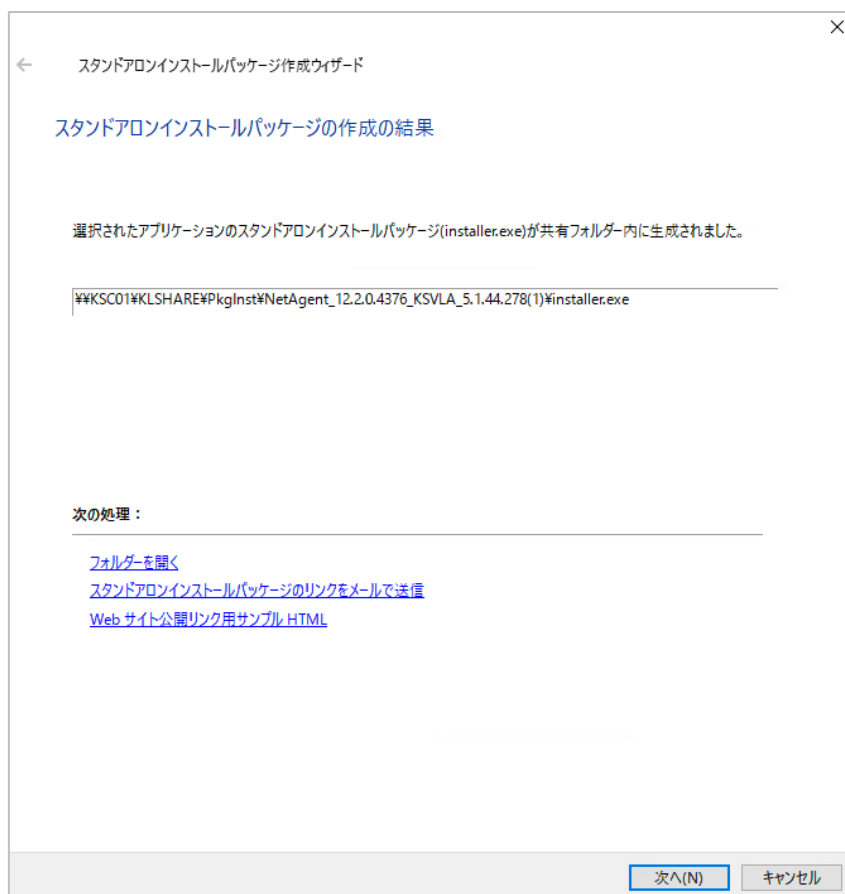
⑥ 仮想マシングループ選択後、「OK」をクリックします。



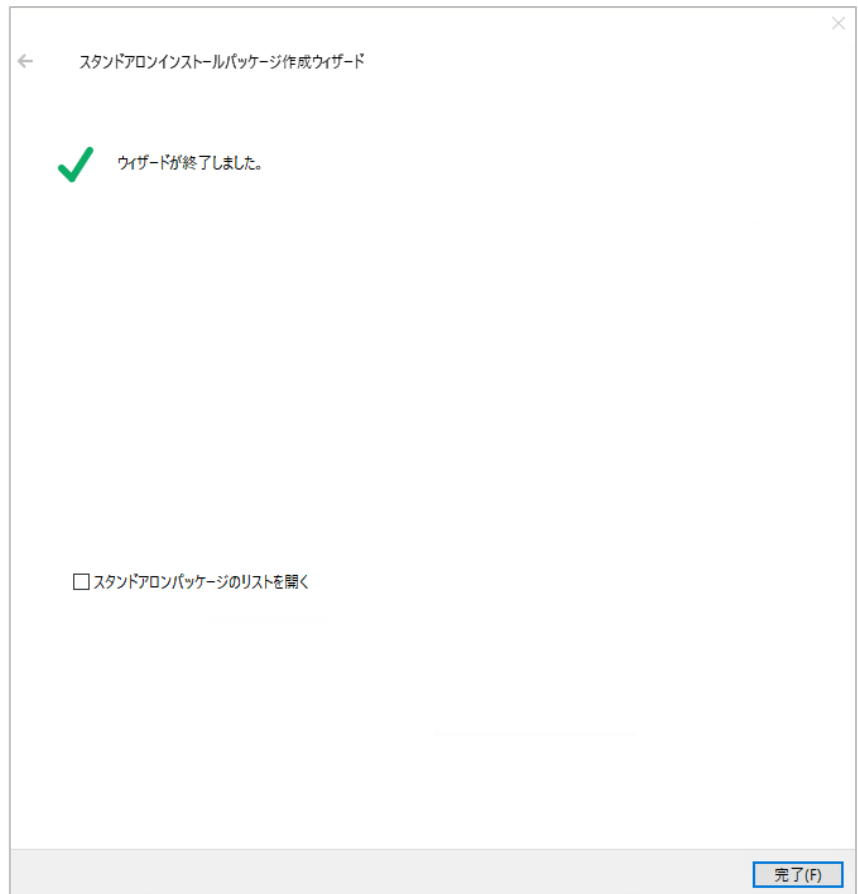
- ⑦ 「次へ」をクリックすると、  
パッケージの作成が始まります。



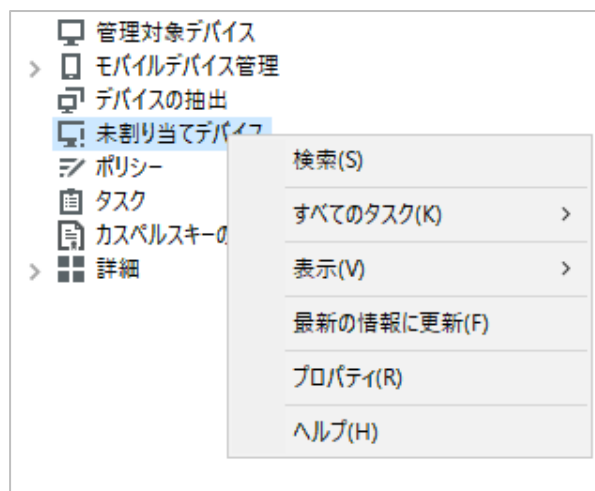
- ⑧ マスター仮想マシンから、このフォルダーにアクセスし、インストールを行います。



