2019 年 12 月 27 日

第 1.0 版

トレンドマイクロ株式会社
セールスエンジニアリング部

VMware NSX-T Data Center & Trend Micro Deep Security インテグレーションガイド

～エージェントレスセキュリティとマイクロセグメンテーション～

[VMware NSX-T Data Center 2.4/2.5.0 + Deep Security Virtual Appliance 12.0 対応]

改定履歴

Revision No.	Date	Change	Author
1.0	2019/12/27	初版作成	Trend Micro

目次

はじめに

本ガイドについて

本ガイドは、VMware NSX-T Data Center 環境にて、エージェントレスによるセキュリティ保護を目的として Trend Micro Deep Security 12.0 を導入する際のトレンドマイクロが推奨する構成、設定手順および関連情報を取りまとめたものです。
また、特に関連性の深い VMware NSX Manager、Guest Introspection Service、分散ファイアウォールについての仕組み、構築にあたって知っておくほうがよいと思われる事項についても記載しています。
（VMware NSX-T Data Center を前提として記載をしており、VMware NSX for vSphere については本ガイドでは触れておりません。）

なお、本ガイドに記載されている内容については、あくまで弊社での実績を元に指標となる内容をまとめて記載をしています。実環境における性能、動作を必ずしも保証するものではありません。また、お客様環境、要件によっては弊社エンジニアおよびサポート担当より異なる設定、推奨内容の提案、提示がされる場合があります。

用語について

本ガイドでは、特別に必要な場合を除いて、下記の略称を使用します。
「Trend Micro Deep Security」→「DS」
「Deep Security Manager」→「DSM」
「Deep Security Agent」→「DSA」
「Deep Security Relay」→「DSR」
「Deep Security Virtual Appliance」→「DSVA」
「VMware vSphere」→「vSphere」
「VMware vCenter Server」→「vCenter Server」
「VMware ESXi」→「ESXi」
「VMware NSX-T Data Center」→NSX-T

本ガイドの作成時の検証バージョン

VMware vSphere 6.7.0
VMware NSX-T Data Center 2.4.2 （一部 2.5 に添った記載を追記）
Deep Security 12.0

1. Deep Security と VMware NSX について

1.1. Deep Security と VMware NSX 連携ソリューション

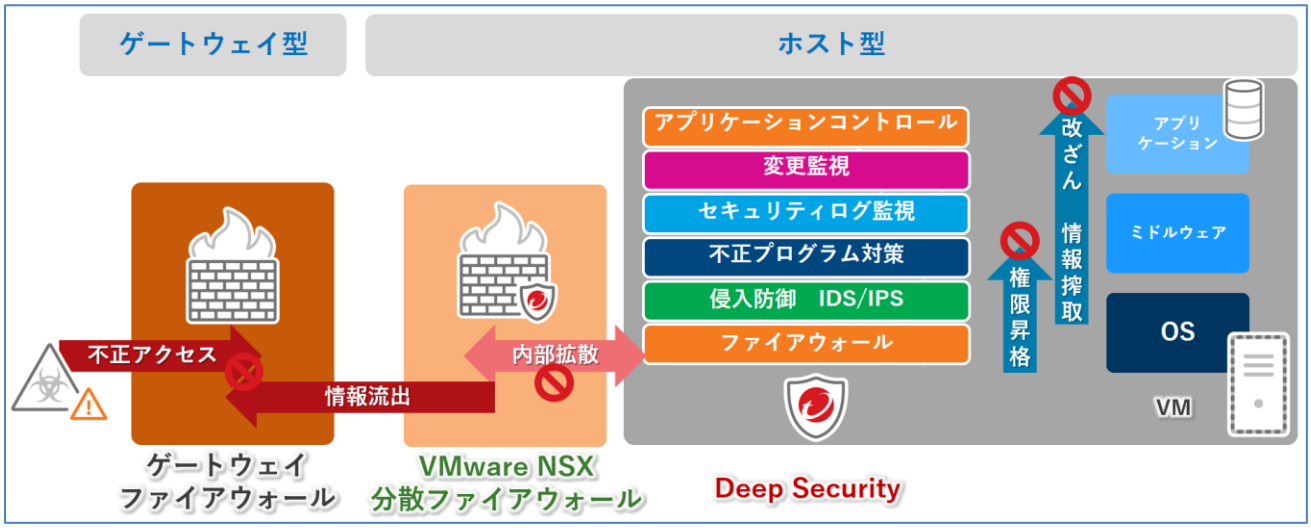
1-1-1. Deep Security と VMware NSX の連携メリット

Deep Security と VMware NSX を組み合わせて導入することにより、サーバ・ネットワークの仮想化により効率化されたプラットフォーム環境に対して、運用性を担保しながら必要なセキュリティを柔軟に提供することが可能となります。

特に VMware Horizon などで仮想マシンが展開される仮想デスクトップ環境では、エージェントレスでのセキュリティ実装と多くの仮想マシンに対する均一なセキュリティサービスを提供できます。

Deep Security と VMware NSX の連携によるメリットは以下のとおりです。

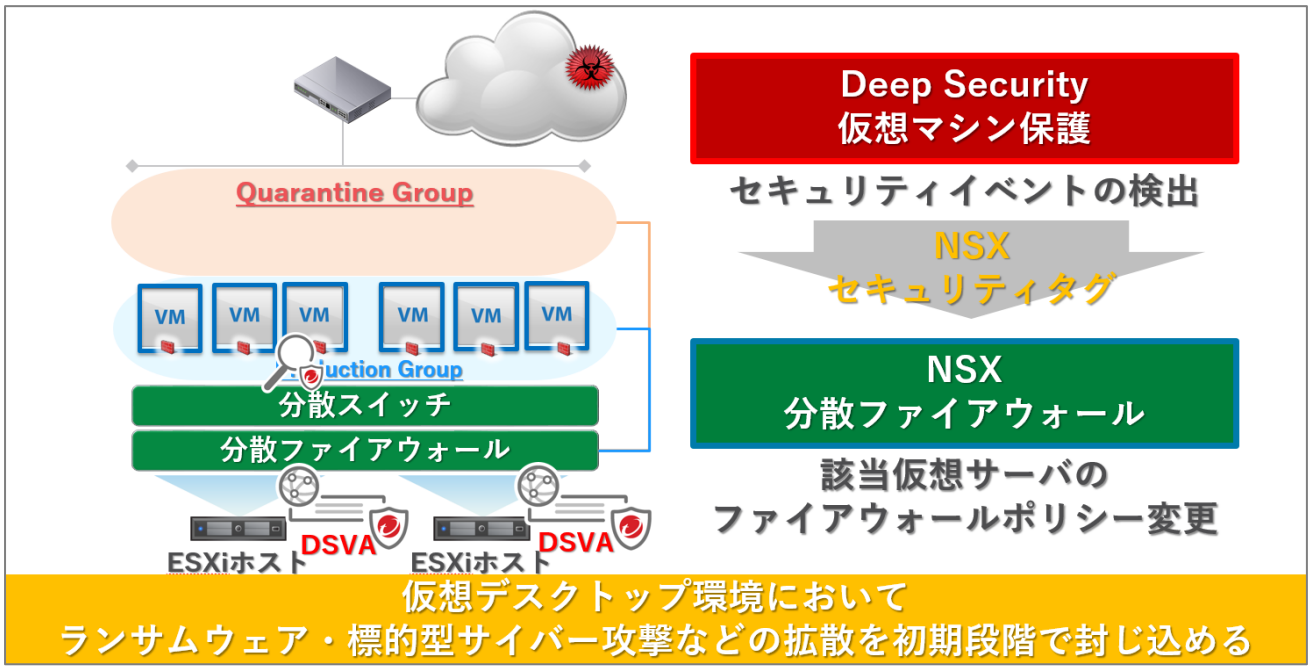
- VMware NSX の分散ファイアウォールによる仮想マシン毎にきめ細やかなアクセス制御の実現
- Deep Security による仮想マシンの要塞化の実現



- 仮想マシンにエージェントを導入しないエージェントレス型の採用によるセキュリティレベルの統一とユーザにとってストレスフリーな利便性の両立
- vCenter Server と Deep Security Manager のインベントリ情報の同期によって、仮想環境のリソース変化による仮想マシンのホスト間移動へのシームレスなセキュリティ適用の継続とセキュリティ機能の実装状況の可視化
- Deep Security のセキュリティイベント検出時に NSX セキュリティタグを付与することで、仮想マシンに適用される分散ファイアウォールの付け替えによる自動隔離を実現するとともに、一次対処の迅速化と運用負荷の軽減が可能
  （物理環境において、ウイルス検出をした際に LAN ケーブルを抜線する運用を自動化するイメージ）
- 2019 年 12 月時点では、VMware NSX-T と Deep Security のポリシー連携が不可のため、仮想マシン生成時に適切なセキュリティポリシーを自動適用する場合には、DSM でイベントベースタスクを別途設定する必要があります。

1-1-2. DSVA による仮想マシン要塞化と NSX セキュリティタグを利用した分散ファイアウォールによる自動隔離

DSM にてある仮想マシンでセキュリティイベントが検出された際に NSX セキュリティタグを付与するオプションを設定しておくことにより、Deep Security のイベントをトリガーとして該当する仮想マシンの属性（所属するセキュリティグループ）をセキュリティタグによって変更することによって、適用されるファイアウォールポリシーを変更することが可能となります。



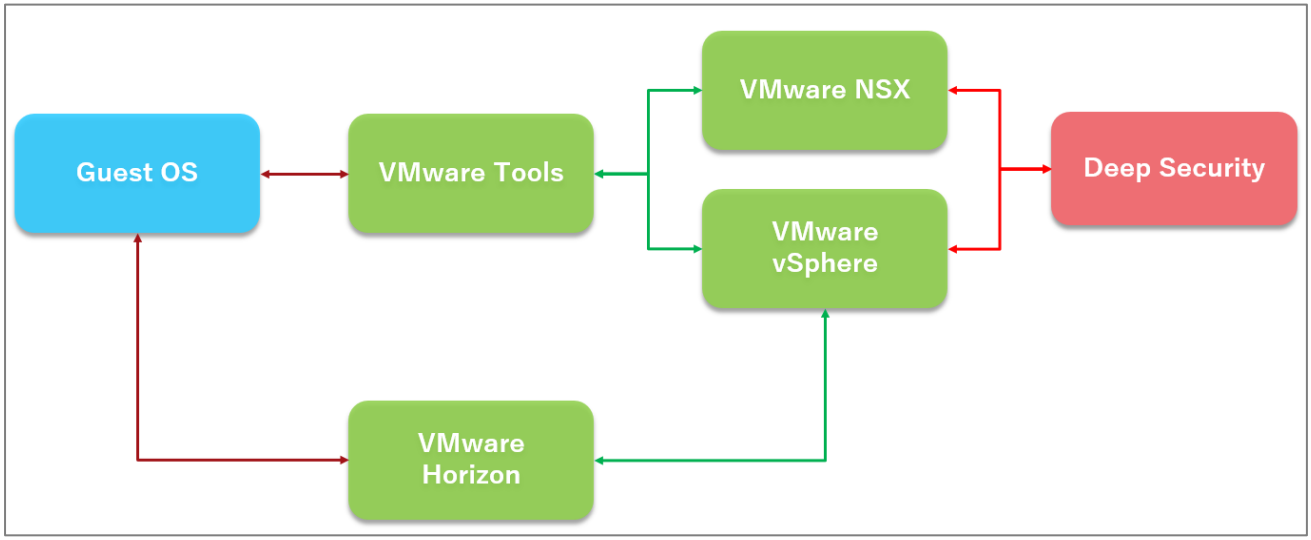
実装方法については、以下のセクションを参照してください。

2-4. セキュリティタグを利用した自動隔離の考え方と設定手順

1-2. システム要件および互換性の確認

設計及び導入を行う前にお使いの環境が DS12.0 のシステム要件、および VMware 関連ソリューションとの互換性を満たしているか確認する必要があります。

以下にソリューション間の互換性の関係性を記載します。



詳細の互換性情報については以下のページをご確認ください。

■ **DS12.0のシステム要件**

http://www.trendmicro.co.jp/jp/business/products/tmds/index.html?cm_sp=GNav-_-Business-_-tmds#requirement

