kaspersky

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

Microsoft
Hyper-V 編

2020/12/11

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

kaspersky

目次

1. はじめに

1.1. 本資料の目的

本資料では、Kaspersky Security for Virtualization 5.x Light Agent を利用し、Microsoft Hyper-V 環境上のゲスト OS の保護を行う手順を紹介しています。

1.2. 製品概要

Kaspersky Security for Virtualization 5.x Light Agent

Kaspersky Security for Virtualization 5.x Light Agent (以下、KSVLA) は、VMware vSphere および Microsoft Hyper-V、Acropolis Hypervisor 等の仮想化基盤に構築されている仮想サーバーや仮想デスクトップ(VDI)に対し、最新のセキュリティテクノロジーを提供し、多重多層防御を用いて保護を行います。

KSVLA のシステム要件は以下の URL にて必ず確認してください。

- システム要件
  https://support.kaspersky.com/KSVLA/5.1/ja-JP/64743.htm
  仮想化基盤毎に注意点等が記載されています。

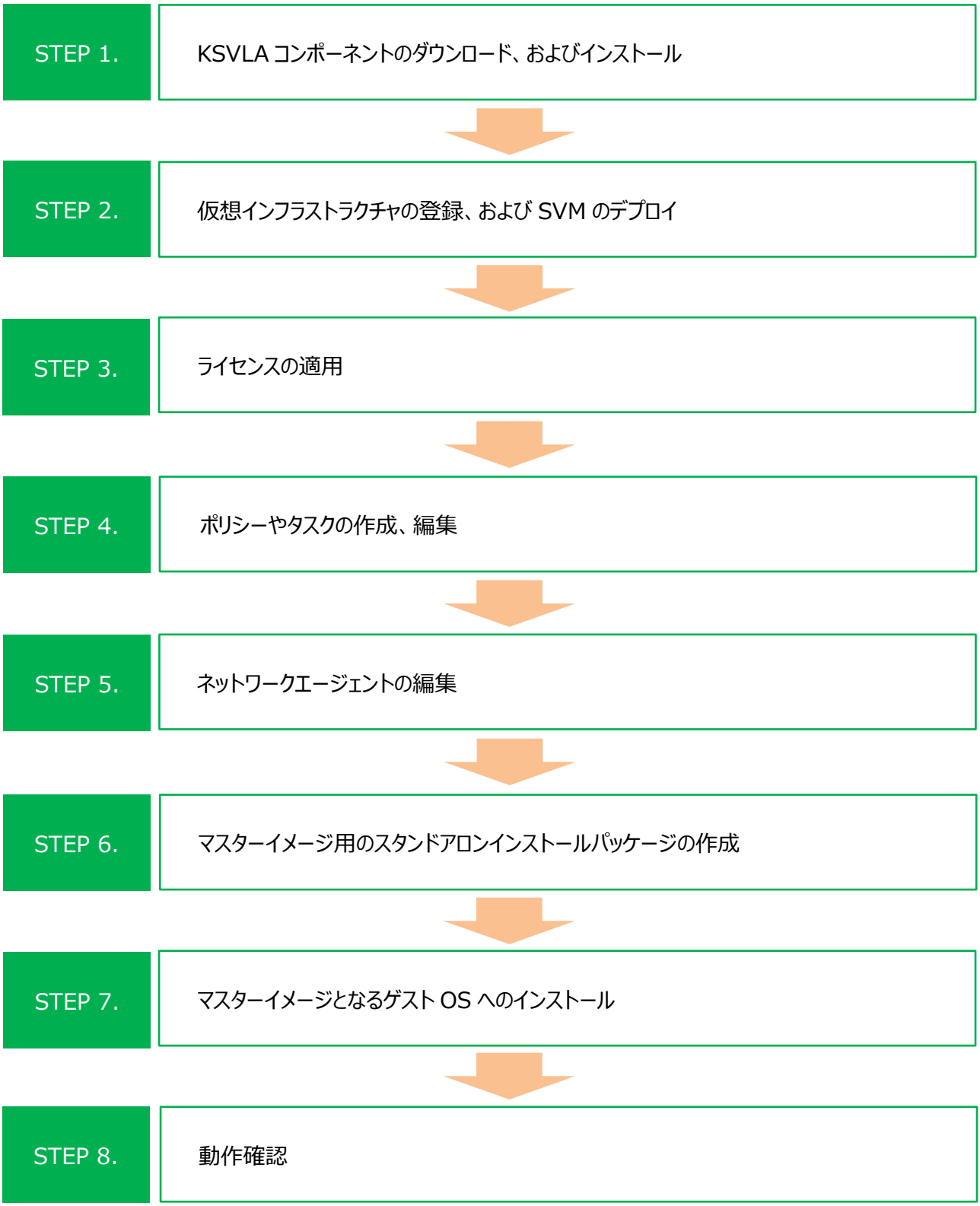
1.3. 前提条件

以下、前提条件です。

- **KSC12 が構築済みであること(12.2.0.4376 が 2020/11/17 現在の最新バージョン)**
  KSC の構築は https://kasperskylabs.jp/biz/にある資料を参照ください。
  また KSC のシステム要件は以下の URL にてご確認ください。
  https://support.kaspersky.com/ksc/12/ja-JP/96255.htm
- **名前解決(正、逆引き共に)が問題なくできる環境にあること**
- **製品をアクティベーションするための有効なライセンスキーファイル、もしくはアクティベーションコードを保有していること**
- **Internet 接続ができる環境であること**

1.4. インストールの流れ

以下の流れでインストール、及び設定を行います。

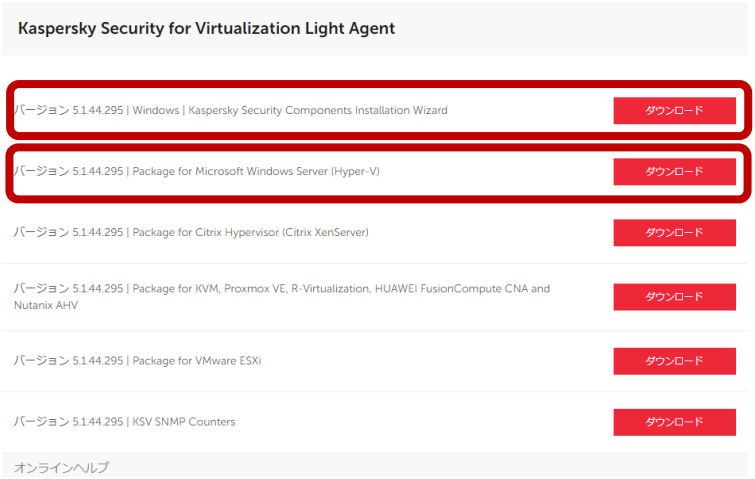


2. KSVLA コンポーネントのダウンロード、およびインストール

以下の手順にて KSVLA コンポーネントのダウンロード、およびインストールを行います。
また併せて Integration Server のアカウント(admin)のパスワード設定や基本的なポリシー、タスクの自動生成も行います。

1. 外部アクセスができる環境で以下のサイトへアクセスします。
2. https://www.kaspersky.co.jp/small-to-medium-business-security/downloads/virtualization-hybrid-cloud

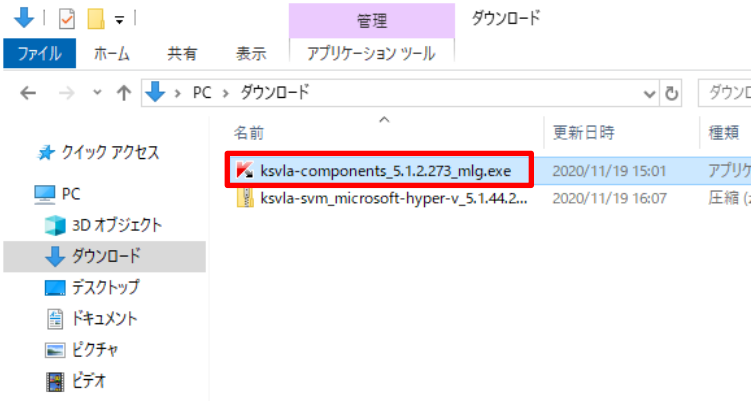
   画面をスクロールし”Kaspersky Security for Virtualization Light Agent”下部にある「**Kaspersky Security Components Installation Wizard**」と「**Package for Microsoft Windows Server（Hyper-V）**」のところにある「ダウンロード」をクリックします。



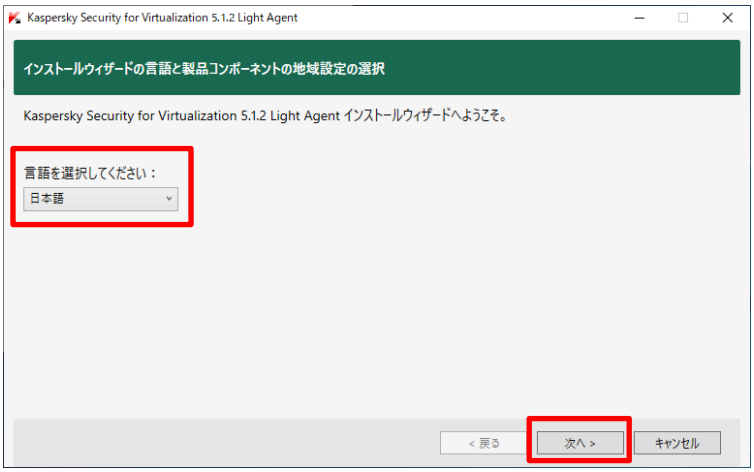
3. ダウンロードしてきた KSVLA の管理コンポーネントと SVM を KSC に複製します。

   その後、管理コンポーネントである ksvla-components_5.1.2.273_mlg.exe を実行します。

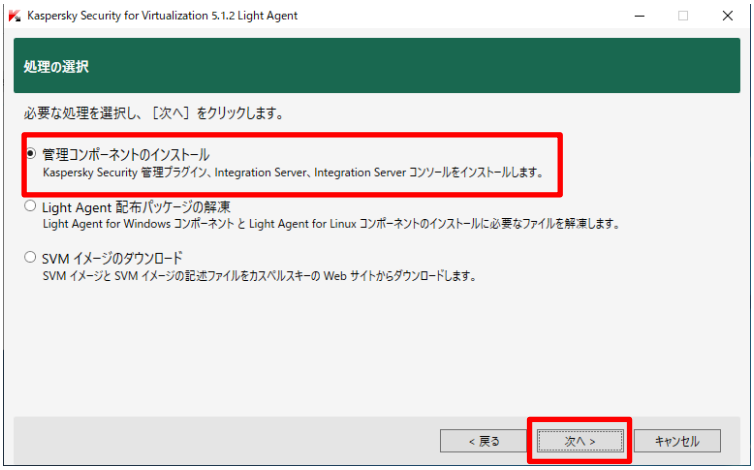
   なお、KSC の GUI が起動している場合は終了しておいてください。



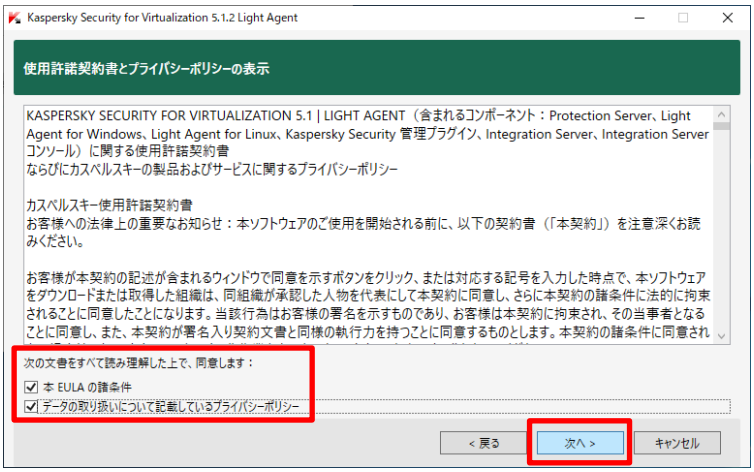
4. インストールウィザードが起動するので、言語選択の部分が日本語になっていることを確認し、「次へ」をクリックします。



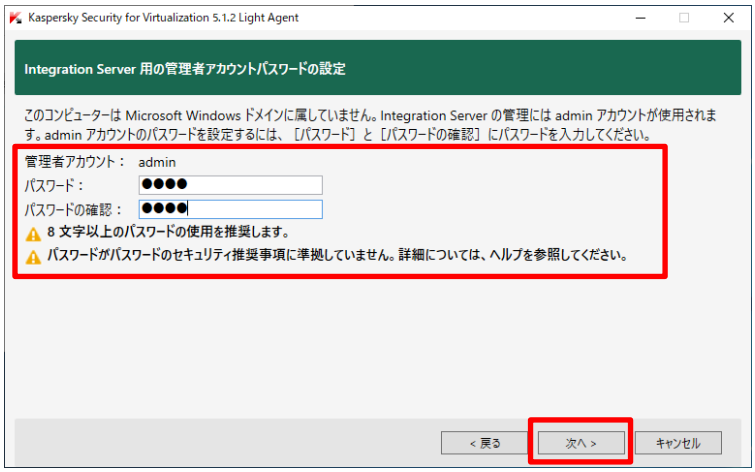
5. “処理の選択”画面では「管理コンポーネントのインストール」が選択されていることを確認し、「次へ」をクリックします。