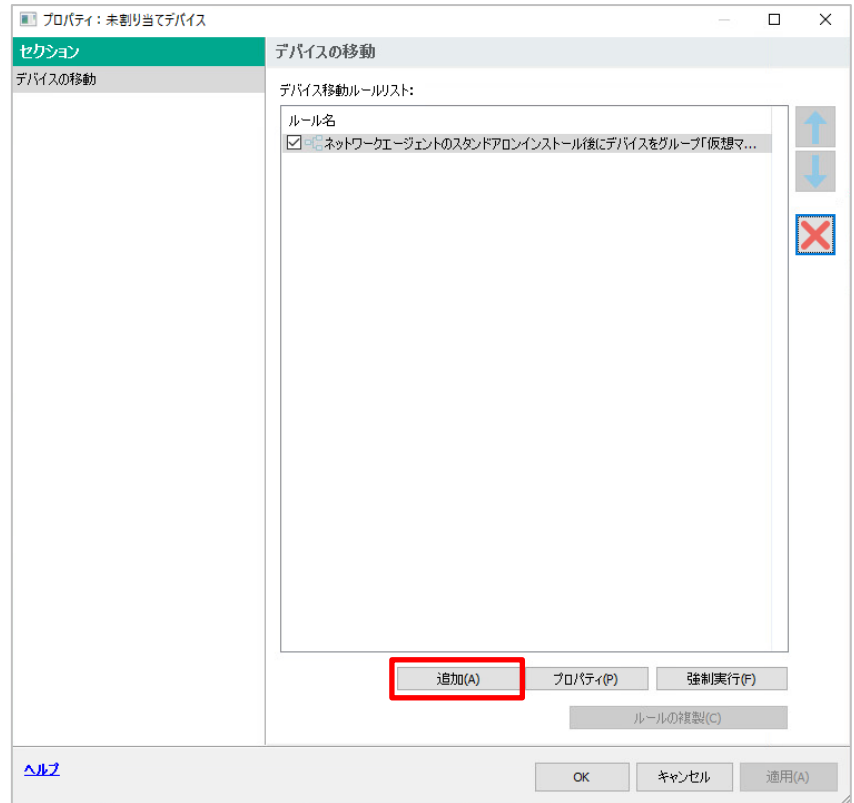
- ⑨ 「完了」をクリックしてウィザードを終了します。



- ⑩ 未割り当てデバイスを右クリックし、プロパティを開きます。

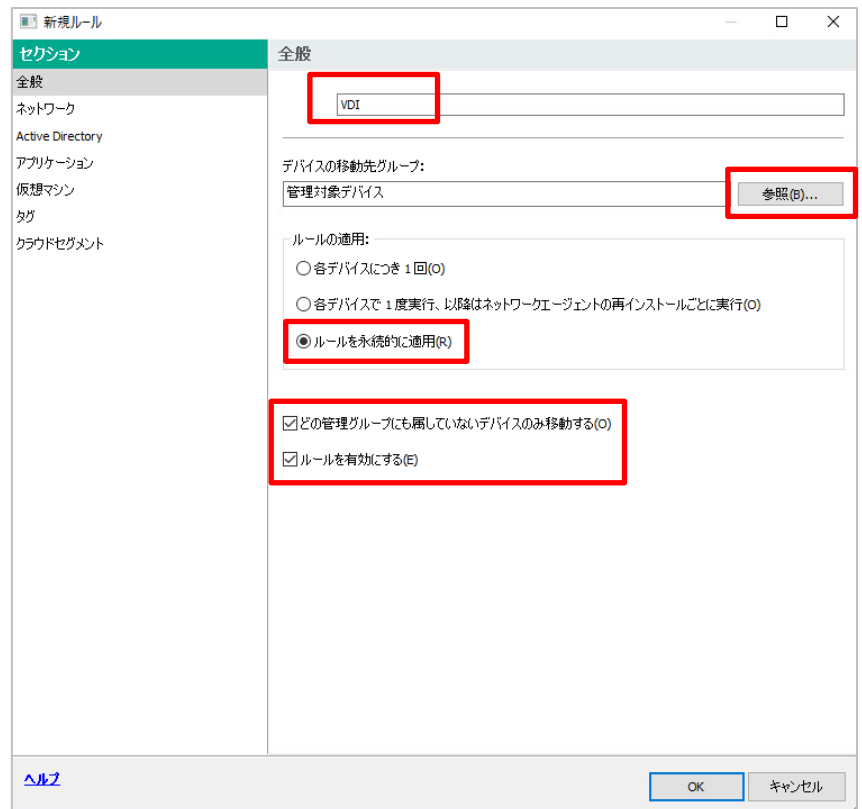


- ⑪ 先ほどインストールパッケージを仮想マシングループに紐づけたので、ルールが存在します。さらに移動ルールを追加します。

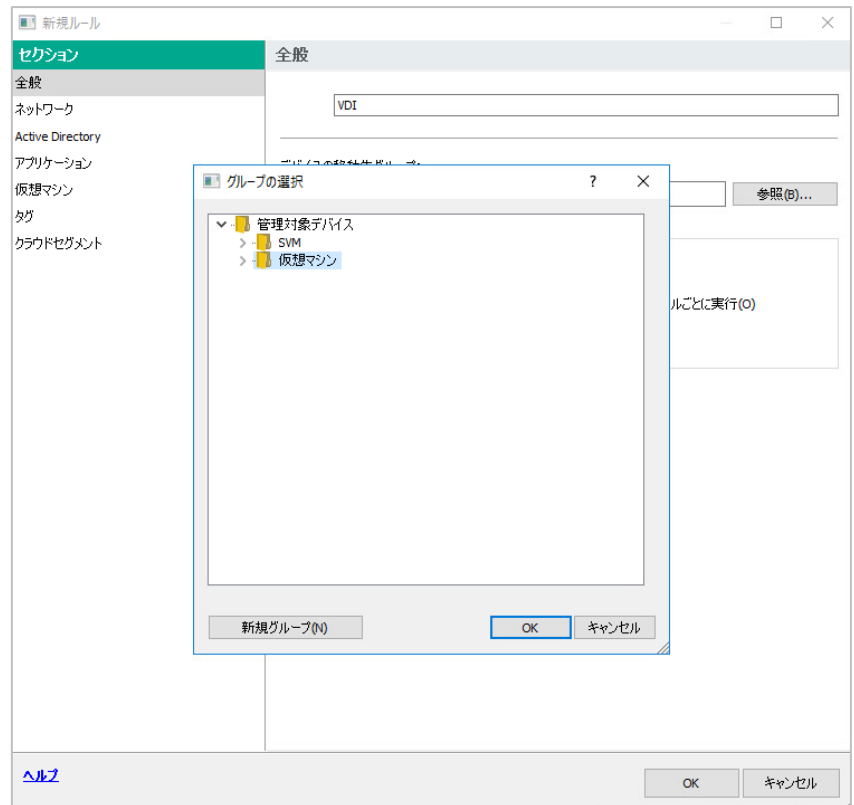


- ⑫ 名称を VDI などと付けます。「ルールを永続的に適用」に変更し、「ルールを有効にする」にチェックを入れます。

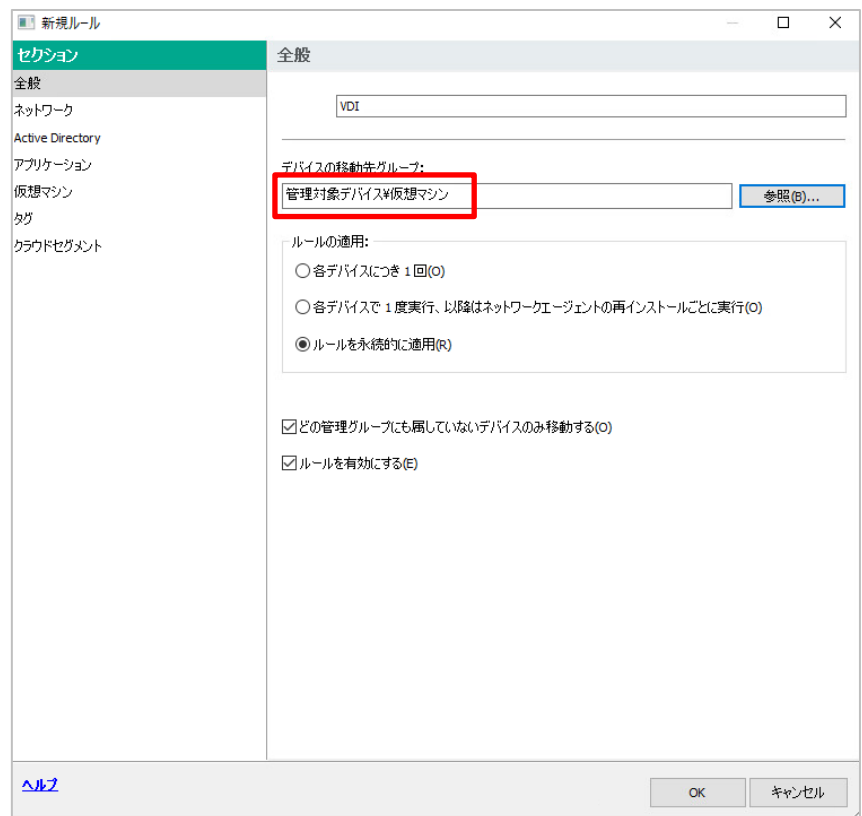
「参照」をクリックします。



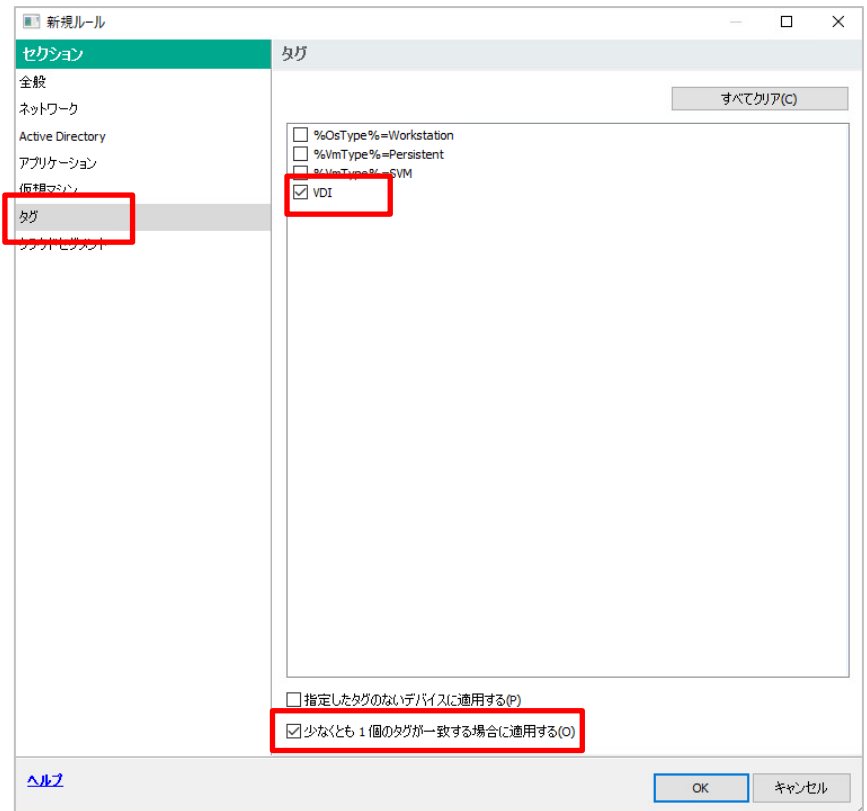
⑬ 仮想マシングループを指定します。



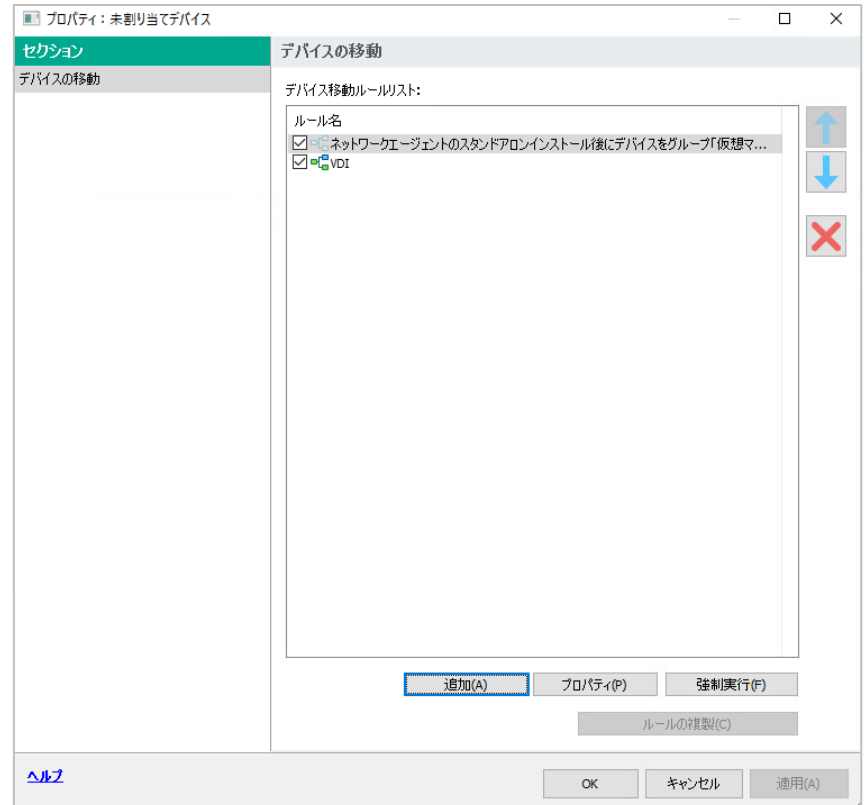
⑭



- ⑮ タグをクリックし、“VDI”タグにチェックを入れます。  