※システム要件を満たしていないコンピュータでの動作検証は行っていない為、サポート対象外となります。

■ **Deep Security Virtual Appliance と VMware 製品の互換性対応表**

http://esupport.trendmicro.com/solution/ja-jp/1314170.aspx

■ **Deep Security and VMware compatibility matrix（VMware各コンポーネントの対応互換表）**

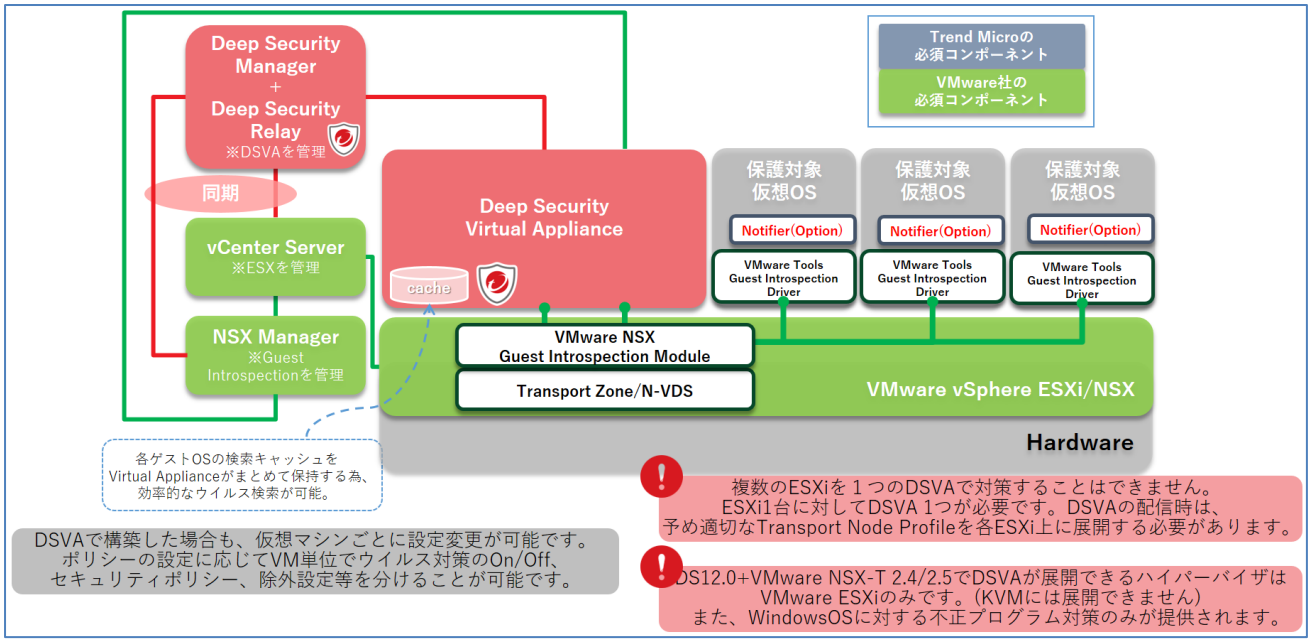
http://www.vmware.com/resources/compatibility/sim/interop_matrix.php

■ **VMware Compatibility Guide（VMware ESXiに対するDSVAを含む3rd Party製品の互換対応表）**

http://www.vmware.com/resources/compatibility/search.php

1-3. コンポーネントの概要

1-3-1. 各コンポーネントの役割



＜NSX 環境における Deep Security Virtual Appliance 基本構成＞

■ **Trend Micro Deep Security**

➢ **Deep Security Manager(DSM)**

Deep Security Manager(DSM)は、Web ベースの強力な中央管理システムです。DSM は、データベースを使用しており、セキュリティ管理者が実行する包括的なセキュリティポリシーの作成や管理、記録(ログ)を集中的に管理します。また、状況を把握するためのダッシュボードやレポートの作成、サーバに対するタスクを作成するなど、Deep Security におけるすべての管理処理を実行します。なお、データベースについては構成によって、DSM と同じ OS 上に構築する場合と、DSM 用のデータベースを別 OS 上で構築する場合があります。

➢ **Deep Security Agent(DSA)**

Deep Security Agent(DSA)は、最小限のリソースで最大限のセキュリティ保護を提供するソフトウェアで、仮想マシンの OS 上に直接インストールされ動作することで、Deep Security で提供されるほぼすべてのセキュリティ保護機能を一括で提供できます。また、DSA をリレー化することによって DSR として機能させることも可能です。

➢ **Deep Security Virtual Appliance(DSVA)**

Deep Security Virtual Appliance(DSVA)は、仮想化環境で実行されるセキュリティコンポーネントです。Agent が直接仮想マシンの OS 上にインストールされるのに対して、DSVA は VMware NSX と連携し、VMware ESXi 上で実行される仮想アプライアンスとして動作し、ESXi ホスト上の他の仮想マシンの OS 上にセキュリティソフトウェアをインストールすること無く、エージェントレスによる Deep Security のセキュリティ機能を提供することができます。

➢ **Deep Security Relay(DSR)**

Deep Security は新たな脅威に対応するため、Deep Security ソフトウェアやウイルスパターンファイル、侵入防御シグネチャなどを日々アップデートする必要があります。Deep Security システムにおいて、コンポーネントのアップデートを実行するのが Deep Security Relay(DSR)です。DSR はインターネット上から最新コンポーネントをダウンロードし、DSA および DSVA に配信します。そのため、DSR はシステム全体で最低 1 台は必要となります。

DSR は DSA の一機能として該当の DSA をインストールされたコンピュータを Relay Group に所属させることにより Relay 機能を有効化します。通常は DSM と DSR を同居させてください。また、DSVA 環境では仮想マシンに対する一部の設定情報を DSR 同士でやりとりする場合があります。複数の Relay Group を作成する場合には、DSVA の配信するホストの範囲と DSR の Relay Group が合致するように設定するようにしてください。

➢ **Notifier**

DSVA で保護されている仮想マシン(Windows)内で動作します。Notifier をインストールしていると不正プログラムをブロックしたとき、または不正な Web ページにアクセスしたときなどに、ユーザにポップアップ通知が表示されます。Notifier がクライアントマシン上で占有するスペースは小さく、必要なディスク容量は 1MB 未満、メモリサイズは 1MB 未満です。

➢ **Smart Protection Server(SPS:オプション)**

Smart Protection Server(SPS)は、Web レピュテーションおよびファイルレピュテーションのデータベースをローカルに保持するための仮想アプライアンスです。SPS は社内ネットワークに構築され、トレンドマイクロ

がクラウド提供している Smart Protection Network（SPN）と連携します。DSA や DSVA は SPS を参照して Web レピュテーションおよびファイルレピュテーションの機能を提供します。

■ **VMware**

➢ **ESXi（ハイパーバイザ）**

ESXi は ハイパーバイザ型仮想化ソフトウェアのことであり、ホスト OS の代わりにハードウェア上で直接動作し、ESXi 上でゲスト OS を複数台動作させることが可能です。NSX-T 環境では ESXi ホストは Transport Node の 1 つとして管理されます。

➢ **vCenter Server**

vSphere 環境において、各 ESXi ホスト、仮想マシンの管理、機能の有効化・リソース監視などの統合管理を実現します。管理者は vCenter から、ESXi や仮想マシンの状態をリアルタイムに確認し、仮想マシンのデプロイやスマップショットの取得、バックアップ等も実行することができます。NSX-T 環境で Deep Security を展開する場合には、予め NSX Manager から vCenter Server をコンピュートマネージャとして登録しておく必要があります。

➢ **NSX Manager**

NSX Manager はすべての NSX コンポーネントの管理を実施する管理サーバとして動作します。DSVA の展開に必要となる Transport Node Profile（N－VDS）の ESXi への展開、セキュリティポリシーの作成、DSVA の展開を NSX Manager から行います。また、NSX Manager は本番環境では 3 台をクラスタとして展開することが必要となります。

➢ **Guest Introspection Service**

Deep Security などサードパーティ連携機能を使用する場合に各 ESXi ホストに配信される分散型のサービスモジュールです。エージェントレスにて主に不正プログラム対策などを行う際に各仮想 OS から DSVA へ検索対象などの情報をオフロードする際にハイパーバイザ間のやりとりを許可するためのコネクション管理機能を担います。

➢ **VMware Tools VMCI ドライバ － NSX ファイル自己検証ドライバ**

エージェントレスで仮想マシンの不正プログラム対策などを行う際に保護対象の仮想マシンにこのドライバをインストールすることで、仮想マシンで検出されるファイルへのアクセス情報を ESXi 経由で DSVA へ連携します。（VMware Tools の VMCI ドライバとして統合されています。）

ファイアウォール、侵入防御、Web レピュテーション機能を利用する場合には直接このコンポーネントは利用されません。

VMware Tools についても vSphere/NSX とのバージョン依存があるため、互換性の確認を必ず行う必要があります。

➢ **NSX 分散スイッチ（N-VDS）**

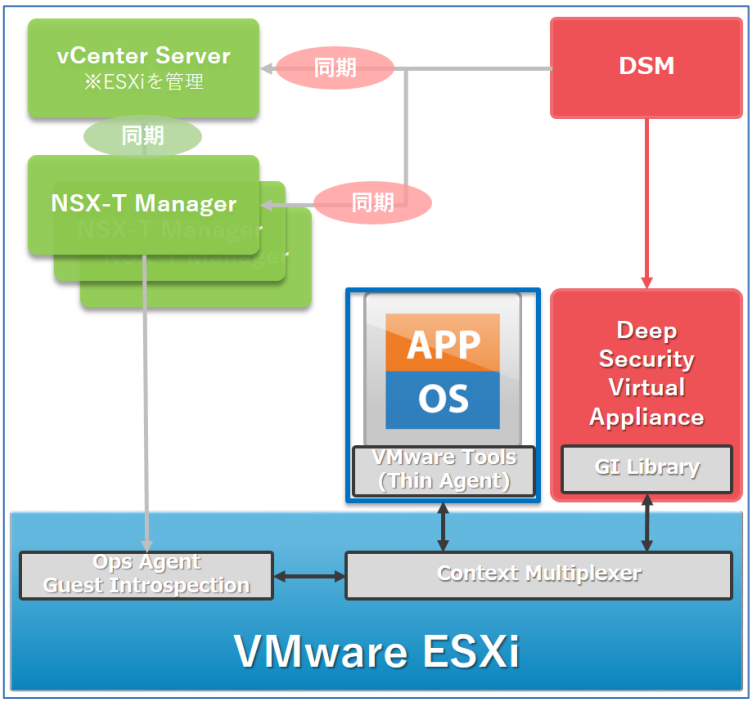
複数の ESXi ホストをまたがって構成する NSX 仮想スイッチで、Transport Node でスイッチング機能を実行する NSX ソフトウェアコンポーネントです。