6. 使用許諾契約書とプライバシーポリシー画面が表示されるので、画面下部にある 2 か所のチェックボックスにチェックを入れ、「次へ」をクリックします。



7. Integration Server 用管理者アカウントの設定画面が表示されます。

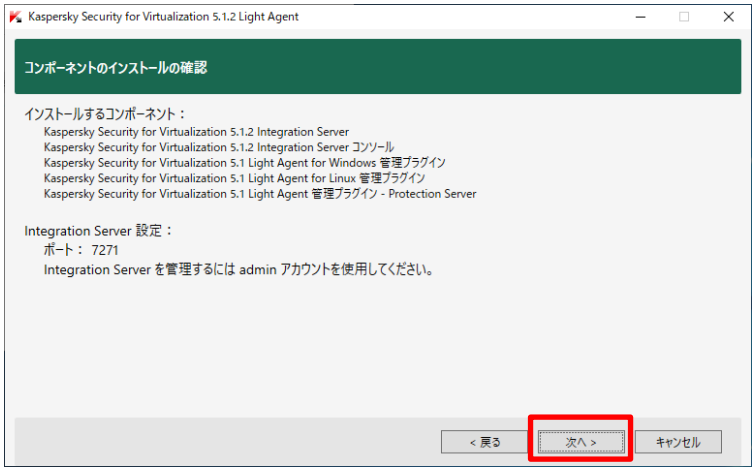


セキュリティの観点から、長さは 8 文字以上、小、大文字、数字、特殊文字の 4 つカテゴリから 3 つ以上使用したパスワードを設定することを推奨します。

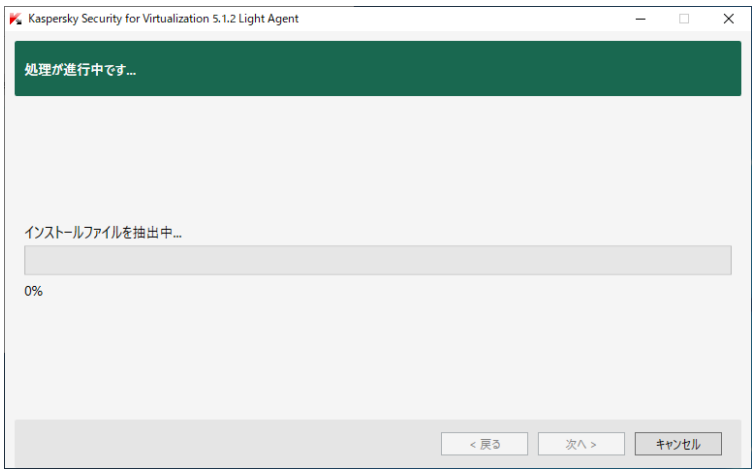
本資料ではわざと要件を満たさない画面を表示しています。

設定後、「次へ」をクリックします。

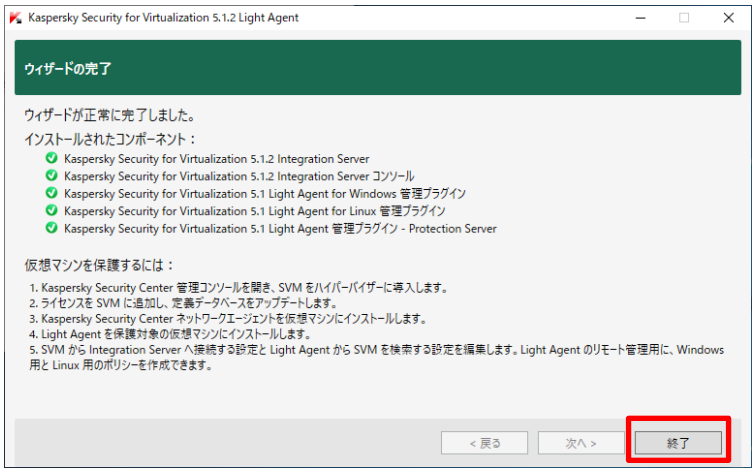
8. コンポーネントのインストールの確認画面が表示されます。
「次へ」をクリックしてウィザードを進めます。



9. コンポーネントのインストール完了までしばらくお待ちください。



10. インストールが完了するとウィザードの完了画面が表示されます。
「終了」をクリックしてウィザードを終了します。



11. コンポーネントのインストール後、KSC の GUI を起動します。
起動すると KSVLA for Windows のクイックスタートウィザードが起動してくるので「次へ」をクリックしてウィザードを進めます。

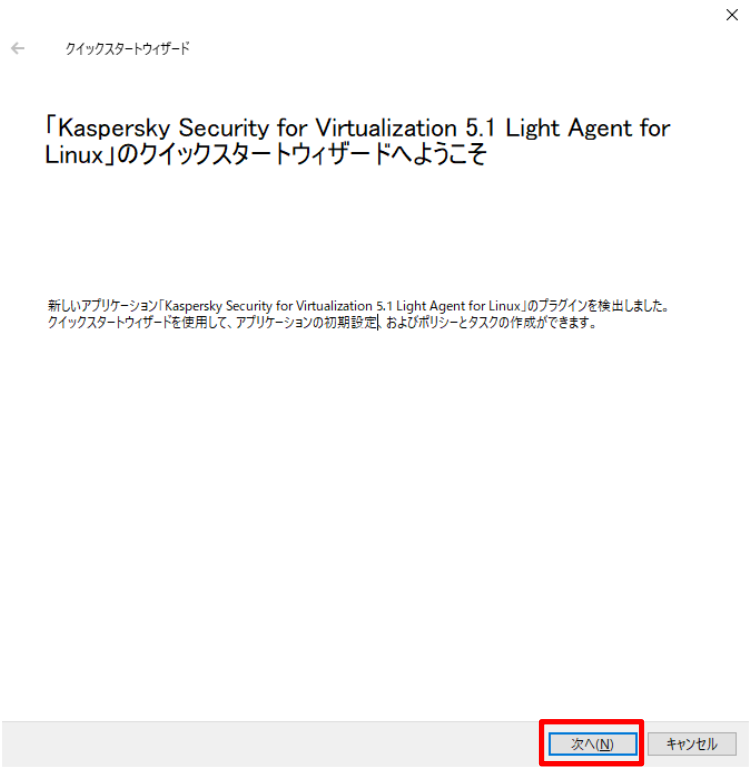
その後、「完了」が表示されるのでクリックしてウィザードを　終了します。

この処理で for Windows 用のスキャンタスクが作成されます。
作成されたスキャンタスクは後から編集できます。

12. 同じく KSVLA for Linux のクイックスタートウィザードが起動してくるので「次へ」をクリックしてウィザードを進めます。

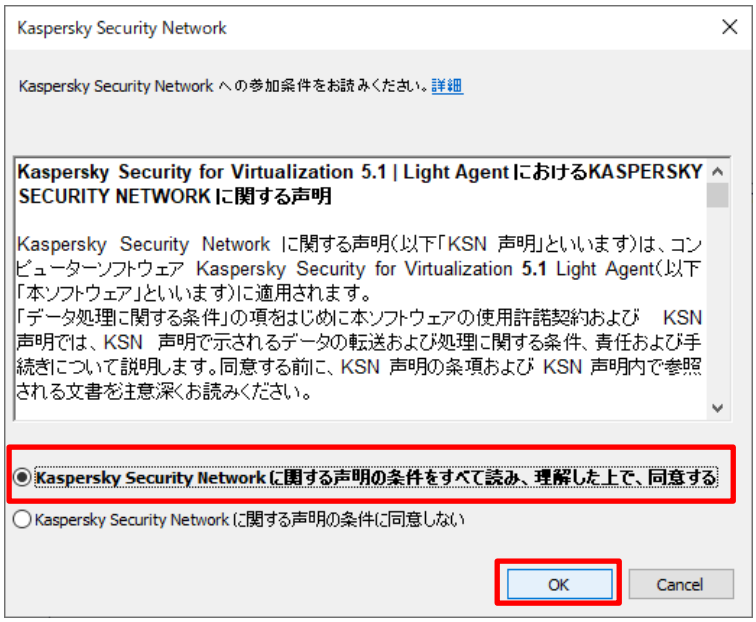
    その後、「完了」が表示されるのでクリックしてウィザードを　終了します。

    この処理で for Linux 用のスキャンタスクが作成されます。
    作成されたスキャンタスクは後から編集できます。



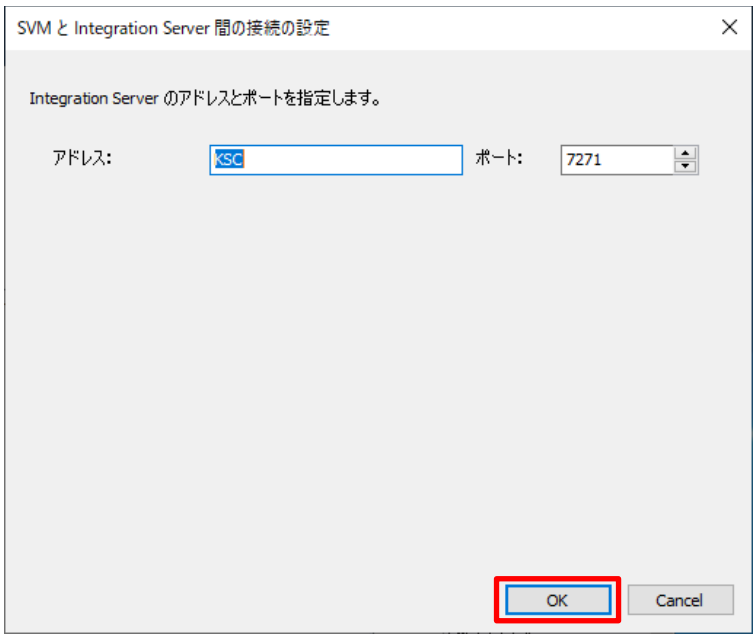
13. 続いて KSVLA Protection Server のクイックスタートウィザードが起動してくるので「次へ」をクリックします。

14. Kaspersky Security Network の声明画面が表示されます。
画面下部にある「Kaspersky Security Network に関する声明の条件をすべて読み、理解した上で、同意する」を選択し、「OK」をクリックします。



15. Integration Server 証明書の確認画面が表示されるので「無視」をクリックします。

16. SVM と Integration Server 間の接続の設定画面が表示されます。
Integration Server のアドレスとして KSC のホスト名、もしくは IP アドレスを入力し、「OK」をクリックします。



17. Integration Server への接続画面が表示されます。さきほど設定したパスワードを入力し、「OK」をクリックします。

その後、「完了」が表示されるのでクリックしてウィザードを 終了します。

この処理で SVM 用のポリシーが作成されます。
このポリシーは後ほど編集することもできます。

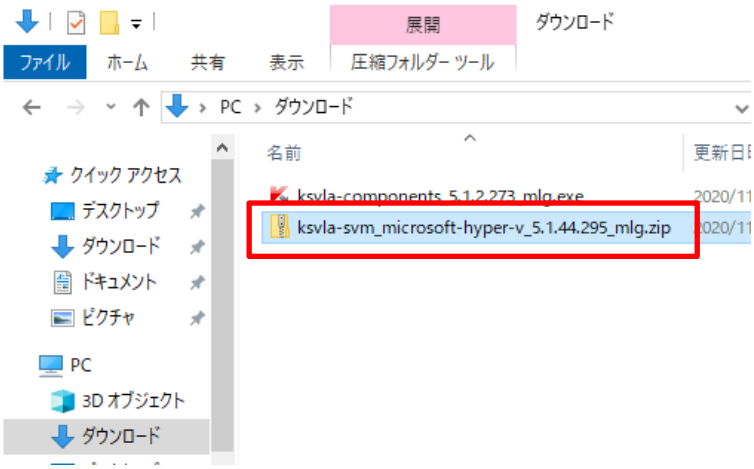
以上で KSVLA のコンポーネントの DL、およびインストールのインストールは終了です。
続いて Integration Server へ仮想インフラストラクチャの登録、および SVM のデプロイを行います。

3. 仮想インフラストラクチャの登録、および SVM のデプロイ

次に Integration Server に仮想インフラストラクチャの登録と SVM のデプロイを行います。
以下より手順です。

1. 先の手順で DL した zip ファイルを OS の機能等を使い、展開します。
   このファイルが SVM です。

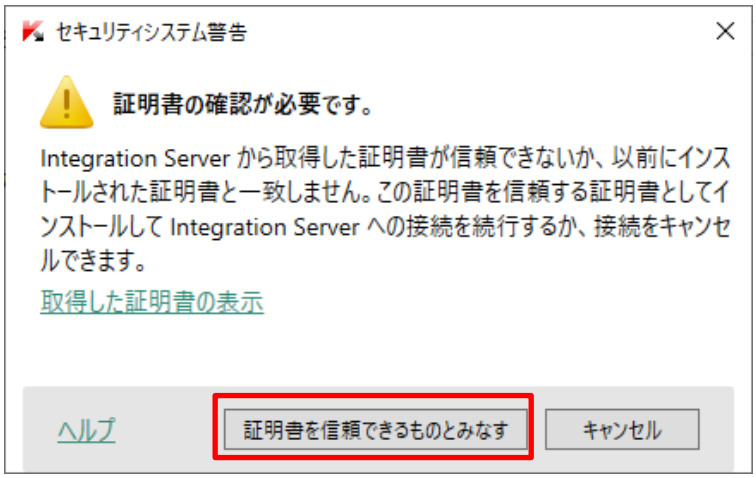
   展開後のサイズが大きいため、disk に余裕のある場所に展開してください。
   本手順では"ダウンロード"フォルダ内に展開しています。



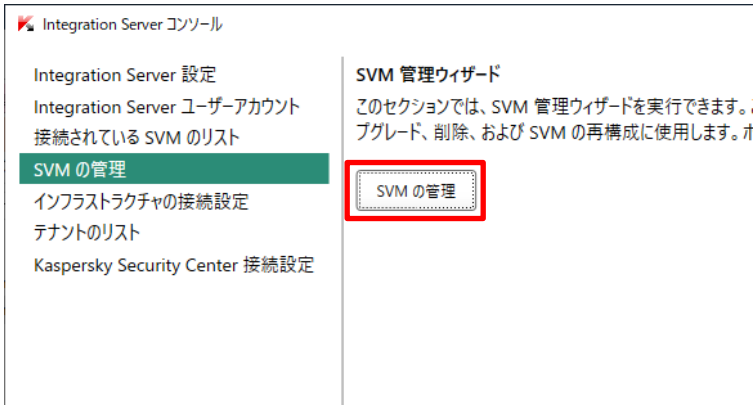
2. 次に Integration Server を起動します。
   KSC の GUI を起動し、左側の項目から「管理サーバー ホスト名」を選択、その後、右側の画面で"製品の導入"内にある「Kaspersky Security for Virtualization 5.1.2 Light Agent を管理する」をクリックします。