「少なくとも 1 個のタグが一致する場合に使用する」にチェックを入れます。



- ⑯ 「OK」をクリックします。

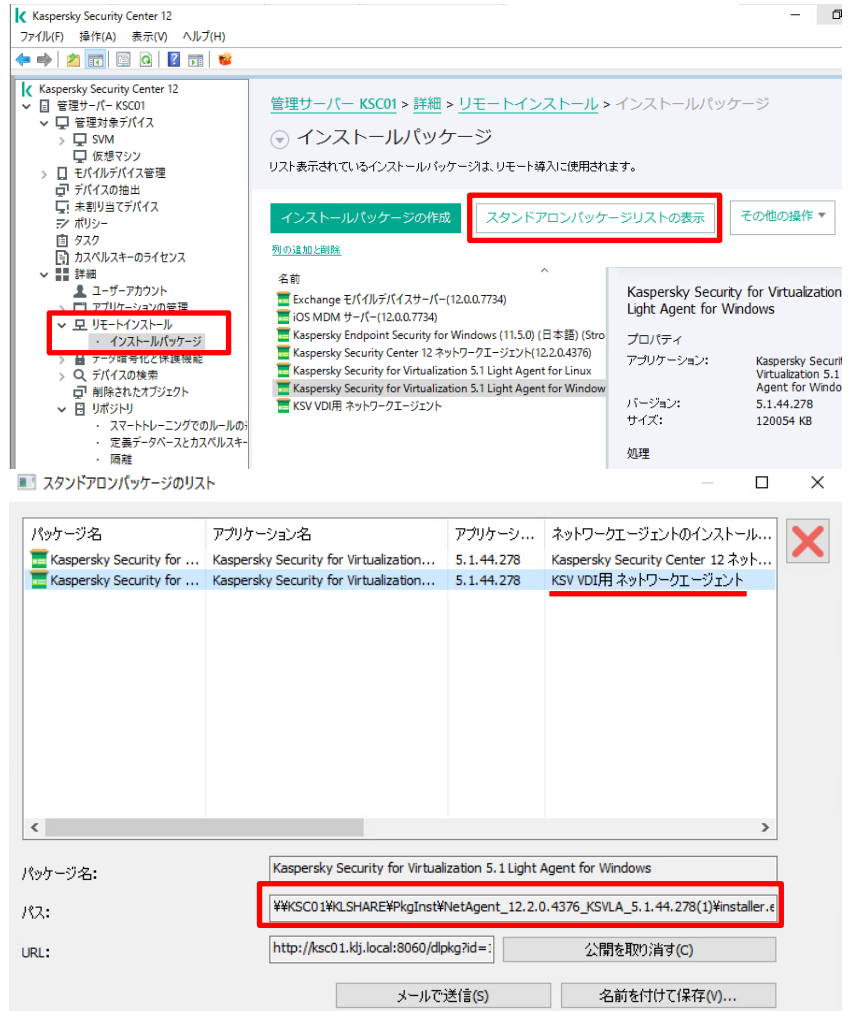


※ **以下は仮想マシン（ゲスト OS）側での操作です。**

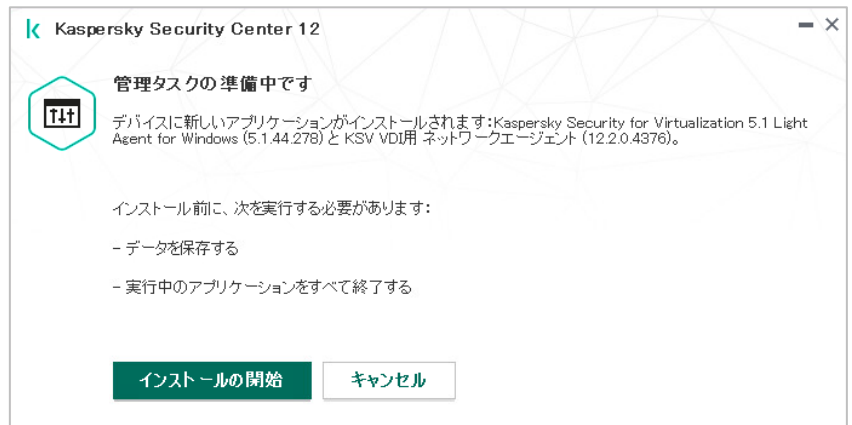
各クライアント（仮想マシン）から管理サーバーの共有フォルダーにアクセスできる場合、共有フォルダーに保存されているパッケージを直接実行してネットワークエージェントをインストールすることができます。

① 3-2⑦のパスにクライアントクライアントからアクセスします。

分からない場合は、「スタンドアロンパッケージリストの表示」で確認できます。



② カスペルスキー製品のインストール画面が表示されます。「インストールの開始」をクリックします



- ③ インストールが完了したら、「閉じる」をクリックします





## 4. マスター仮想マシンのクローン

### 4.1. 仮想マシンのクローン

お客様環境に応じて、vCenter Server のクローン機能や仮想デスクトップアプリケーション機能などを利用して、マスター仮想マシンのクローン（展開）を行ってください。