N-VDS は vCenter Server 上で仮想スイッチとして生成されますが、vSphere 環境で生成される標準仮想スイッチ（vSS）、分散仮想スイッチ（vDS）とは異なる属性を持ち、vCenter Server からは設定変更などを行うことができません。また、vSS または vDS から N-VDS へ移行することはできず、独立管理されています。

DSVA を配信は必ず N-VDS が展開された Transport Node に対して行う必要があります。

1-3-2. コンポーネント間の関係性

- vCenter Server と NSX Manager は 1:1 で対応させる必要があります。
- DSM（データベースインスタンス単位）は、該当クラスタの ESXi ホストと仮想マシンのインベントリ情報やセッション情報を管理するために vCenter Server、NSX Manager が 1:1 で同期する必要があります。
- 保護対象の仮想マシンが配置される各 ESXi ホストに対して、Guest Introspection、DSVA をそれぞれ配信する必要があります。



＜NSX・Deep Security コンポーネントの関係性＞

コンポーネント間の関係性からも分かるとおり、DSVA を利用したエージェントレス型セキュリティ対策は NSX との連携がキーとなっており、仮想デスクトップの展開方式には依存していません。
Horizon によるフルクローン、リンククローン、インスタントクローンに関わらず適用することが可能です。
（展開方式によって仮想マシンの展開スピードが異なるため、サイジング、チューニングが必要になります。）

1-3-3. Deep Security 管理コンポーネントの構成と配置

Deep Security を機能させるためには、必ず DSM、DSR を配置する必要があります。NSX 環境において DSVA を展開する際の標準的な構成と配置について以下に解説します。

■ **Deep Security Manager（DSM）**

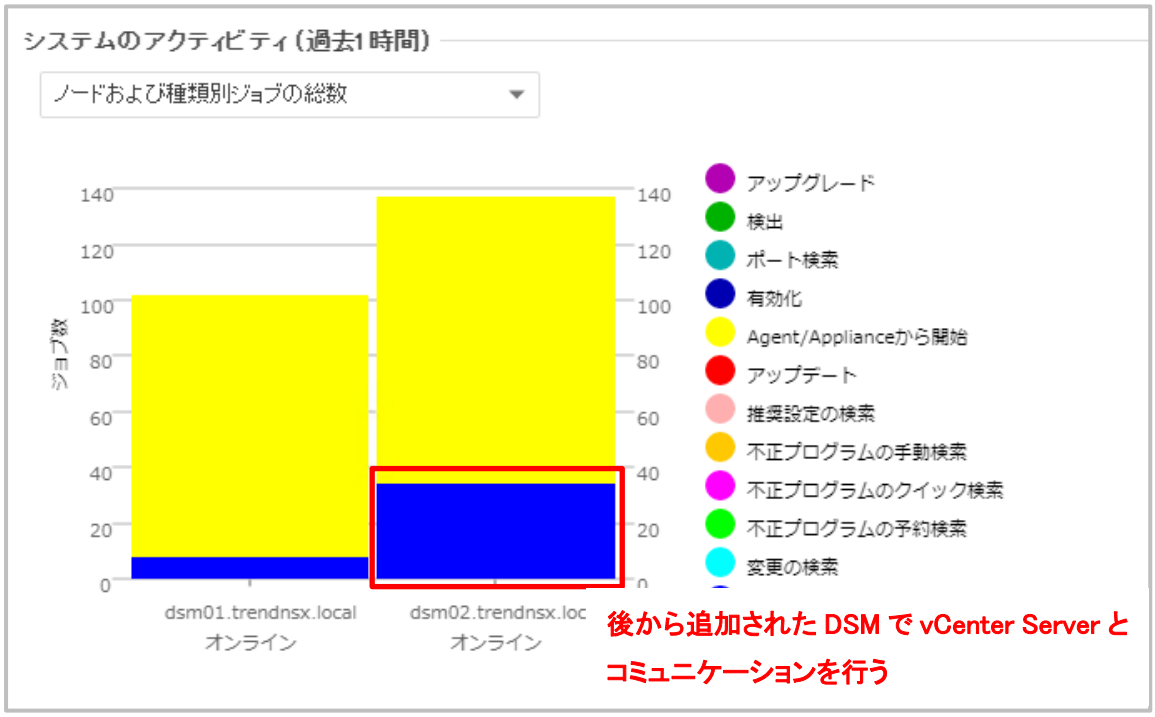
DSM が管理するセキュリティポリシー、インベントリ情報、イベント情報などすべての情報はデータベースに格納されます。DSM ソフトウェアパッケージにはデータベースは含まれておらず、事前に Microsoft SQL、Oracle または PostgreSQL のデータベースを準備しておく必要があります。データベースは DSM をインストールするサーバに同居させることも可能ですが、VDI 環境など一定規模以上での展開を行う場合、DSM を 2 台構成以上で接続する場合には、データベースは別サーバで構築することを推奨します。

NSX 環境において、DSM を複数ノードで構成する場合、以下の点を留意して設計してください。

DSM を 2 台以上で構成する場合には、各 DSM からデータベースサーバに対して同一インスタンスへ接続させることで同一の情報を参照することで、DSM の負荷分散、冗長性の担保がされます（データベースの冗長化は別途検討する必要があります）。

➢ **複数 DSM ノードと vCenter Server の同期**

最後にデータベース接続された DSM が vCenter Server との同期処理を実行します（設定による変更は不可）。

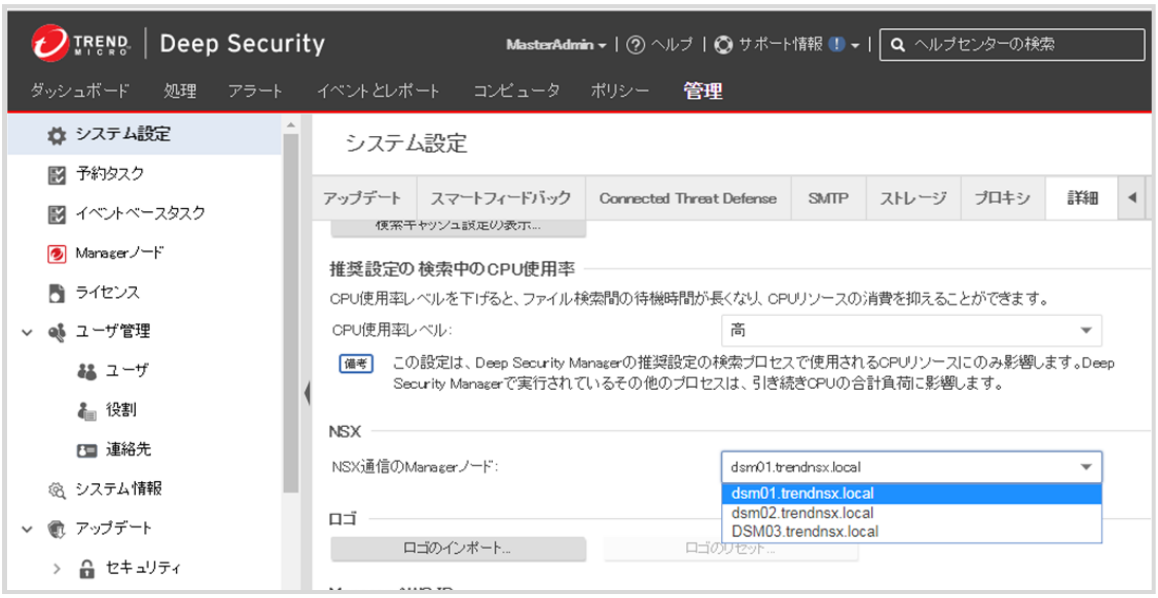


＜複数 DSM ノード構成時の vCenter Server とのコネクション＞

- **複数 DSM ノードと NSX Manager の同期**

  デフォルトでは最初にデータベース接続された DSM は、NSX Manager とのコネクション処理を行うとともに、NSX Manager 経由で vCenter Server から DSVA を配信する際に DSVA の ovf ファイルの格納先としても指定されます。NSX Manager との同期する DSM は、以下の設定で変更可能です。

  [管理]＞[システム設定]＞[詳細]＞[NSX 通信の Manager ノード]