3. Integration Server コンソールにアクセスするための画面が表示されるので、先の手順で設定したパスワードを入力し、「接続」をクリックします。

4. セキュリティシステム警告画面が表示されるので、「証明書を信頼できるものとみなす」をクリックして進めます。



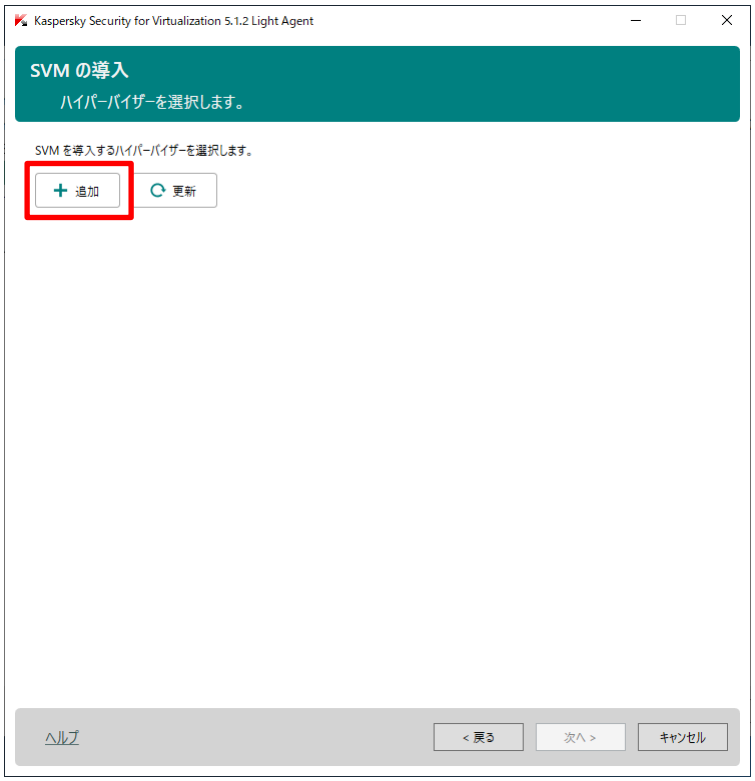
5. Integration Server コンソールが表示されます。
このコンソールを使い、SVM のデプロイや変更等を行います。
まず初めに「SVM の管理」をクリックします。



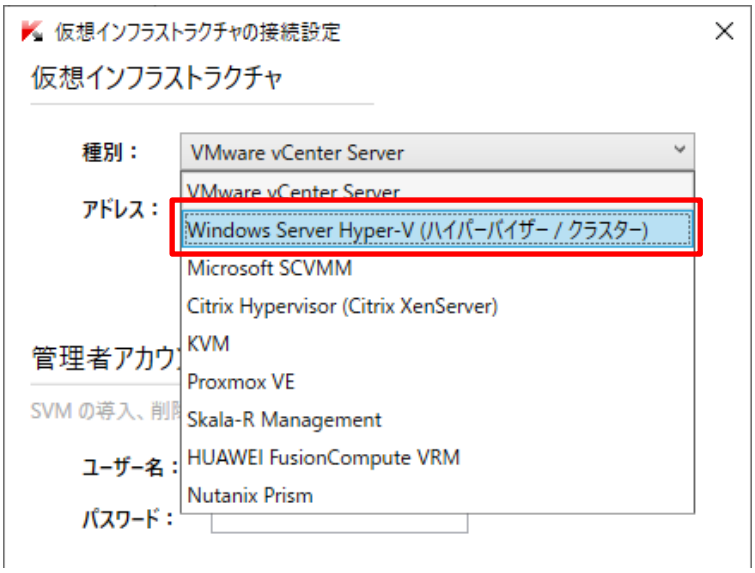
6. ウィザードが起動してきます。
「SVM の導入」が選択されていることを確認して「次へ」をクリックします。

7. SVM をデプロイする先の Hypervisor を登録する必要があります。
「追加」をクリックして処理を進めます。

なお、この処理は初回のみです。
また新しく Hypervisor が追加され、そこに SVM をデプロイしたい、ということが発生した場合は「追加」をクリックして追加処理をしてください。

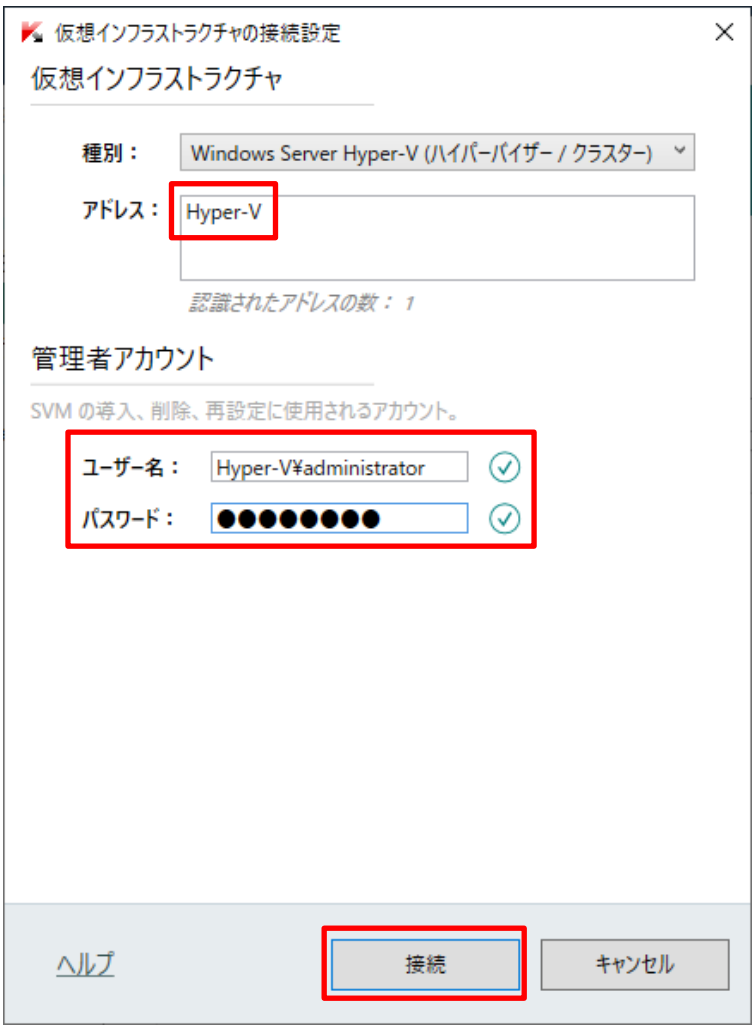


8. 仮想インフラストラクチャの選択画面が表示されます。
“種別”のところのメニューを展開し、「Windows Server Hyper-V(ハイパーバイザー/クラスター)を選択します。



9. “アドレス”部分に Hyper-V のアドレスを入力します。

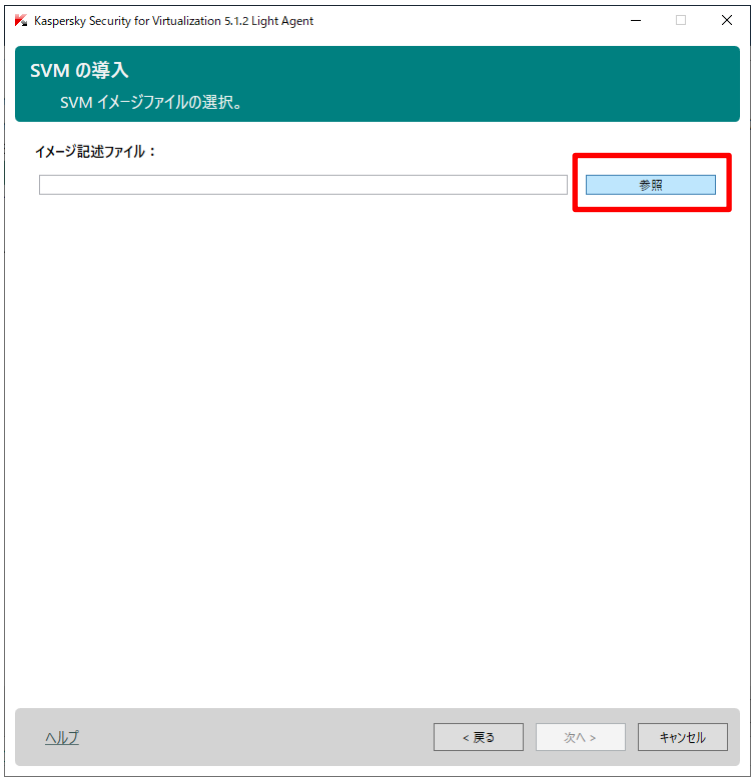
その後、”管理者アカウント”のところでユーザー名、パスワードを入力した後、「接続」をクリックします。



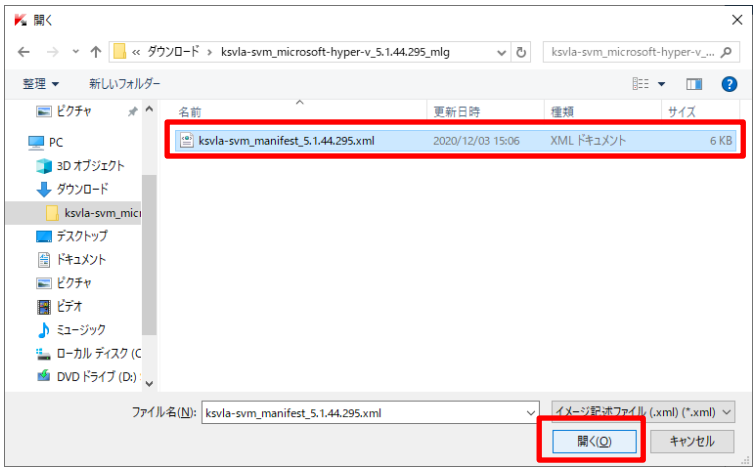
10. 接続に成功するとハイパーバイザーの IP アドレスまたはホスト名が表示され、名前の左に緑色の「○」が表示されます。
(本資料ではホスト名で表示されています)