クローン時は vCenter Server の仮想マシンのカスタマイズ機能や Sysprep 機能を利用して、OS の SID が、マスター仮想マシンと重複しないようにしてください。（VMware Horizon の Quickprep 可）

- ① 作成した仮想マシンを起動し、KSC から正常に認識されたことを確認します。

右図のように適切なホスト名が記載されており、緑色の OK ステータスになっていれば、問題ありません。

【OK 例】 ホスト名が正しく表示されており、「OK」ステータスになっている。

The screenshot shows the Kaspersky Security Center 12 interface. The left sidebar contains a navigation tree with '管理対象デバイス' (Managed Devices) expanded. The main window displays '管理対象デバイス' (Managed Devices) for '管理サーバー: KSC01 > 管理対象デバイス > 仮想マシン'. Below this, there are buttons for 'デバイス', 'ポリシー', and 'タスク'. A table lists the managed devices with columns for '名前' (Name), '前回の管理サーバ' (Last Management Server), 'ネットワーク接続' (Network Connection), 'リアルタイム保護のステータス' (Real-time Protection Status), '作成日' (Creation Date), 'OS のビルド' (OS Build), and 'OS のリリース ID' (OS Release ID). The table shows four entries: MASTER, HR-PC-1, HR-PC-2, and HR-PC-3, all with a status of 'OK'.

名前	前回の管理サーバ	ネットワーク接続	リアルタイム保護のステータス	作成日	OS のビルド	OS のリリース ID
MASTER	15 分前	はい	OK	4 日前	19041	2004
HR-PC-1	3 分前	はい	OK	8 分前	19041	2004
HR-PC-2	2 分前	はい	OK	7 分前	19041	2004
HR-PC-3	1 分前	はい	OK	3 分前	19041	2004

## 株式会社カスペルスキー

〒101-0021 東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F

カスペルスキー公式ホームページ [www.kaspersky.co.jp](http://www.kaspersky.co.jp)

法人のお客様向けダウンロード資料 <https://kasperskylabs.jp/biz/>

©2020 Kaspersky Labs Japan. Kaspersky Anti-Virus および Kaspersky Security は、Kaspersky Lab の登録商標です。

その他記載された会社名または製品名などは、各社の登録商標または商標です。なお、本文中では、TM、®マークは明記していません。

記載内容は 2020 年 11 月現在のものです。記載された内容は、改良の為に予告なく変更されることがあります。