＜複数 DSM ノード構成時の NSX Manager と同期する DSM の設定＞

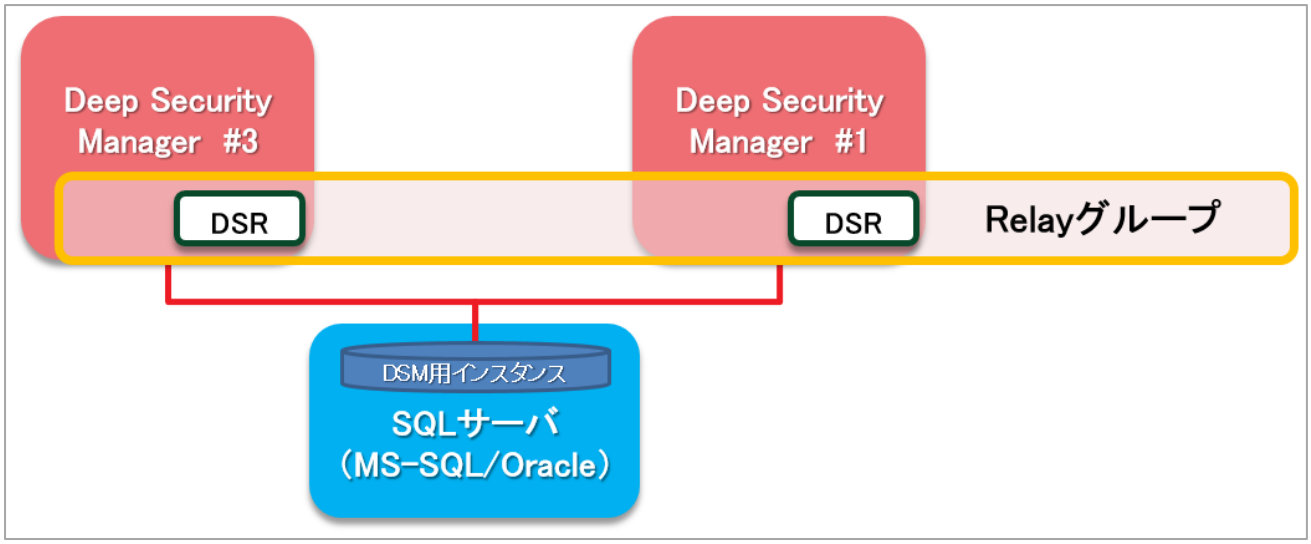
■ **Deep Security Relay（DSR）**

DSR については、通常 DSM と同一サーバに同居するケースが一般的です。構成にあたっては以下の点に留意して設計してください。

- インターネットへの接続性の確保

  →SPN からのパターンファイル、ルール（DSRU）のダウンロード

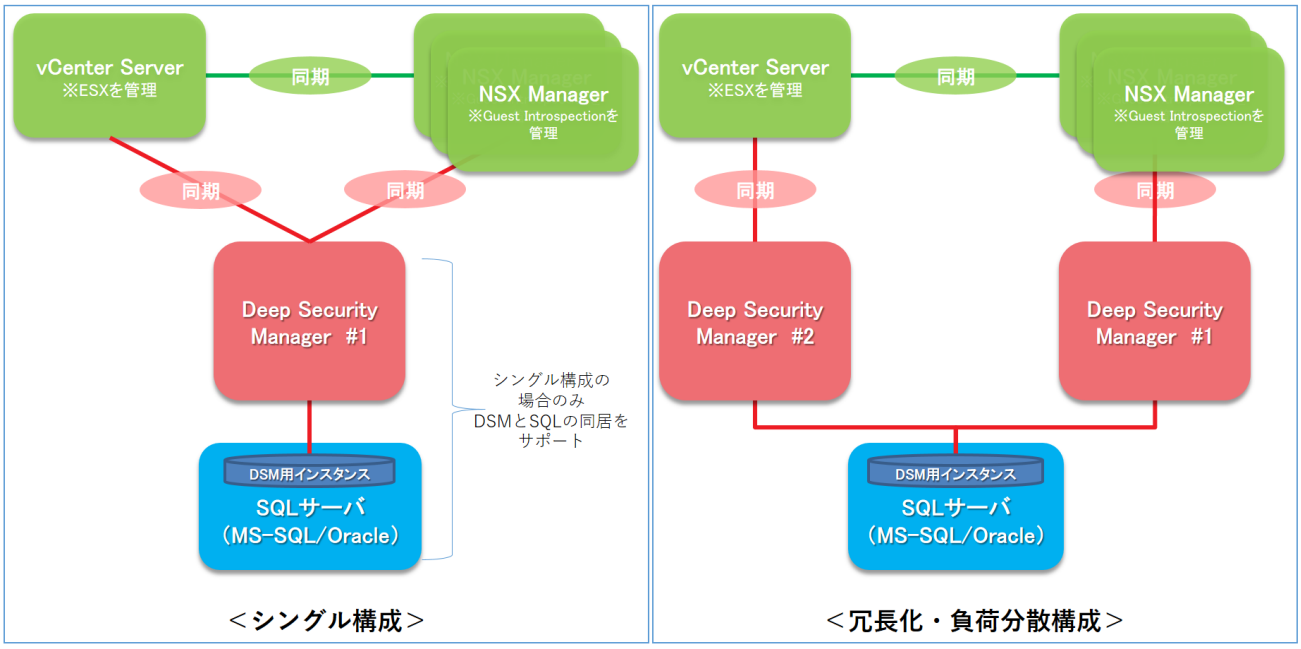
- 通常のパターンやコンポーネントのダウンロード機能に加え、vMotion/DRS 実行時に移動する仮想マシンのポリシーを DSVA 間で移行する際にも利用されます。そのため、VDI 環境などで仮想マシンの移動が多く見込まれる環境では最低でも DSM ノード数と同数（DSM ノードと同居を推奨）、またはそれ以上の DSR を配置してください。
- DSR は必ず Relay グループに所属する必要があります。Relay グループに DSR を所属させることにより、サービスを提供する DSVA（及び DSA）を規定します。通常は DSM をインストール時に生成される「初期設定の Relay グループ」を利用することで問題ありません。大規模環境な VDI 環境において VDI グループ単位で分割したい場合や DSM に同居した DSR が直接インターネットへ接続できず、SPN からのダウンロード専用に DSR を別セグメントに配置したい場合（DSR の多段構成）などに複数の Relay グループを作成することも可能です。



＜複数 DSM ノード構成と Relay グループ＞

- **DSM/vCenter Server/NSX Manager 管理マネージャ群の基本構成**

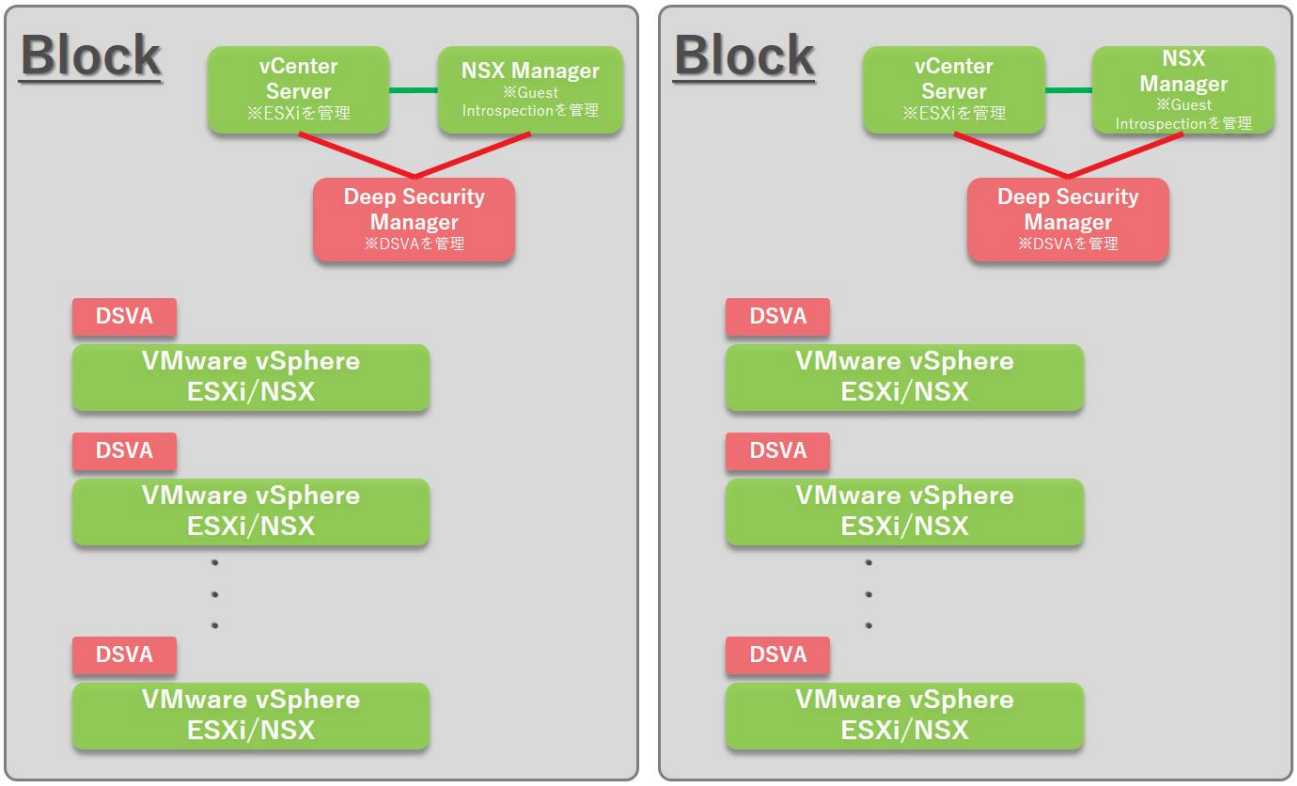
  NSX 環境で DSVA を展開する上では、DSM が vCenter Server と NSX Manager が常にリアルタイムかつ安定的にコネクションをされている必要があります。それにより、仮想マシンの生成、移行（vMotion 及び DRS など）、仮想マシン単位（NSX ではセキュリティグループ単位）でのポリシーの管理を行うことが可能となります。



＜管理マネージャ群の基本構成＞

また、上記管理マネージャ群の基本構成を踏まえて、DSVA を配信するプロダクションのクラスタ（または NSX-T における Transport Zone）を設計してください。仮想デスクトップ環境のようにフローティング方式で仮想マシンが

展開・削除が繰り返される環境の場合、または、仮想マシンの集約率が高い環境では、複数の vCenter Block を 1 セットの DSM セットで管理することは、パフォーマンス面から推奨していません。



※NSX-T 環境では、NSX Manager が複数の vCenter Server と連携（コンピュートマネージャとして登録）することで
1:N での構成を組むことが可能となりました。ただし、Deep Security 12.0 では、NSX Manager と vCenter Server が 1:N で構成された環境で DS を構成することはできません。（12.5：Feature Release で（FR）対応していますが、サポート期間が通常のメジャーリリース（Long Term Support）に比べると短くなっていますので、ご注意ください。NSX Manager と vCenter Server が 1:N で構成された環境への対応は次期メジャーリリースを予定しています。）

1-4. 構築時にチェックするべき点

1-4-1. 通信要件と時刻同期

Deep Security を導入する際には、各コンポーネント間で指定の通信が許可されている必要があります。

- **Trend Micro Deep Security コンポーネント間の通信ポート**

以下の FAQ をご参照ください。

Trend Micro Deep Security の使用通信ポート

http://esupport.trendmicro.com/solution/ja-jp/1313476.aspx

Deep Security ヘルプセンター

https://help.deepsecurity.trendmicro.com/ja-jp/Manage-Components/ports.html

- **Trend Micro Deep Security と VMware コンポーネント間の使用通信ポート**

  DSM から vCenter Server、NSX Manager に対しては TCP443 でアクセスできることが必要となります。また、NSX 環境では、各 ESXi ホストへの Guest Introspection Service コネクションをハンドルする Multiplxer に紐づく Kernel Module と DSVA のコネクションは ESXi ホスト上に内部コネクション用の仮想スイッチ（vmservice-vswitch）を通して行われます。vmservice-vswitch は自動的に生成されます。この仮想スイッチのポートグループ、IP アドレス、ポート番号は手動で変更する必要はありません。

＜vmwervice-vswitch イメージ図＞

- **名前解決**

  Deep Security を利用する環境においては、コンポーネント間の通信において名前解決が可能な設計を行う必要があります。また、ローカル環境での名前解決をスムーズに行えるようにするため、DNS サフィックスにローカルドメインを規定しておくことを推奨します。

- **ハートビート**

  DSM と DSVA/DSA の間ではステータス管理のため、10 分毎（デフォルト：最短 1 分に変更可能）にハートビート通信を行っています。DSM⇔DSVA 間のハートビートは双方向通信（デフォルト）が必須となりますので、ハートビートの通信方向の変更を行わないようにしてください。

- **時刻同期**

  Deep Security の環境構築においては、システム間の連携が重要となること、イベントログの正確な取得のためにシステム全体を NTP による時刻同期を計ることが重要です。また、Deep Security Manager の OS のシステム時間は、データベースコンピュータの時間と同期している必要があります。コンピュータの時間がデータベースの時間と 30 秒以上前後すると、Manager 管理コンソールの［アラートステータス］ウィジェットにこのアラートが表示されます。NTP の設定においては、タイムゾーンが一致するように同一の NTP ソースを指定するようにしてください。

1-4-2. DSM を vCenter Server/NSX Manager と同期する際に必要な権限

- **DSM を vCenter Server と同期する際にユーザが必要とする権限**

  以下の FAQ をご参照ください。

  vCenter Server との同期に使用するユーザに必要な権限

  http://esupport.trendmicro.com/solution/ja-JP/1313306.aspx?print=true

- **DSM を NSX Manager と同期する際にユーザが必要とする権限**

  Enterprise Administrator ロールの割り当てが必要です。(NSX Administrator ロール以下の権限では同期はできません。)