導入対象ハイパーバイザーのところにあるチェックボックスにチェックを入れ、「次へ」をクリックします。

11. “SVM の導入”画面が表示されるので、「参照」をクリックします。

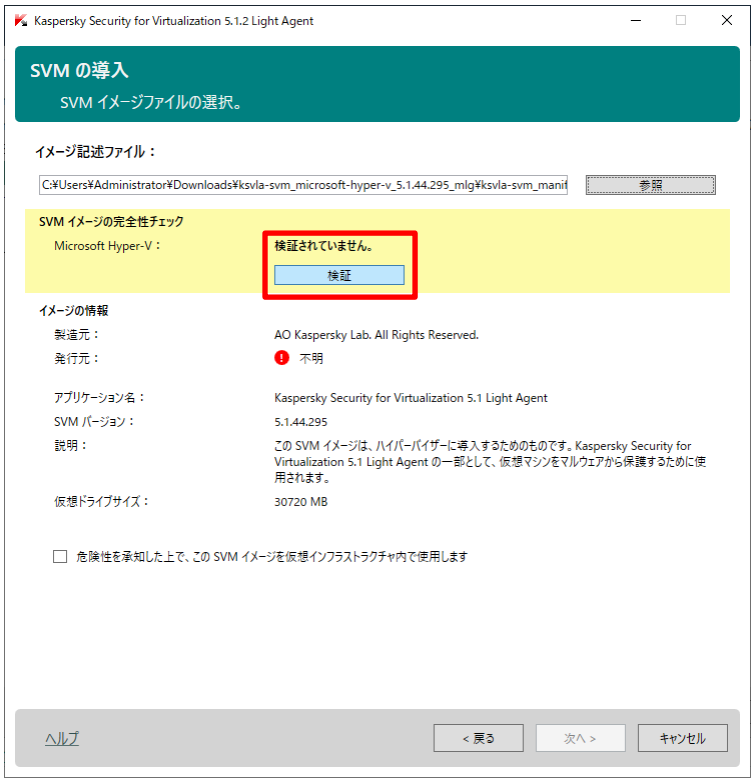


12. 展開した SVM イメージファイルを選択し、「開く」をクリックします。

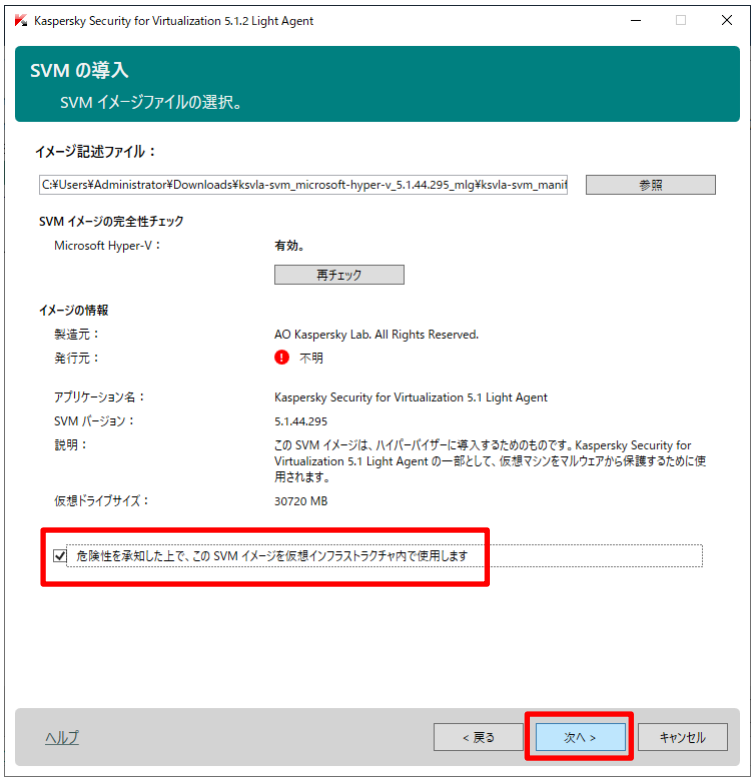


13. 「検証」をクリックし、“SVM イメージの完全性チェック”を行います。

なお、この検証を行わなくてもデプロイは可能ですが、状況が許す限り検証は実施ください。

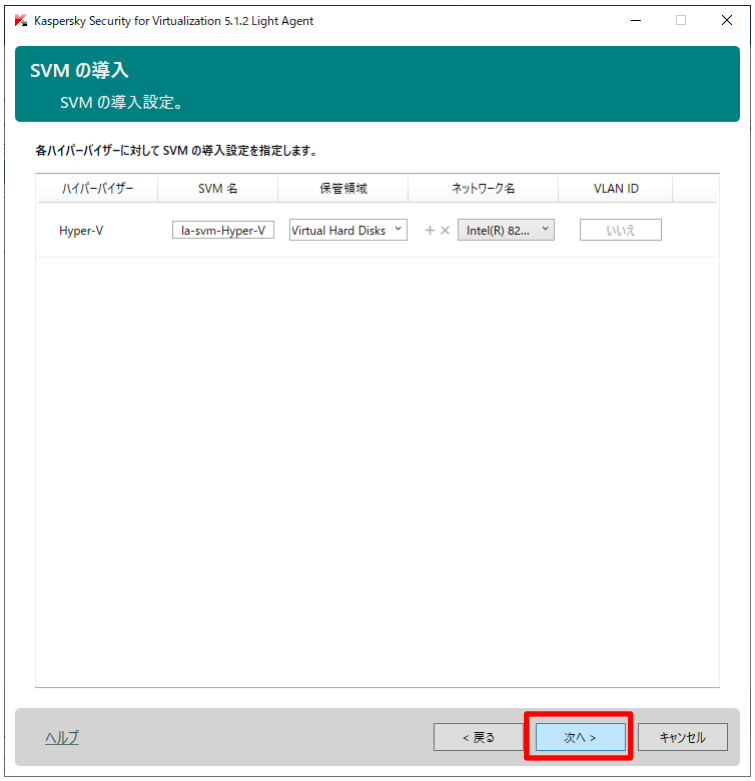


14. 検証が完了後、「危険性を承知した上でこの SVM イメージを仮想インフラストラクチャ内で使用します」にチェックを入れ、「次へ」をクリックします。



15. “SVM の導入”画面が表示されます。ここでは SVM の名前や保管領域等の変更ができます。

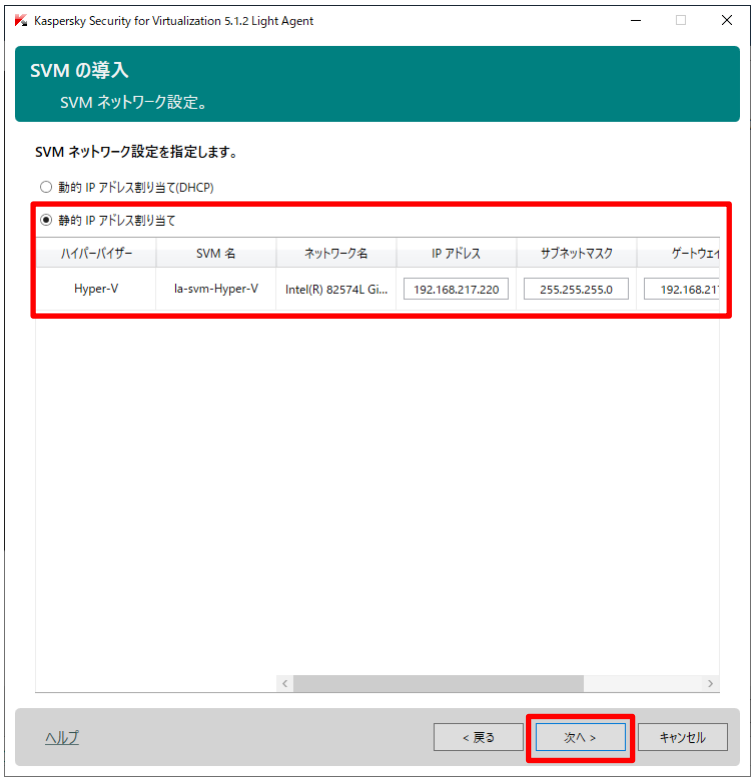
    本資料では SVM 名や保管領域等の値は初期値のまま処理を進めます。



16. 次に SVM の割り当てる IP アドレスの設定を行います。
初期値では”動的 IP アドレス割り当て”が選択されていますが、これを「性的 IP アドレス割り当て」に変更し、その後、適切な IP アドレス等を入力します。

入力するのは
・IP アドレス
・サブネットマスク
・デフォルトゲートウェイ
・DNS サーバー、代替 DNS サーバー
これらを入力ください。

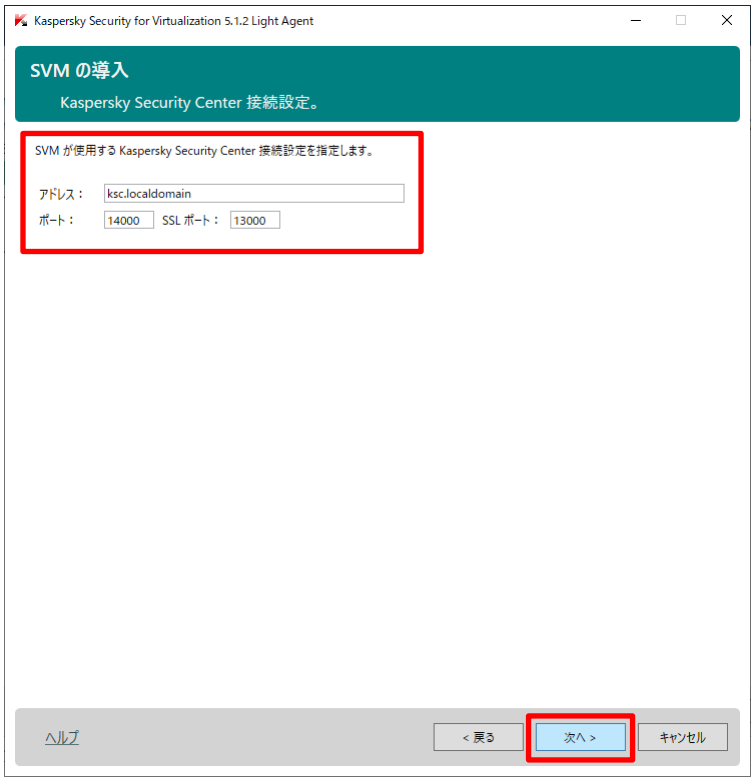
入力後、「次へ」をクリックします。



17. Kaspersky Security Center への接続設定を行います。
(SVM のネットワークエージェントの設定)

各値は自動的に入力された状態ですので問題がなければ「次へ」をクリックして処理を進めます。

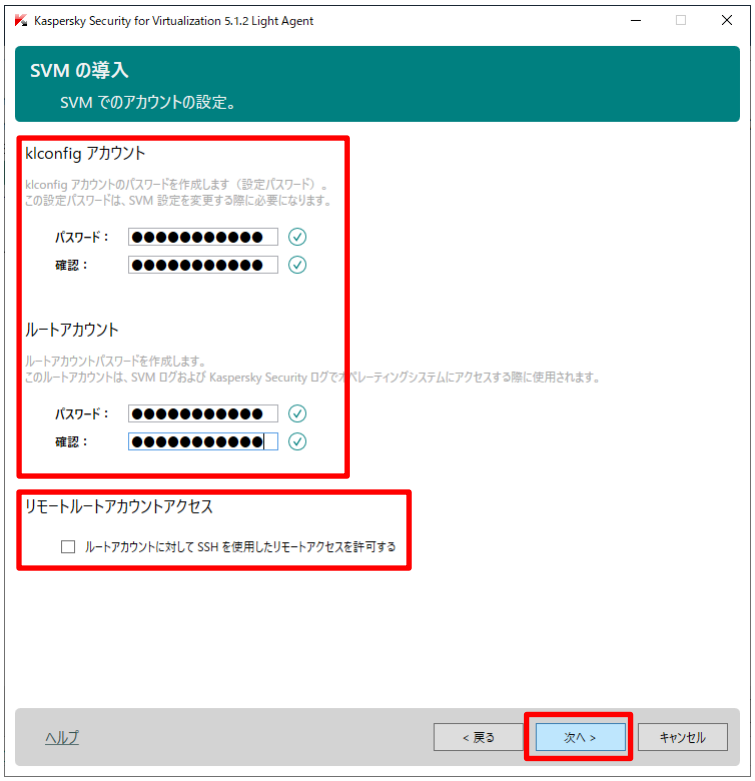
何か不都合(名前解決ができていない等)があれば適切な変更をここで行ってください。



18. 次に SVM のアカウント設定を行います。"klconfig アカウント"、”ルートアカウント”それぞれに適切なパスワードを入力し、「次へ」をクリックします。

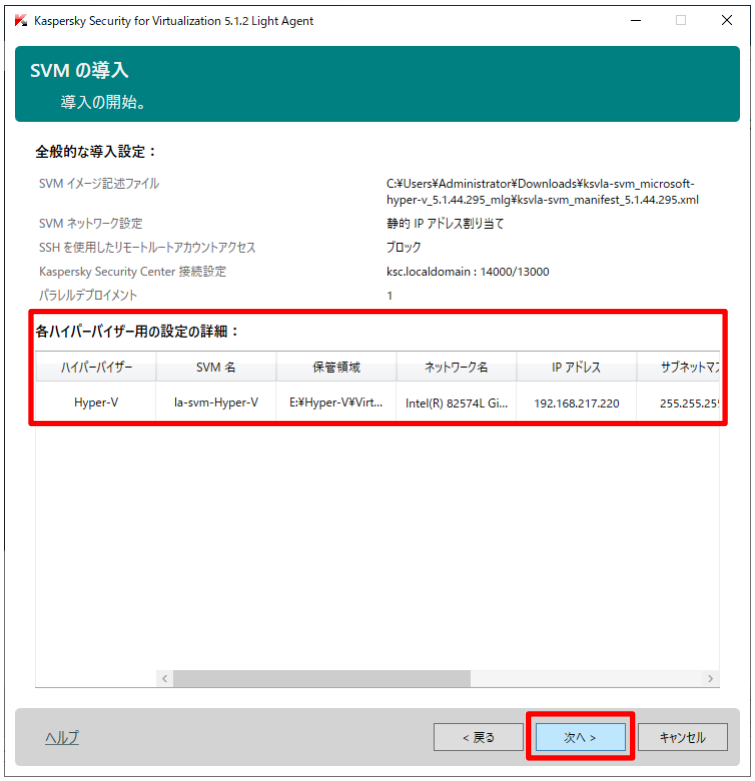
なお、”リモートルートアカウントアクセス”のところにあるチェックボックスは必要に応じてチェックを入れてください。

本資料ではチェックを入れず進めます。



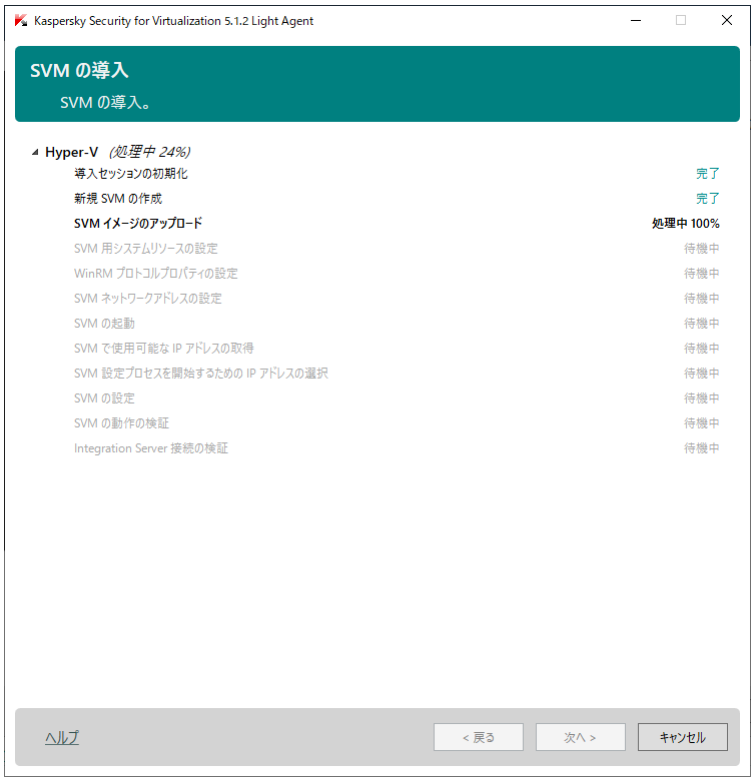
19. 最終確認画面が表示されます。何も問題がなければ「次へ」をクリックします。