1-4-3. NSX ライセンスと Deep Security のセキュリティ機能

DSVA によるエージェントレスでのセキュリティ機能の提供を行う場合には、VMware NSX のコンポーネントと連携をする必要があります。NSX のライセンスによって DSVA で提供することができるセキュリティ機能が異なりますので、留意が必要です。

NSXライセンス	不正プログラム対策	変更監視	DSポリシー連携	セキュリティタグ NSXと連携した自動隔離機能	侵入防御ファイアウォール	Web レピュテーション	セキュリティログ監視	アプリケーションコントロール
Standard Professional	×	△ ※1	△ ※2	×	△ ※1	△ ※1	△ ※1	△ ※1
Advanced Enterprise plus	○	△ ※1	△ ※2	◎	△ ※1	△ ※1	△ ※1	△ ※1

記号	対応状況
◎	対応可能。
○	Windows OS に対して、Deep Security Virtual Appliance (=DSVA) と Deep Security Agent (=DSA) 双方で利用可能。Linux OS に対しては、DSA のみ対応可能。
△※1	DSAで利用可能。
△※2	イベントベースタスクで仮想マシン生成時の有効化、ポリシー適用を代替可能。
×	対応不可。

NSX-T 2.4 及び 2.5.0 と Deep Secuiry 12.0 において実現できるエージェントセキュリティ機能は以下の通りです。

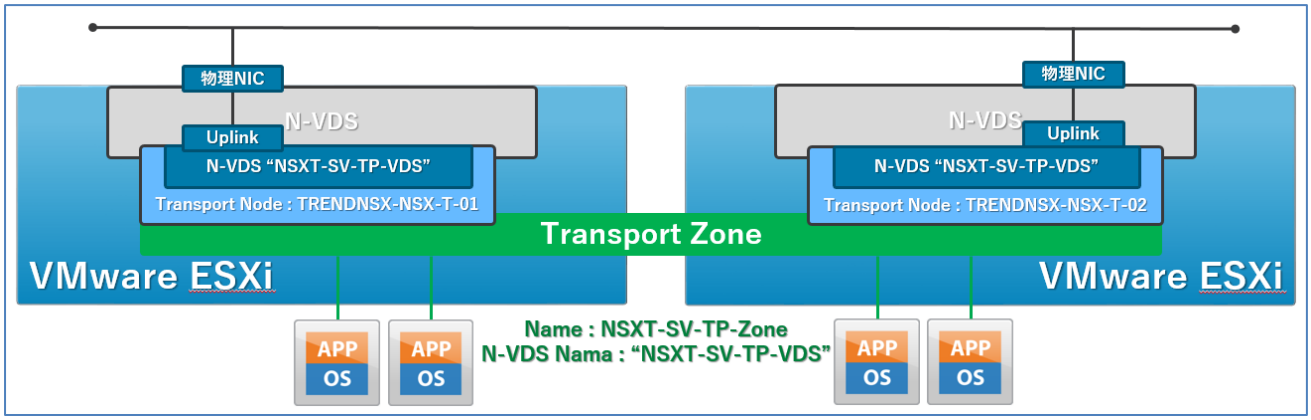
- NSX-T Manager & vCenter Server 連携による仮想マシン情報の取得
- VMware ESXi に対して NSX-T を展開することで DSVA によるエージェントレス型不正プログラム対策を提供 ※Windows OS のみ
- 不正プログラム対策イベント検出時の NSX-T Manager への NSX セキュリティタグの付与

1-4-4. NSX-T 環境における DSVA 展開の前提条件と把握しておくべき事項

NSX-T を展開した ESXi に対して DSVA によるエージェントレス型セキュリティ保護を提供するためには事前に NSX Transport Node Profile を適用しておく必要があります。

- DSVA が展開できる NSX-T 環境は、VMware ESXi のみ(KVM は現時点では対応不可)
- DSVA によるエージェントレスセキュリティを展開するためには、保護対象仮想マシンを NSX-T で指定する Transport Zone で指定された Overlay または VLAN ネットワークに配置

- ESXi ホストでは Transport Node Profile をベースにホスト上へ N-VDS(NSX 仮想スイッチ)を生成、Transport Zone の物理アップリンクポートを指定



1-4-5. NSX Data Center for vSphere と NSX-T Data Center の相違点

DSVA の展開にあたり、NSX-T 環境では NSX Data Center for vSphere とは仕様面で違いがあります。相違点を理解した上で設計を行う必要があります。

- セキュリティ仮想アプライアンス(SVM)としての Guest Introspection 廃止
  - NSX-T Manager から各 ESXi ホストに展開される Guest Introspection Service によってエージェントレス型ウイルス対策(エンドポイントセキュリティ)を提供
- NSX-T サービスは NSX-T Manager から直接管理を行うため、vCenter Server を中心とした管理体系から NSX-T Manager GUI による管理へ変更
  - NSX-T Manager から vCenter Server をノード登録
  - 各仮想マシンの NSX サービスステータスは NSX-T Manager で管理
- vCenter Server では仮想マシンの NSX セキュリティグループやセキュリティタグは表示できない
- NSX-T セキュリティプロファイル(ポリシー)に対する Deep Security ポリシーの連携は未対応
- NSX-T2.4 より NSX-T Manager に Controller が内蔵されたことにより、商用利用では NSX-T Manager を 3 セット構築することが必要
  - DSM からの登録は NSX-T Manager Cluster VIP を設定することを推奨
- NSX for vShield Endpoint 相当のライセンスなしでの DSVA 展開は不可

1-4-6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更

VMware NSX-T Data Center(以下 NSX-T)2.5 から Trend Micro Deep Security Virtual Appliance(以下 DSVA)を含めた VMware NSX Guest Introspection を利用する 3rd Party Security VM をデプロイする際の仕様に変更がありました。この NSX-T 2.5 における Guest Introspection 関連の仕様変更により DSVA パッケージの仕様変更、DSVA デプロイ手順についても変更があります。

■NSX-T 2.5 Guest Introspection の仕様変更の概要

NSX-T 2.5 における Guest Introspection の仕様の変更により、DSVA など 3rd Party Security VM を各ホストへデプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチェックを実行するプロセスが追加されています（ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署名が付与されます）。この仕様変更に伴い、DSVA を NSX-T 環境でデプロイする際に以下の影響が発生します。

- VMware 社によってデジタル署名がされたソフトウェアパッケージのみが NSX-T 環境にデプロイできる
- Deep Security Manager（以下 DSM）DSM へ DSVA ソフトウェアパッケージをアップロード後、DSM 上で事前に DSVA に割り当てる vCPU 及びメモリの指定を実施することができない

■NSX-T2.5 以降の DSVA の展開方法について

NSX-T2.5 以降では VMware 社によりデジタル署名された DSVA ソフトウェアパッケージを利用してデプロイをする必要があります。

一方で従来 DSVA のソフトウェアパッケージ内の OVF ファイルはメジャーリリース毎に 1 つずつ提供されていましたが、今回の NSX-T Guest Introspection に関する仕様変更に伴い、デプロイ前に DSVA OVF ファイルの割り当て vCPU 及びメモリを指定することができなくなりました。

上記の観点から、トレンドマイクロでは今後リリースする DSVA のソフトウェアパッケージでは以下の 4 種類の OVF が提供される方針に変更されます。

OVF Files	vCPU	Memory
dsva.ovf	2	4096MB
dsva-small.ovf	2	8192MB
dsva-medium.ovf	4	16384MB
dsva-large.ovf	6	24576MB

VMware NSX for vSphere（以下 NSX-V）及び NSX-T 2.4 までの環境では、DSVA を各ホストへデプロイする際には、DSVA ソフトウェアパッケージを DSM にアップロード後、OVF ファイル内の vCPU 及びメモリの値を変更することにより、DSVA の展開リソースを事前に指定した上で NSX Manager から DSVA を展開することが可能です。

Deep Security 12.0 では、DSVA 12.0 Update 3（Deep Security Appliance 12.0.0-682 for ESX-x86_64：2019 年 12 月 5 日リリース）から上記 4 つのタイプのソフトウェアパッケージに対して VMware 社のデジタル署名がされた形で提供されます。

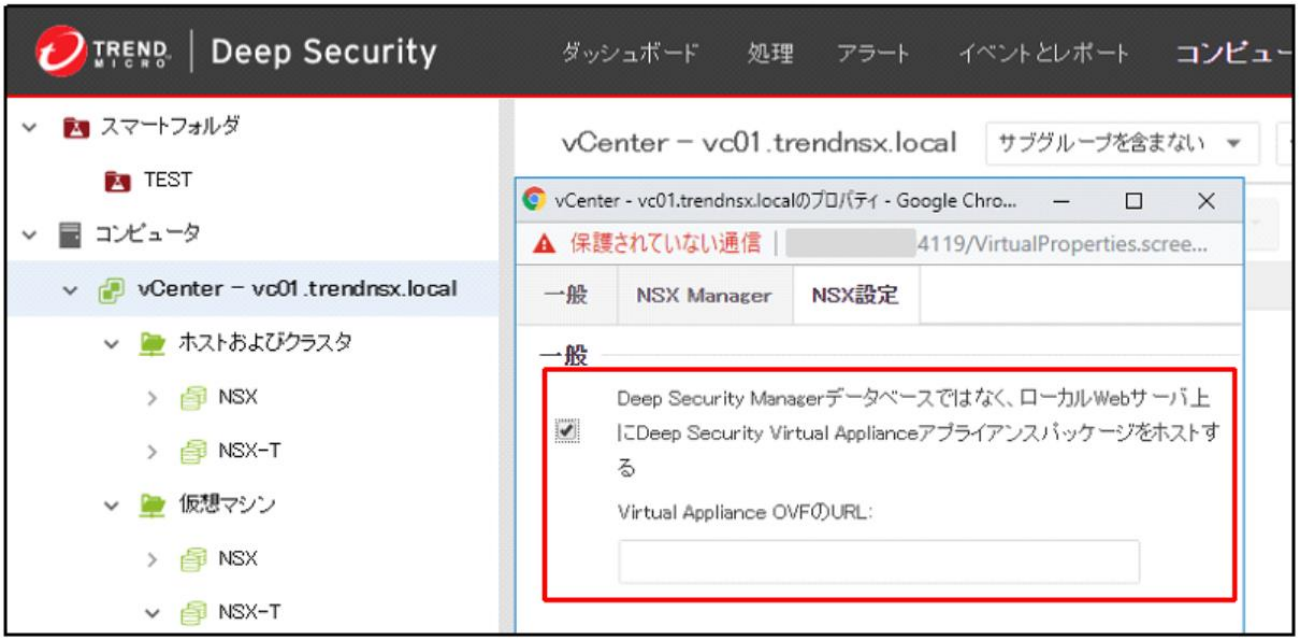
（初期リリースの DSVA12.0.0-364 は NSX-V または NSX-T2.4 環境でのみ利用できます。）

上記の対応により、NSX Manager において DSVA をデプロイする際には、デプロイするソフトウェアパッケージを指定することが可能となります。なお、2019 年 12 月末時点での最新ビルドである Deep Security 12.0 Update 4 では NSX Manager から DSVA をデプロイする際の“展開の仕様”は“Deep Security-Medium”以外の選択ができません。