もし変更したい項目がある場合は「戻る」を利用して該当項目まで戻ってください。

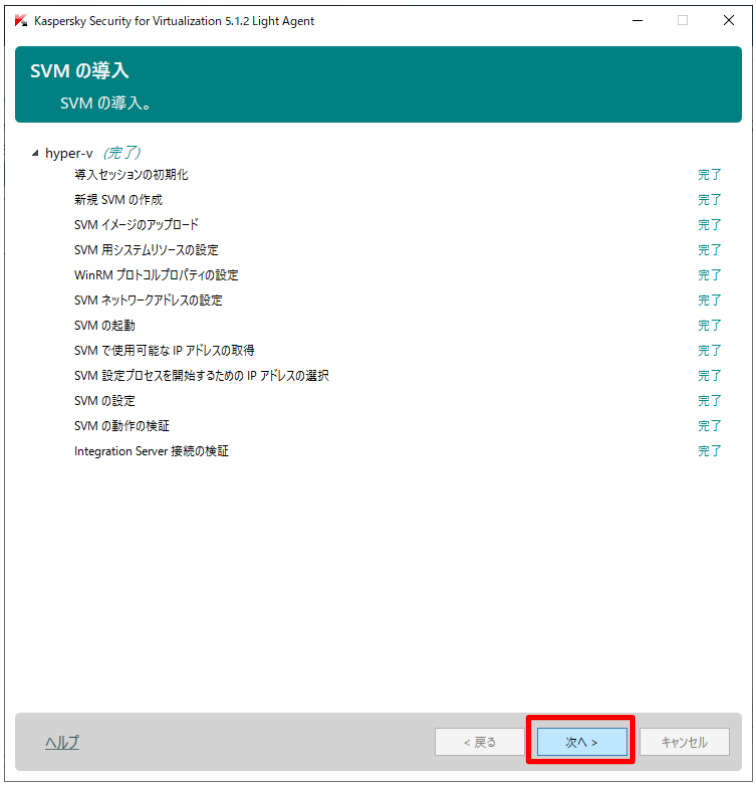


20. SVM のデプロイが終了するまで少々お待ちください。

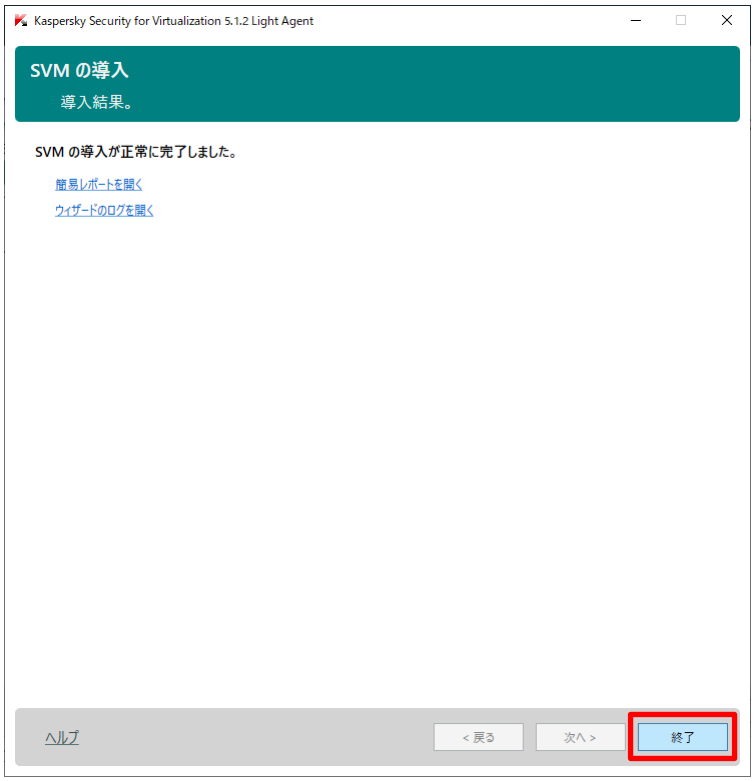
この画面はデプロイ中の詳細を表示するため、ツリーを展開しています。



21. すべての項目が"完了"となり、デプロイが正常に終了しました。
「次へ」をクリックします。

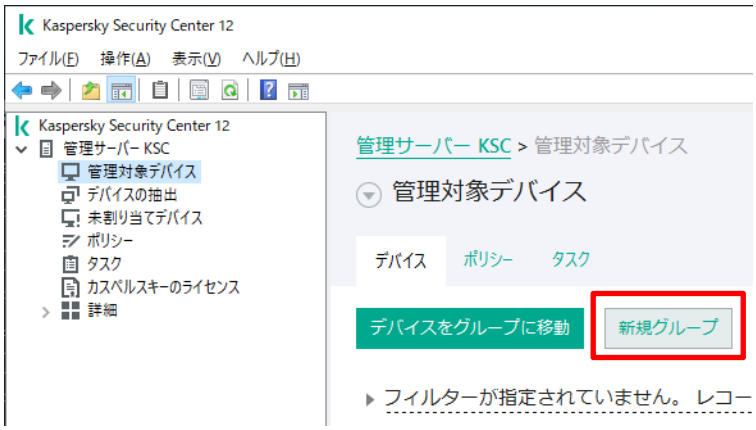


22. SVM のデプロイが終了したことが表示されます。
「終了」をクリックし、ウィザードを終了します。



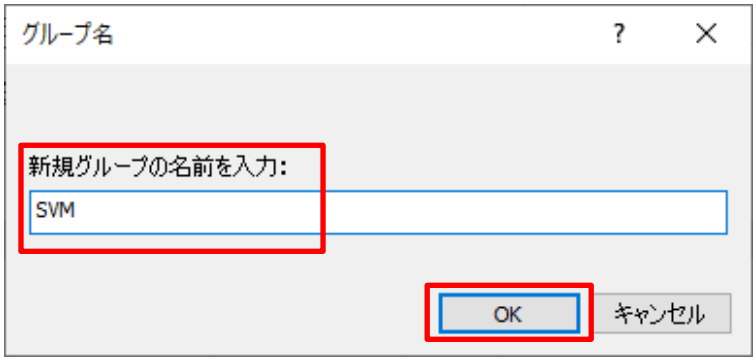
23. デプロイが完了した SVM ですが、そのままではまだ利用することができません。
そのため KSC の管理配下へ移動します。
その準備として専用グループを作成します。

「新規グループ」をクリックします。

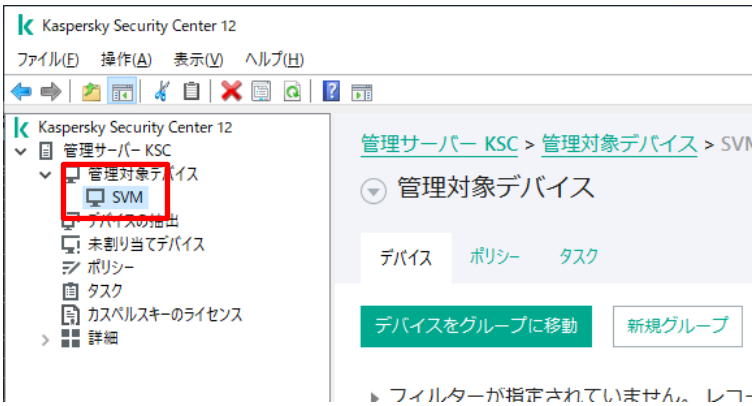


24. 新規グループ名を入力する画面が表示されるので、適切な名前を入力し、「OK」をクリックします。

本資料では「SVM」として処理を進めます。



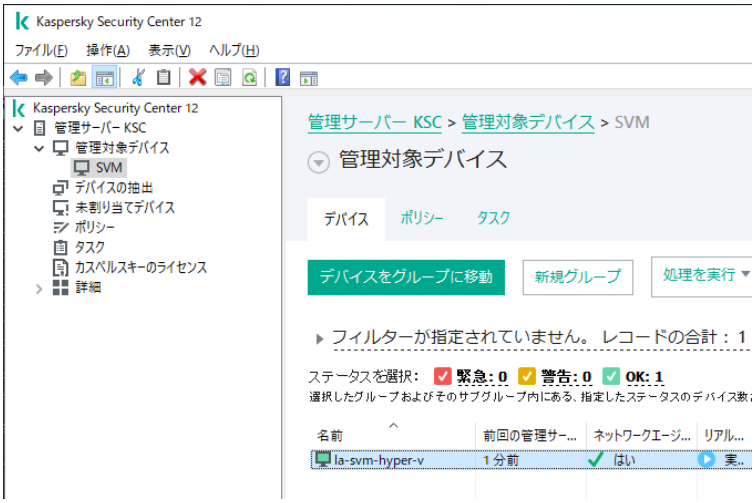
25. SVM グループが作成されたことがわかります。こちらへ先ほどデプロイした SVM を移動します。



26. デプロイされた SVM は「未割り当てデバイス」配下にいます。
これを先ほど作成した SVM グループへ移動します。

移動方法は SVM を選択後、ドラッグ＆ドロップで SVM グループへ移動してください。

27. SVM グループにデプロイした SVM が移動し、アイコンの色も変わったことがわかります。

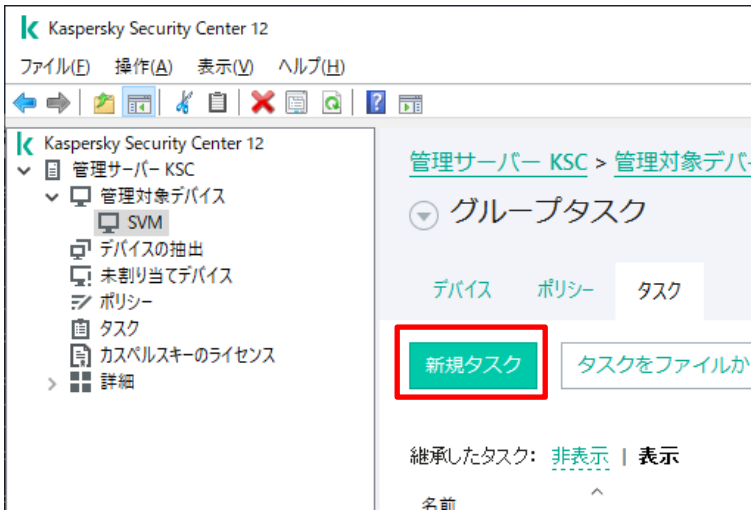


以上で Integration Server へ仮想インフラストラクチャの登録、および SVM のデプロイは終了です。
続いてライセンスの適用を行います。

4. ライセンスの適用

次に SVM へ KSVLA のライセンス適用を行います。
ライセンス適用は SVM のみのため、仮想マシン（VM）に対してのライセンス適用は不要です。
なお、事前に KSC に対し、KSVLA のライセンスは登録済みです。
もし登録を行っていない場合は登録処理を行ってから以下手順を実施ください。

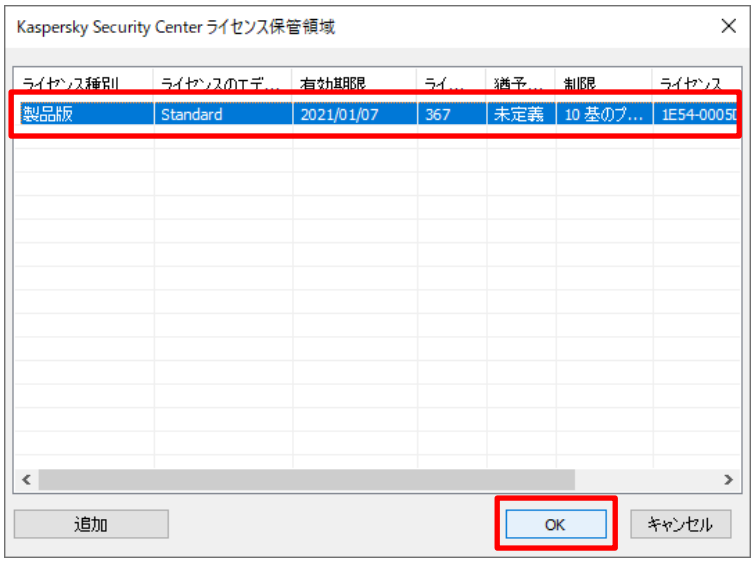
1. SVM グループを選択した状態で右側の画面から「タスク」を選択し、「新規タスク」をクリックします。



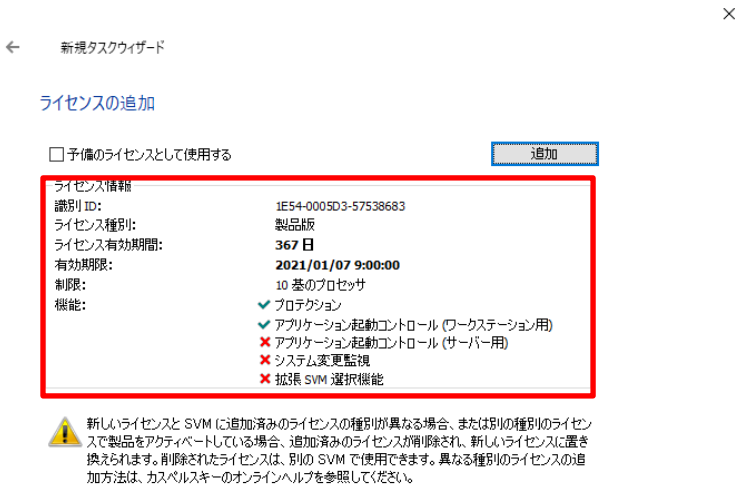
2. “新規タスクウィザード”が起動してきます。タスク一覧の中から”Kaspersky Security for Virtualization 5.1 Light Agent – Protection Server” 内にある「アプリケーションのアクティベーション」を選択し、「次へ」をクリックします。

3. “ライセンスの追加”画面が表示されるので「追加」をクリックします。

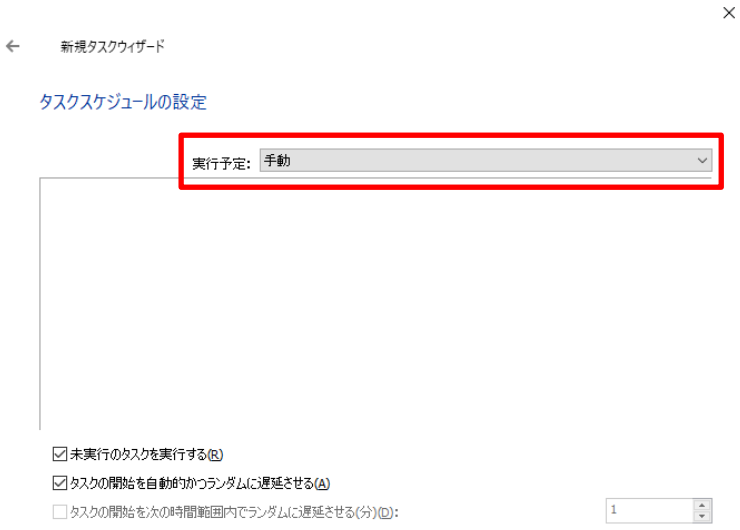
4. KSC に登録されているライセンスが表示されます。
   適切なライセンスを選択し、「OK」をクリックします。



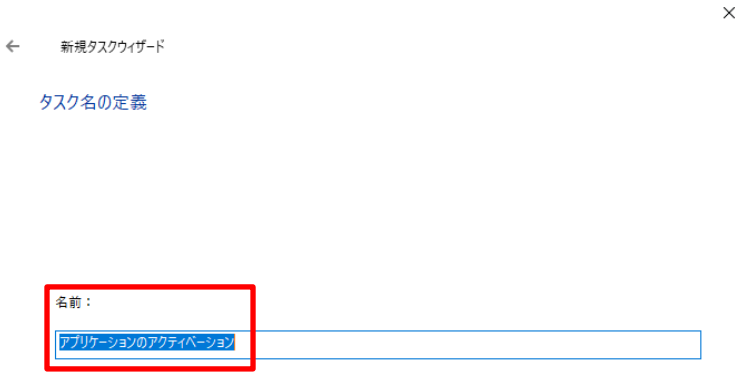
5. “ライセンスの追加”画面に戻るので内容に相違がないことを確認し、「次へ」をクリックします。



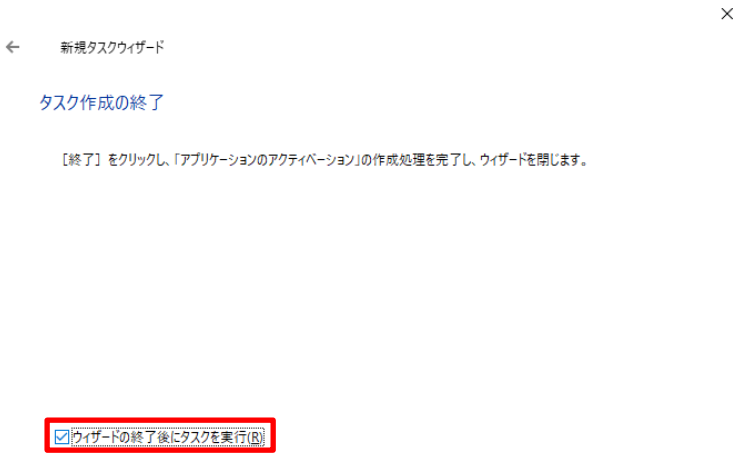
6. スケジュール設定画面では初期値のまま、「次へ」をクリックします。



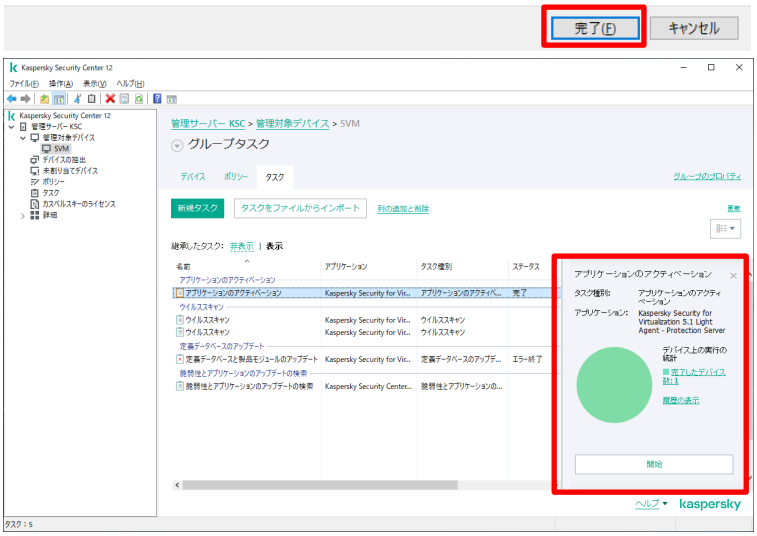
7. “タスク名の定義”画面が表示されるので、適切なタスク名を入力し、「次へ」をクリックします。
本資料では初期値のまま進めます。



8. “タスク作成の終了”画面が表示されます。
「ウィザードの終了後にタスクを実行」にチェックを入れ「終了」をクリックします。



9. KSC の GUI を確認し、先ほど作成したタスクが完了していることを確認します。

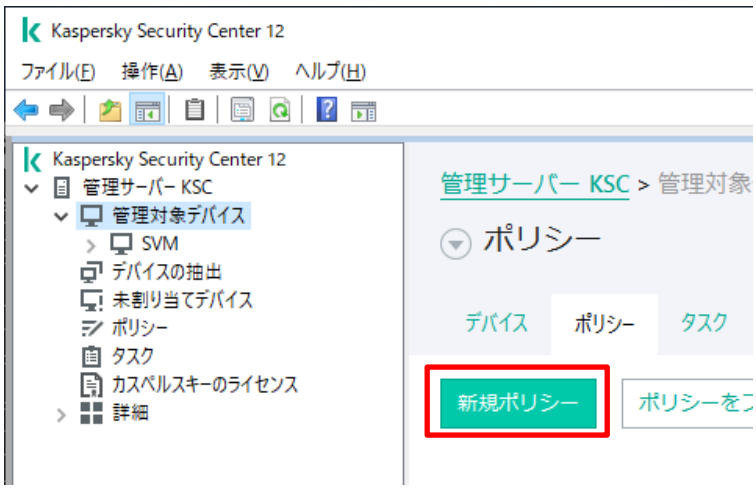


以上でライセンスの適用は終了です。

5. ポリシーやタスクの作成、編集

次にゲスト OS にインストールする KSVLA for Windows 用のポリシーの作成やタスクの編集を行います。
まず、KSVLA for Windows のポリシーを作成します。
なお、本資料では KSVLA for Linux 用のポリシーやタスクについては触れませんが、基本的な操作は同じです。

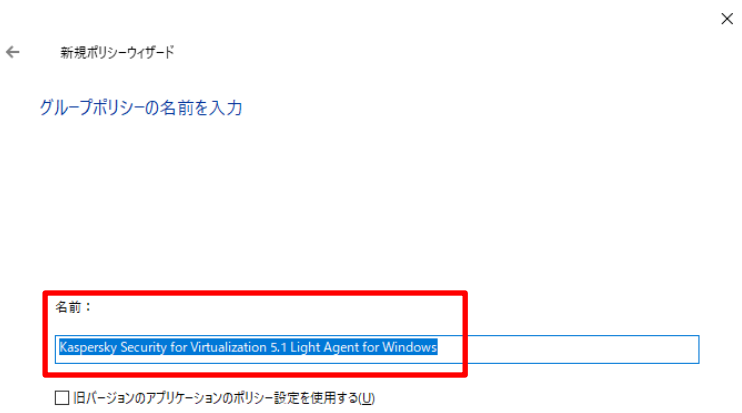
1. まず KSVLA for Windows のポリシーを作成します。
   左側の項目から「管理対象デバイス」を選択し、右側画面の「ポリシー」タブを選択、その後、「新規ポリシー」をクリックします。



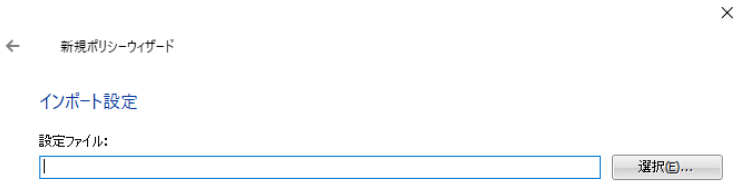
2. “新規ポリシーウィザード”画面が起動してくるので、「Kaspersky Security for Virtualization 5.1 Light Agent for Windows」を選択し、「次へ」をクリックします。

3. ポリシーの名前を入力する画面が表示されるので適切な名前を入力し、「次へ」をクリックします。

   本資料では初期値のまま進めます。

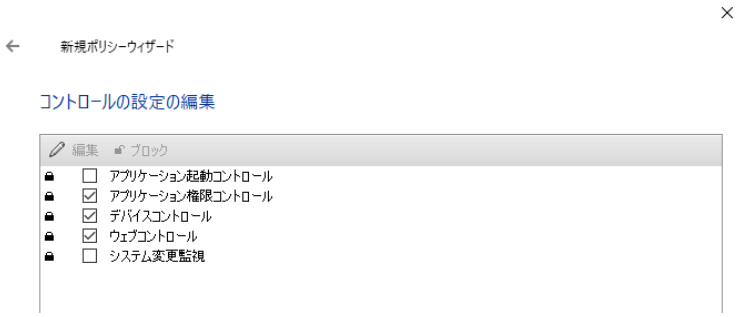


4. “インポート設定”画面では何もせず、「次へ」をクリックします。



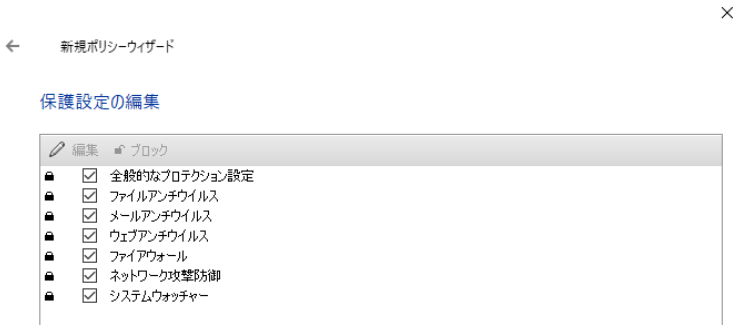
5. “コントロールの設定の編集”画面では初期値のまま、「次へ」をクリックします。

   各機能の有効/無効はポリシー作成後に変更可能です。



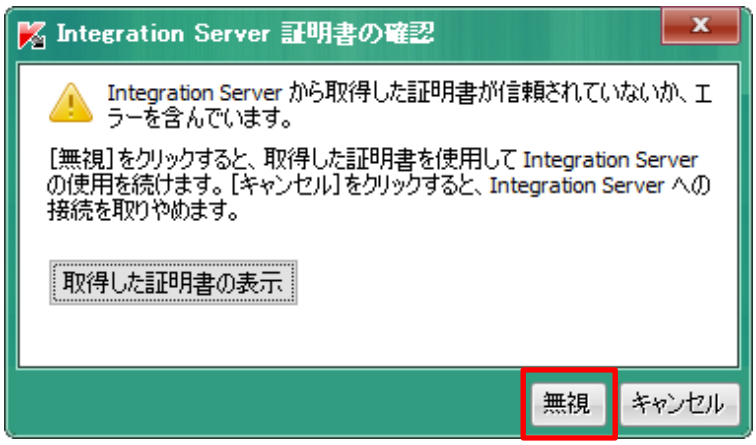
6. “保護設定の編集”画面では初期値のまま、「次へ」をクリックします。

   各機能の有効/無効はポリシー作成後に変更可能です。



7. “SVM 検出設定”画面では「Integration Server を使用する」が 選択されており、Integration Server(KSC)のアドレスが入っていることを確認し、「次へ」をクリックします。

8. “Integration Server 証明書の確認”画面が表示されるので「無視」をクリックします。



9. 続いて”Integration Server への接続”画面が表示されます。

   事前に設定したパスワードを入力後、「OK」をクリックします。

10. “除外リスト”画面では何もせずに「次へ」をクリックします。

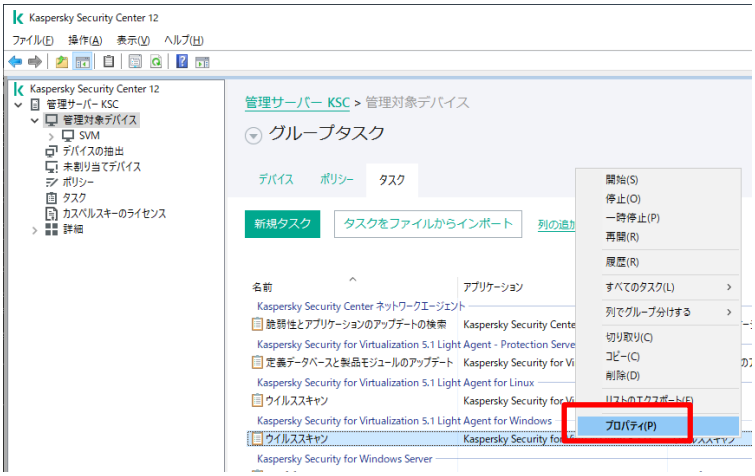
11. “インターフェース”画面では初期値のまま、「次へ」をクリックします。

12. “パスワードによる保護”画面では何もせず「次へ」をクリックします。

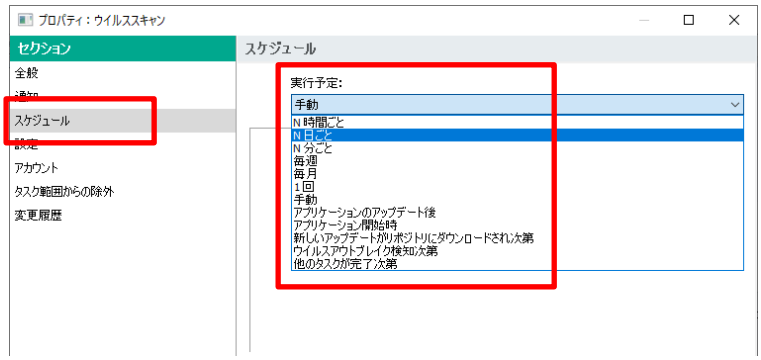
13. “アプリケーションのグループポリシーを作成”画面では「アクティブポリシー」が選択されていることを確認し、「完了」をクリックします。

14. ポリシーが作成されたことが KSC の GUI にて確認ができます。

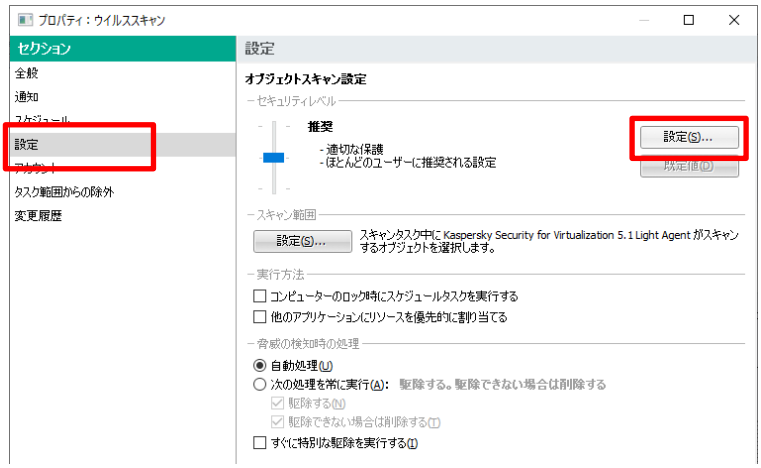
15. 続いて KSVLA for Windows のスキャンタスクを編集します。
このタスクは既に作成されているタスクです。
該当タスクを右クリックし、メニューの中から「プロパティ」を選択します。