また、NSX-T2.5.0 以降の既知の不具合により、ワークアラウンドとして DSVA の展開にあたっては、DSVA のソフトウェアパッケージを DSM サーバ上にアップロードするだけではなく、外部の HTTP サーバ（HTTPS では NG）

にもソフトウェアパッケージをアップロードする必要があります。DSM ではその外部 HTTP サーバを DSVA ソフトウェアパッケージの格納先として明示的に設定することで DSVA の展開が可能となります。
（この設定をしていない場合には DSVA のデプロイに失敗します。）

[コンピュータ] > [該当 vCenter Server からプロパティ]> [NSX 設定] > [Virtual Appliance OVF の URL:]



設定する URL は以下の形式で記載してください。
https://[DSM_ Hostname or IP]:4119/appliance/NSX/dsva.ovf(or dsva-small/medium/large.ovf)
※今後の Deep Security Manager の仕様の拡張に伴い指定方法が変わる可能性があります。

指定できる URL パスは 1 つのみのため、複数のソフトウェアパッケージを環境に応じて使い分ける場合には、デプロイごとに本設定の URL の書き換えを行う必要があります。
設定方法の詳細についてはヘルプセンターの内容も参考にしてください。

NSX-T2.5.0 の仕様変更及び制約事項に伴う Deep Security への影響に関する情報の詳細については以下のサイトを参照してください。
VMware NSX-T Data Center 2.5 環境における Trend Micro Deep Security Virtual Appliance（DSVA）デプロイに関する留意事項
https://www.trendmicro.com/ja_jp/business/campaigns/vmware/resources/nsx-t25-and-DSVA_kb.html

また、NSX-T2.5.0 の仕様変更、制約事項の内容の詳細は VMware 社に問合わせしてください。

2. VMware NSX 環境における DSVA エージェントレスセキュリティ保護環境の構築手順

2-1. 本構築ガイドにおける事前準備しておくべき環境と想定環境

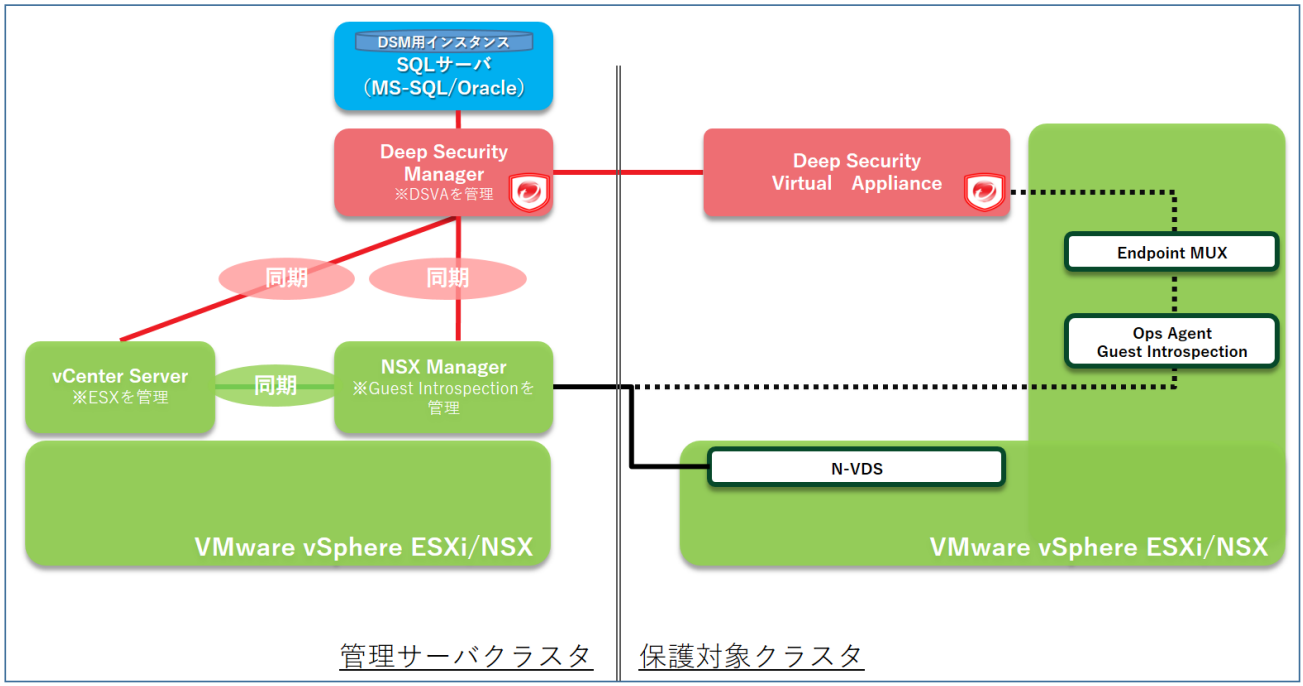
本ガイドに従って作業する際に、事前に以下の環境が準備されていることを確認してください。

- 管理サーバクラスタ、保護対象クラスタのESXiホスト
- vCenter Server
- NSX Manager
- VMware Horizon 7 環境
  （仮想デスクトップ環境利用の場合：WindowsクライアントOSによるリンククローン展開環境を想定）
- 仮想デスクトップ用マスターイメージ（WindowsクライアントOS）
- DSM用Microsoft SQLサーバ インストール環境（WindowsサーバOS）
- VMware NSX コンポーネント
  myVMwareからダウンロードしてください（myVMwareアカウントが必要となります。）
  https://my.vmware.com/ja/group/vmware/downloads
- Deep Security コンポーネント
  トレンドマイクロダウンロードセンターからダウンロードしてください。
  http://downloadcenter.trendmicro.com/index.php?regs=jp

また、DSVAの展開にあたっては予めNSX-Tを展開するESXiホストに対してTransport Node Profileの展開及びDeep Securityの不正プログラム対策イベントの検出をトリガーに仮想マシンを隔離したい場合には、分散ファイアウォールの有効化をする必要があります。

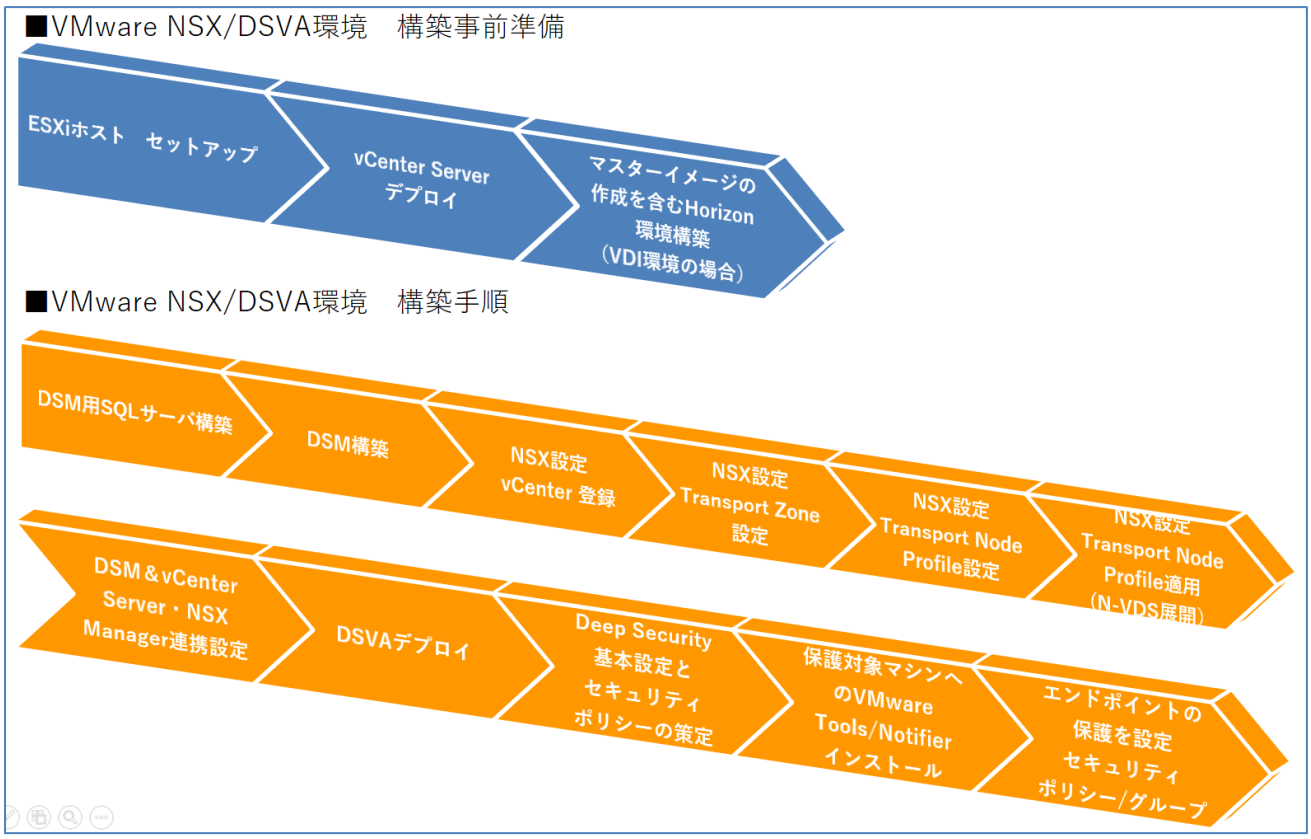
2-2. 本ガイドで想定する環境

- Horizon にて仮想マシン（VDI 用 Windows クライアント）が展開される
- 仮想マシンに対して、Deep Security の不正プログラム対策を有効化
  適用する Deep Security のポリシーは、トレンドマイクロが提供するデフォルトのポリシーである
  “Windows 10 Desktop”を継承してカスタマイズした”**VDI_Windows Desktop_Demo01** “を設定
- オプションとして、Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと連携した自動隔離ができるように隔離用セキュリティグループも設定
- 不正プログラム対策イベント検出時に付与する NSX セキュリティタグを
  “ANTI_VIRUS.VirusFound.threat=high”に設定



2-3. エージェントレスによる仮想マシン保護　構築手順

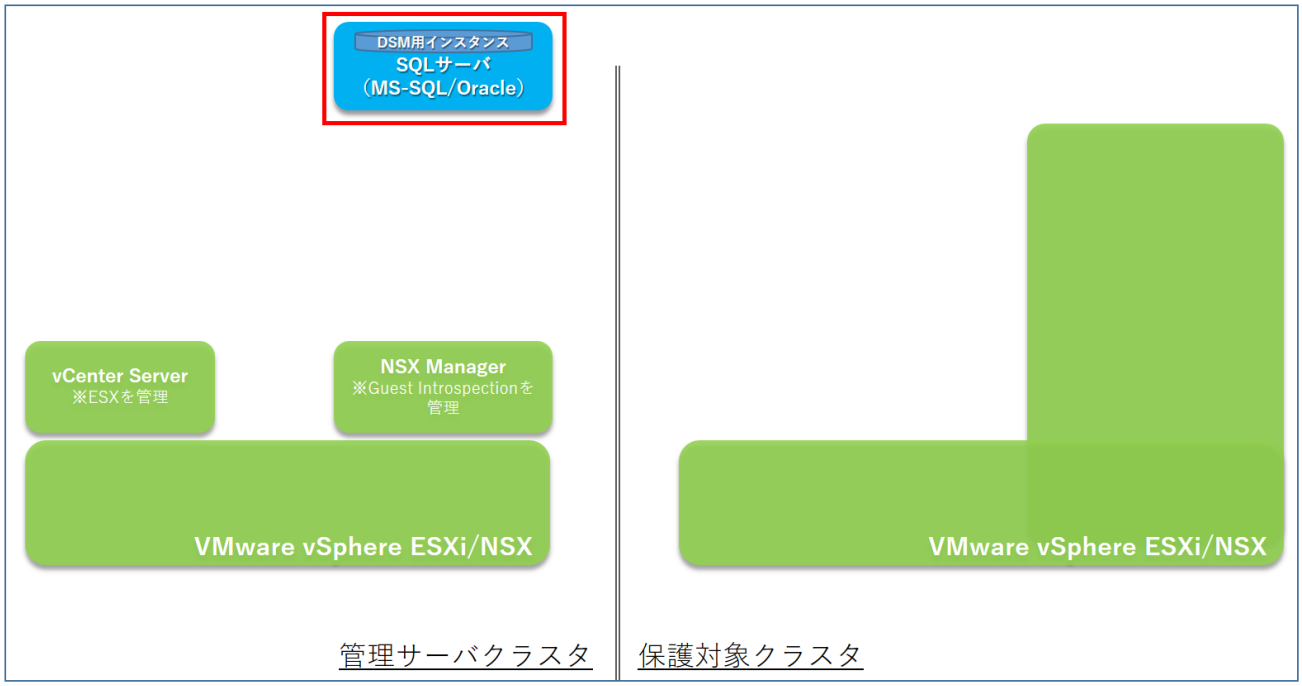
構築の全体の流れは以下となります。



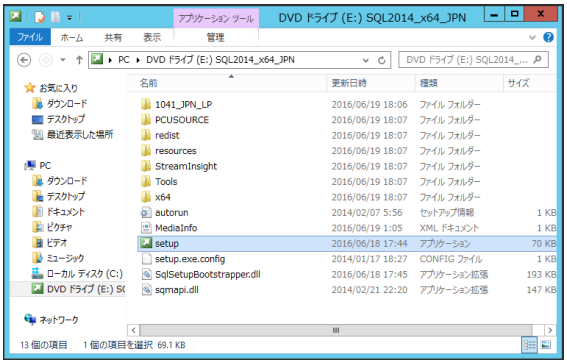
2-3-1. DSM 用 SQL サーバ構築

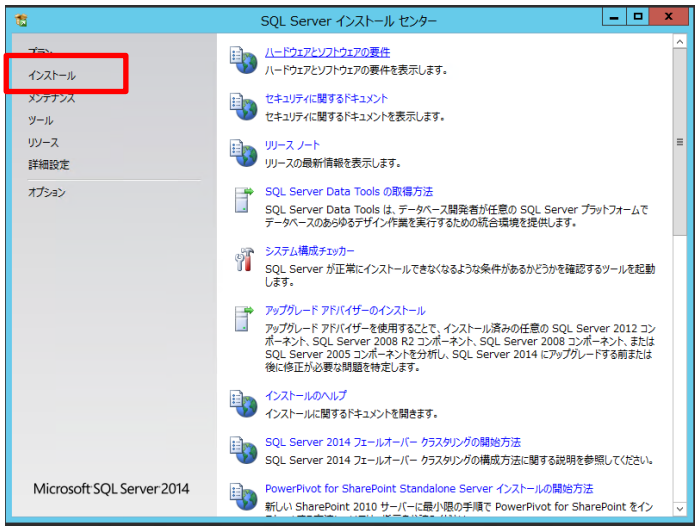
Deep Security の設定、イベントを格納するためのデータベースを構築します。

DSM 用 SQL サーバを構築する前に、SQL インストール時に必要となる.NET Framework3.5 を事前インストールしておく必要があります。

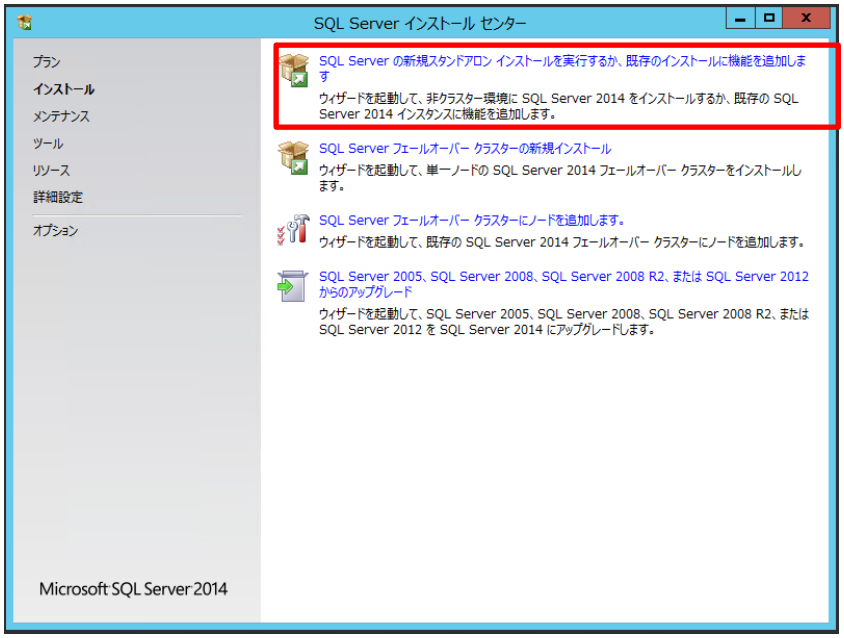


1） DSM 用 SQL サーバ上でインストーラを実行し、インストールを開始する





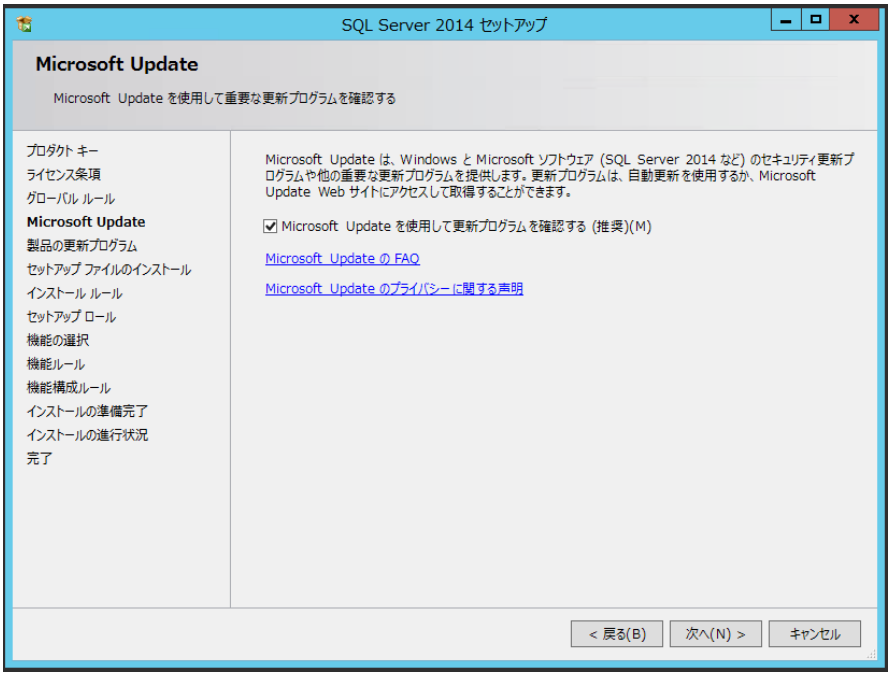
2) ***[SQL Server の新規スタンドアロンインストールを実行するか、既存のインストールに機能を追加します]***を選択し、スタンドアロンインストールを実行する



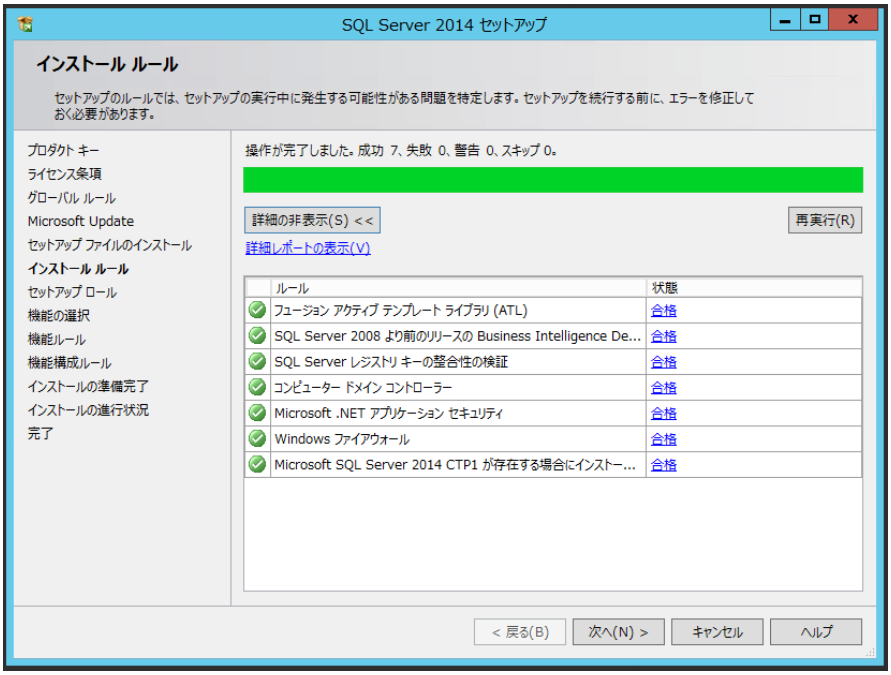
3) プロダクトキーを入力する

4) ライセンス条項に同意する

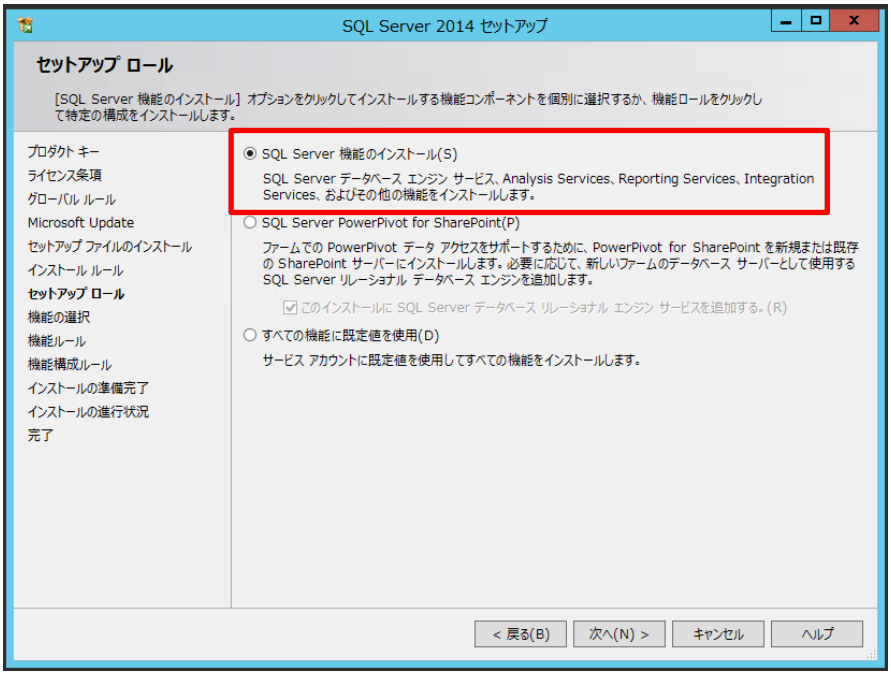
5) Microsoft Update の更新プログラムの確認をするようにチェックする