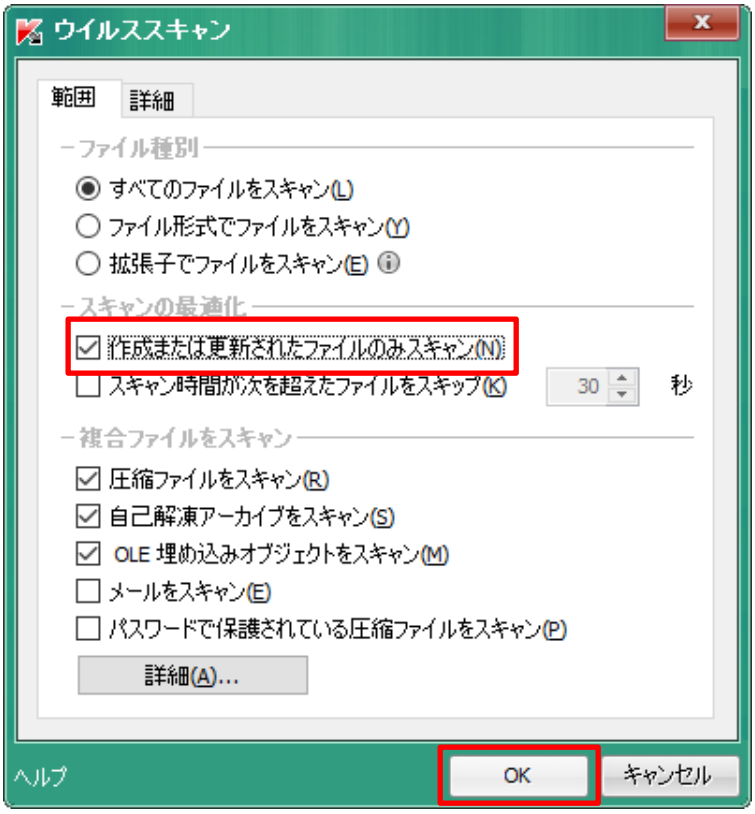
16. プロパティ画面、左側の項目から「スケジュール」を選択します。
初期値だと「手動」になっているので適切なタイミングを選択し、スキャンスケジュールの設定を行います。



17. 続いて差分スキャンの機能を有効にします。
左側の項目から「設定」を選択し、右側の画面内にある「設定」をクリックします。



18. 設定画面が表示されるので、「作成または更新されたファイルのみスキャン」のチェックボックスにチェックをいれ、「OK」をクリックします。



19. プロパティ画面に戻ってきます。
“セキュリティレベル”の部分がカスタムに
変わったことを確認し、「OK」をクリックして
編集を終えます。

以上でポリシーの作成、およびタスクの編集は終了です。
続いてゲスト OS にインストールするネットワークエージェントの設定変更を行います。

kaspersky

6. ネットワークエージェントの編集

次にゲスト OS へインストールするネットワークエージェントの編集を行います。
この編集を行うことで仮想デスクトップインフラストラクチャ(VDI)環境に特化した設定や仮想化環境のパフォーマンス向上が見込める機能を有効にできます。

＊＊＊＊注意＊＊＊

仮想デスクトップインフラストラクチャ(VDI)を使用する、のところにある各オプションについて簡単に説明します。

【VDI 向け動的モードを有効にする】
これはマスターイメージとなるゲスト OS にインストールする場合のみチェックを入れてください。
このため、「動的モードを有効にする」オプションを有効にしたネットワークエージェントは VDI 環境以外には利用はお止めください。

オンラインヘルプ
https://support.kaspersky.com/ksc/12/ja-JP/67243.htm

【VDI 向けに設定を最適化する】
実行ファイルの脆弱性スキャンが実行されません。また、以下の情報が KSC に送信されません。
・H/W レジストリ情報
・インストール済み S/W 情報
・必要なアップデートに関する情報
・検知された脆弱性に関する情報

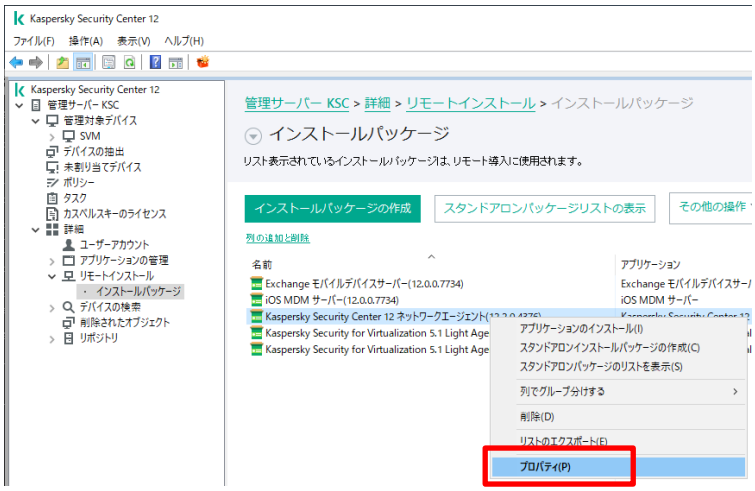
これによりゲスト OS のパフォーマンス向上が見込めます。

オンラインヘルプ
https://support.kaspersky.com/ksc/12/ja-JP/92480.htm

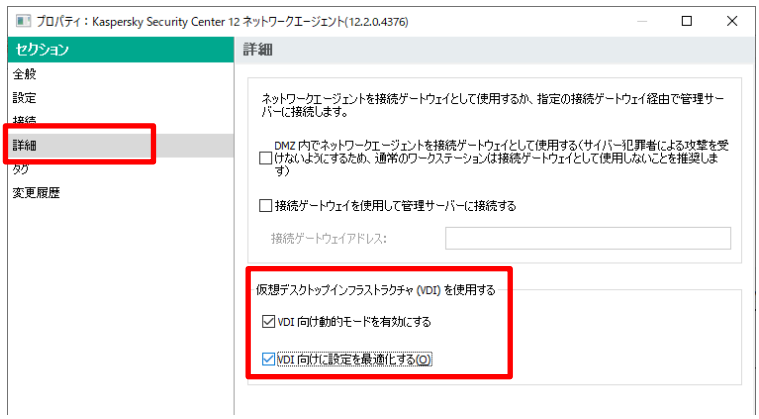
このため、各オプションは導入する環境や要件等からチェックを入れる/入れない、を判断ください。

本資料ではマスターイメージ用ゲスト OS にインストールすること、およびパフォーマンス向上を目的とすることを想定し、処理を進めています。

1. KSC の GUI を起動し、左側の項目から「詳細」→「リモートインストール」→「インストールパッケージ」を選択します。
右側の画面に KSC に登録されているインストールパッケージの一覧が表示されるので、その中から「Kaspersky Security Center 12 ネットワークエージェント」を右クリックし、メニューの中から「プロパティ」を選択します。



2. プロパティ画面、左側の項目から「詳細」を選択し、右側の画面下部にある”仮想デスクトップインフラストラクチャを使用する”内にある各項目のチェックボックスにチェックを入れます。
最後に「OK」をクリックし編集を終えます。



以上で、ネットワークエージェントの編集は終了です。
続いてゲスト OS へのインストールの際に利用するスタンドアロンインストールパッケージを作成します。

kaspersky

7. スタンドアロンインストールパッケージの作成

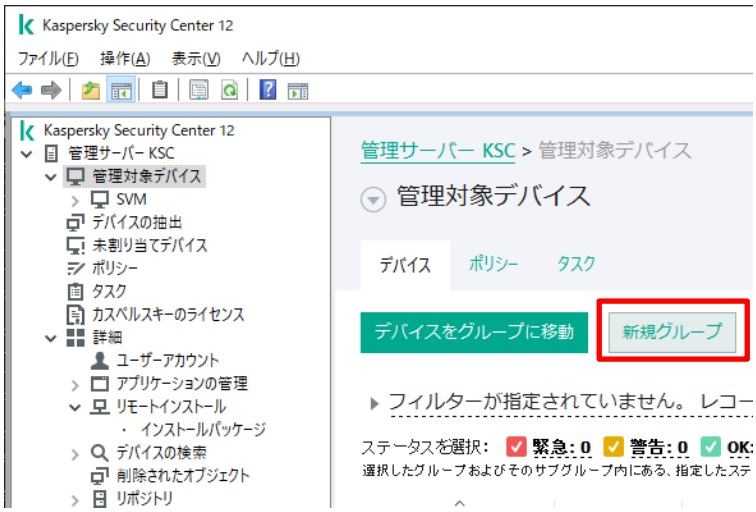
次にマスターイメージ用のゲスト OS へのインストールに利用するスタンドアロンインストールパッケージ作成します。このインストーラは先に編集したネットワークエージェントとマルウェア対策機能部分を 1 つにまとめたインストーラです。

なお本資料は VDI のマスターイメージにインストールすることを想定しています。

(マスターイメージ用に編集したネットワークエージェントを利用するため)

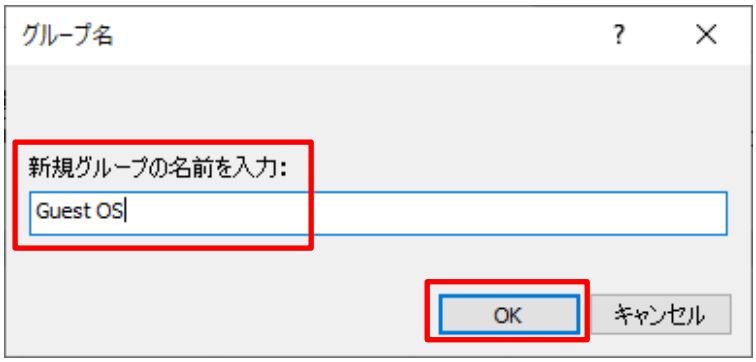
1. はじめにゲスト OS 用のグループを作成します。

   「新規グループ」をクリックします。



2. グループ名を入力する画面が表示されるので適切な名前を入力し、「OK」をクリックします。

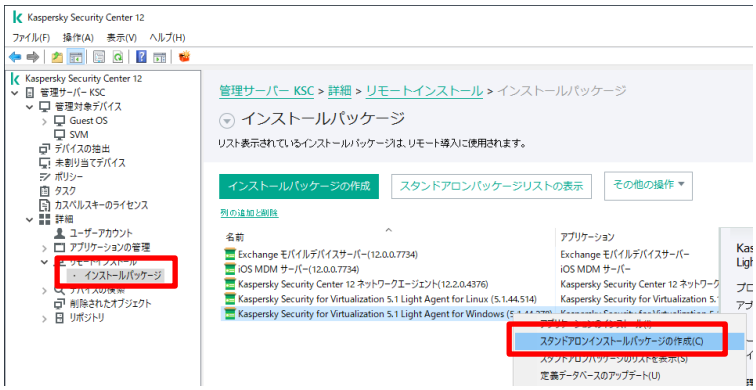
   本資料では”Guest OS”として処理を進めます。



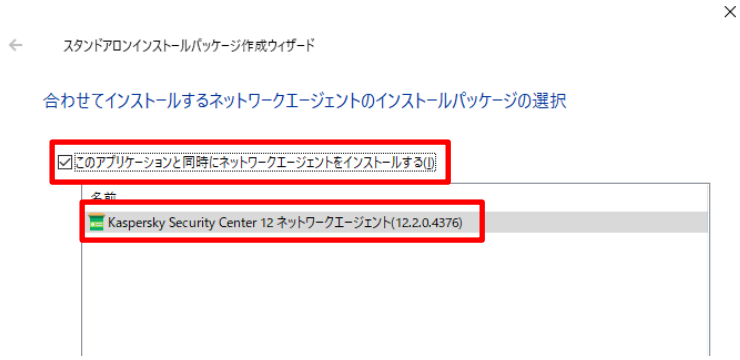
3. グループが作成されたことが確認できます。

   このグループにクローニングされたゲスト OS が自動的に配置されます。
   また電源を切ったゲスト OS は自動的に削除されます。

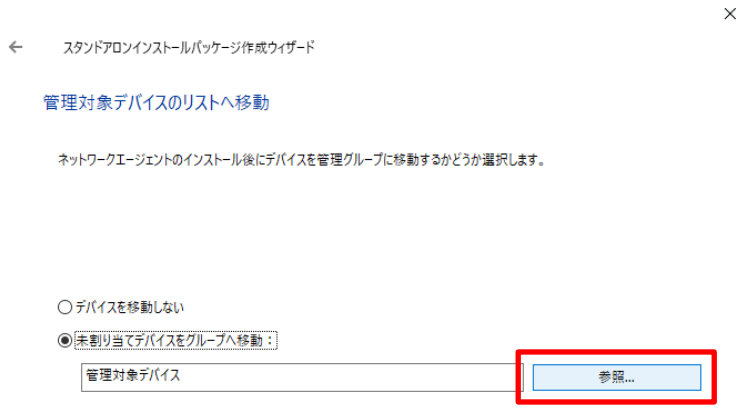
4. 続いてスタンドアロンインストールパッケージを作成します。
左側の項目から「詳細」→「リモートインストール」→「インストールパッケージ」を選択します。
インストールパッケージの一覧の中から「Kaspersky Security for Virtualization 5.1 Light Agent for Windows」を右クリックし、メニューの中から「スタンドアロンインストールパッケージの作成」を選択します。



5. “合わせてインストールするネットワークエージェントのインストールパッケージの選択”画面ではチェックボックスにチェックが入っていることを確認し、「次へ」をクリックします。

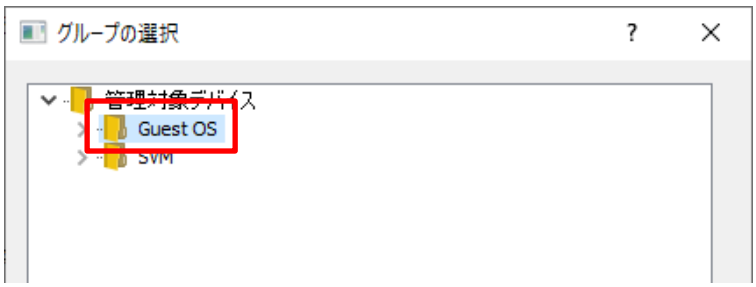


6. “管理対象デバイスのリストへの移動”画面が表示されます。
ここではインストール後の端末を自動的に指定したグループへ移動する設定が行えます。
「参照」をクリックします。

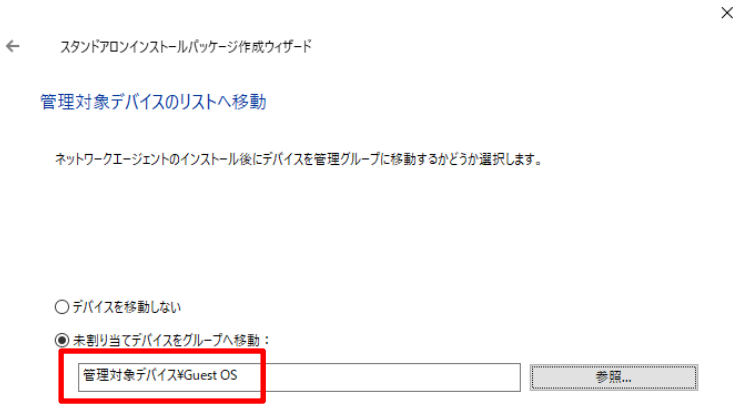


7. “グループの選択”が表示されます。
ツリーを展開し、先ほど作成したグループを選択します。

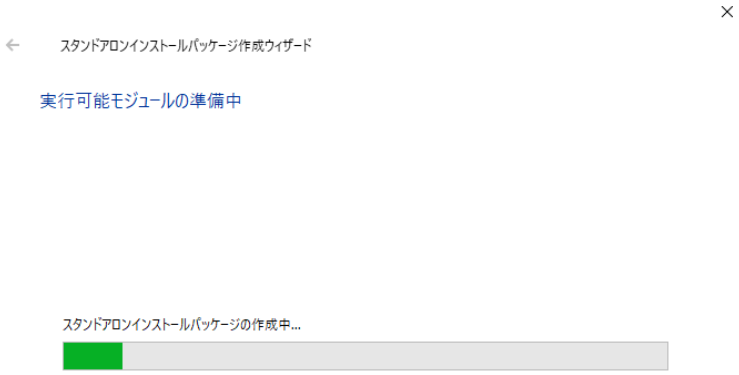
本資料では”Gest OS”グループを選択し、処理を進めます。



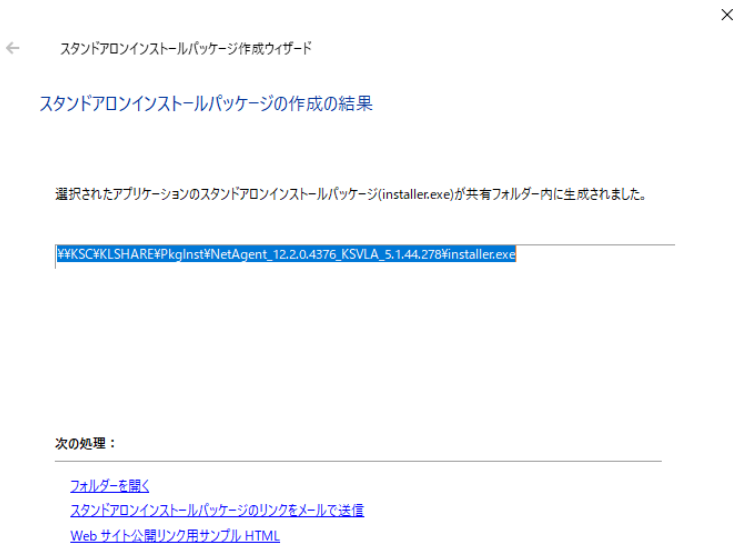
8. 画面が戻るので、画面内の”未割り当てデバイスをグループへ移動”のところが先ほど指定したグループになっていることを確認し、「次へ」をクリックします。



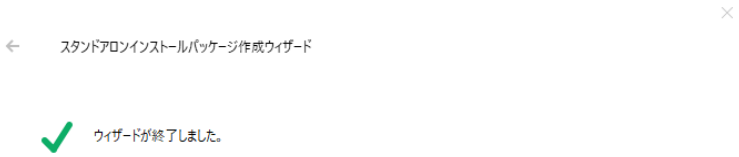
9. 作成完了まで少々お待ちください。



10. 作成結果画面が表示されるので「次へ」をクリックします。

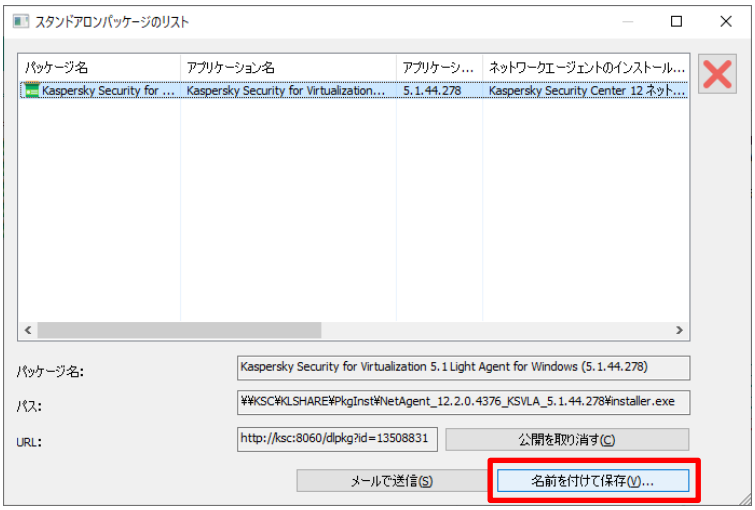


11. ウィザード終了画面が表示されるので「完了」をクリックして終了します。



12. KSC の GUI に戻るので右側の画面内にある「スタンドアロンパッケージリストの表示」をクリックします。

13. 先ほど作成したスタンドアロンインストールパッケージが表示されるので、選択後、画面下部にある「名前を付けて保存」をクリックします。



14. エクスプローラが開くので適切な場所、適切な名前を付けて「保存」をクリックします。

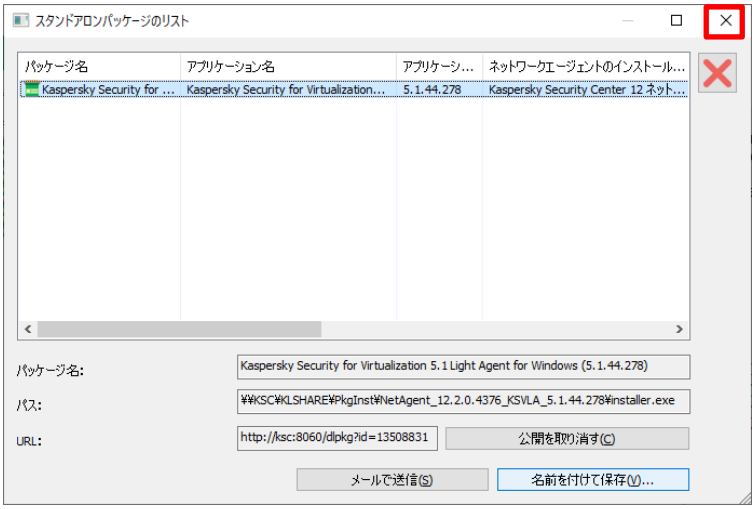
本資料ではデスクトップに「VDI 用インストーラ」と名前を付けて保存しています。

15. インストーラの保存後、リスト画面は右端上にある×ボタンで閉じてください。

*****注意*****

赤い×ボタンは絶対にクリックしないでください。

移動ルールが削除されてしまい、ゲスト OS のグループへの自動移動が行われなくなります。



16. 保存先に指定した場所に設定したファイル名でインストーラが格納されています。
あとはこのインストーラをマスターイメージとなるゲスト OS にインストールします。

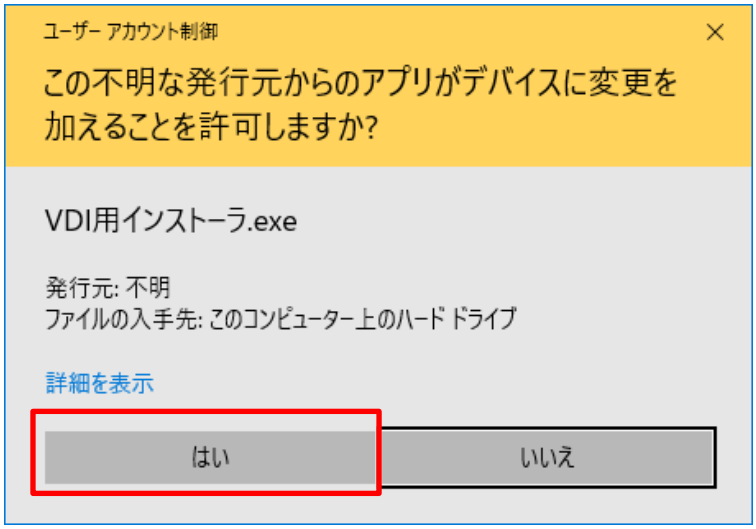
以上で、スタンドアロンインストールパッケージの作成は終了です。

8. ゲスト OS へのインストール

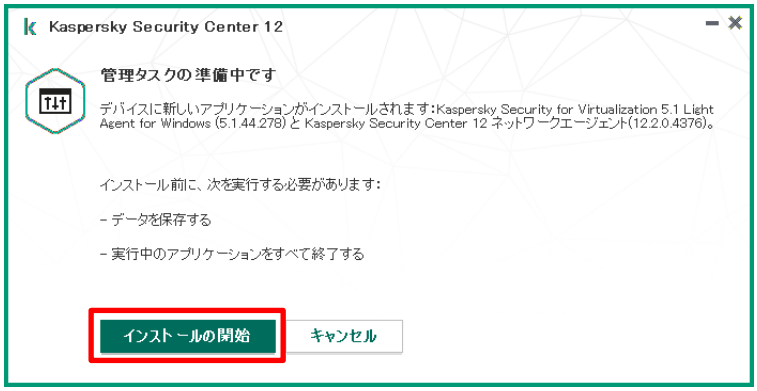
次にマスターイメージとなるゲスト OS へ先ほど作成したスタンドアロンインストールパッケージを使ってインストールを行います。

1. 作成したスタンドアロンインストールパッケージをゲスト OS に複製し、実行します。

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」をクリックし、処理を進めます。



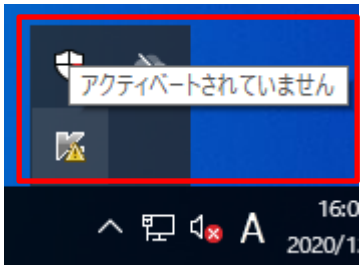
3. インストーラ画面が表示されるので、「インストールの開始」をクリックします。



4. インストールが完了するまで少々お待ちください。

5. インストール完了画面が表示されたら「OK」をクリックし、終了します。

6. インストールが完了するとタスクバーにアイコンが表示されます。
ただし保護機能は停止した状態になります(アイコンがグレーアウトしている)
これはエラーではなく、マスターイメージ用に作成したインストーラの設定が原因です。



7. 右図はその状態で GUI を起動した画面です。
KSC や SVM と通信ができない状態のため、アクティベーションや定義ファイルの更新を含め、一切の機能が停止しています。

このようになるのは前述したとおり、使用したインストーラの設定で「動的モードを有効にする」を有効にした結果です。

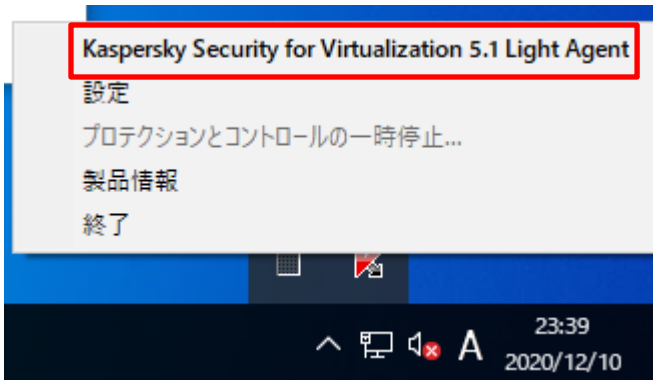
この状態で問題ないので、マスターイメージの電源を切り、クローニングを行ってください。

以上でマスターイメージへのインストールは終了です。

9. 動作確認

クローニングが完了したゲスト OS で KSVLA for Windows の動作を確認します。

1. タスクバーにアイコンが表示されます。
   For Windows の GUI を起動するには
   アイコンを右クリックし、メニューの中から
   「Kaspersky Security for Virtual-
   ization 5.1 Light Agent」を クリックし
   ます。



2. 右図はすべての機能が正常に稼働してい
   る状態です。

   KSC 配下に入り、各機能が稼働している
   ことがわかります。

3. 右図は eicar を検知させた結果です。

以上で動作確認は終了です。

終わりに

以上で KSVLA を利用した Hyper-V 上に構築したゲスト OS の保護については終了です。

本資料では Hyper-V サービスを提供するホスト OS 自身(Parent OS)のマルウェア対策のインストールは実施していません。このため、別途何らかのカスペルスキー製品を利用してマルウェア対策を行ってください。

2020/12 月現在、Windows サーバーOS 専用のマルウェア対策製品として利用いただける製品は以下です。

・Kaspersky Security for Windows Server
https://www.kaspersky.co.jp/small-to-medium-business-security/windows-server-security

ライセンス等を含め、何かご不明点がございましたら弊社までお問い合わせください。

kaspersky

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

www.kaspersky.co.jp | kasperskylabs.jp/biz/