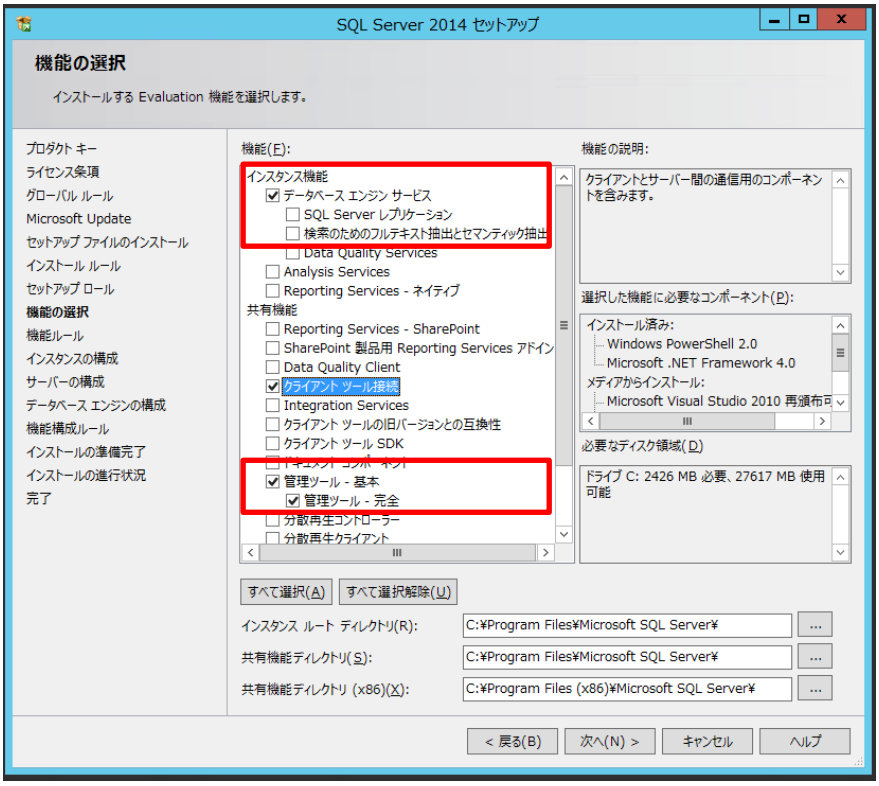
6）インストール要件のチェックを実行し、問題がないことを確認して*[次へ]*



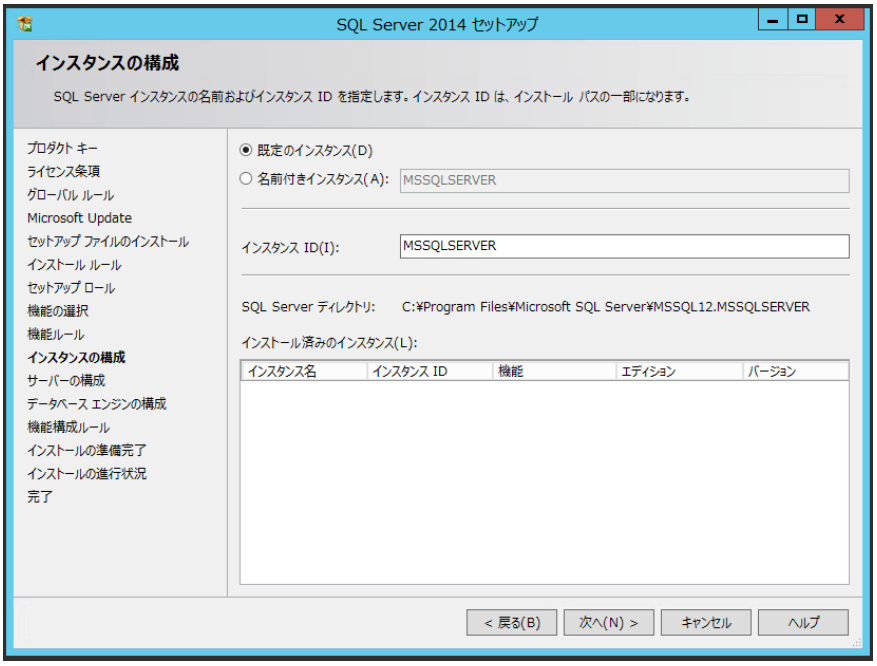
7） *[SQL Server 機能のインストール]*を選択する



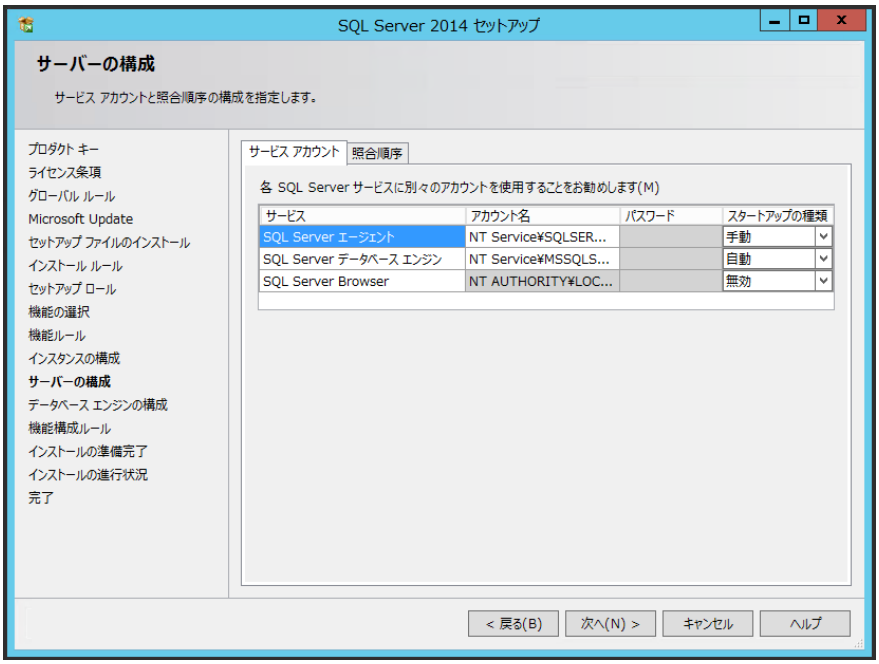
8) ***[機能選択]***にて、***[データベースエンジンサービス][管理ツール・基本]***を選択する



9) ***[インスタンスの構成]***を確認して***[次へ]***

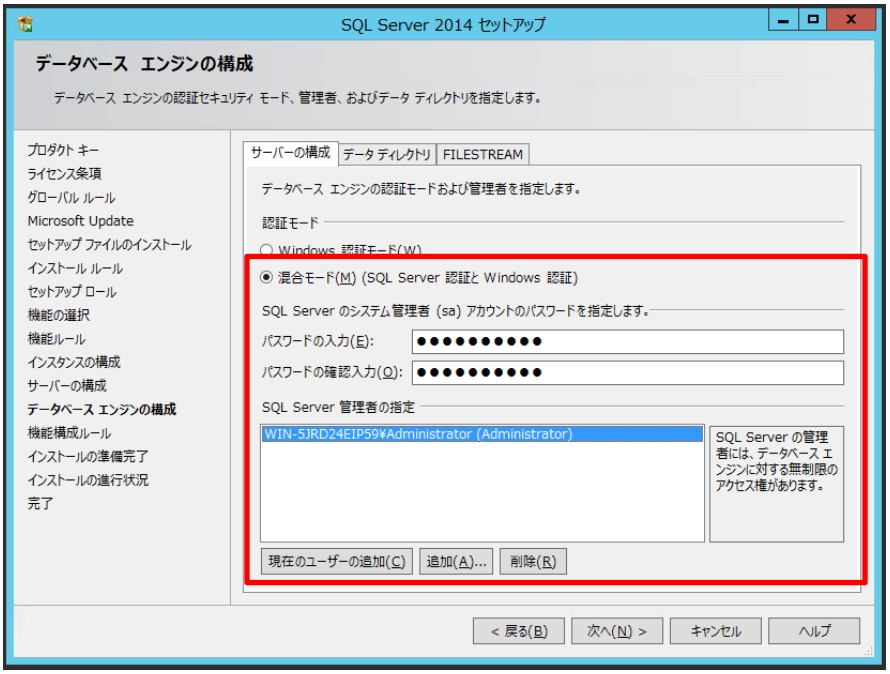


10) *[サーバ構成]*を確認して*[次へ]*



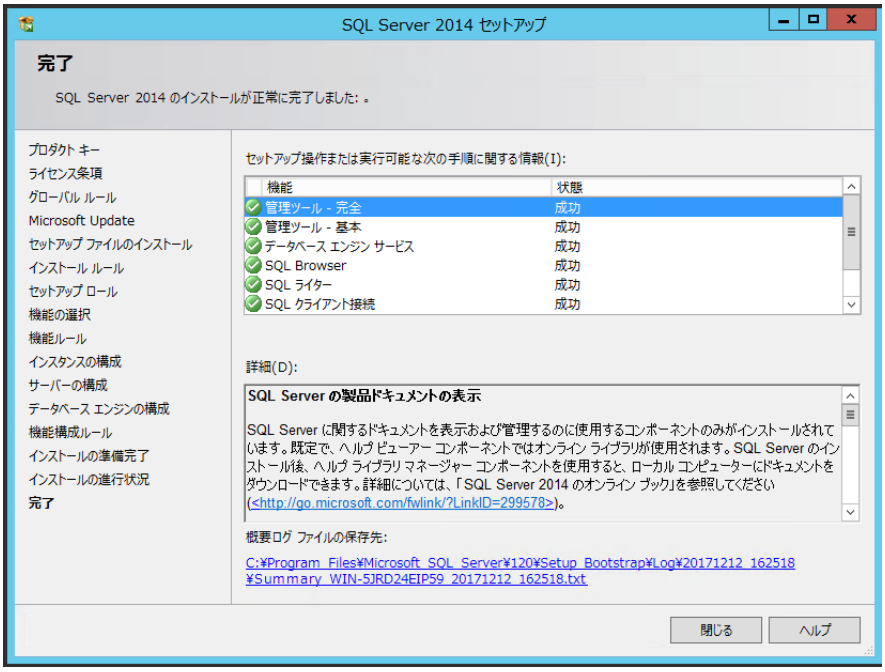
11) *[データベース エンジンの構成]*を設定する

- **[認証モード]** : **[混合モード]**を選択
- **[パスワードの入力]** : sa アカウントのパスワードを設定
- **[パスワード確認入力]** : sa アカウントのパスワードを設定
- **[SQL Server 管理者の指定]** : **[現在のユーザの追加]**でユーザ追加

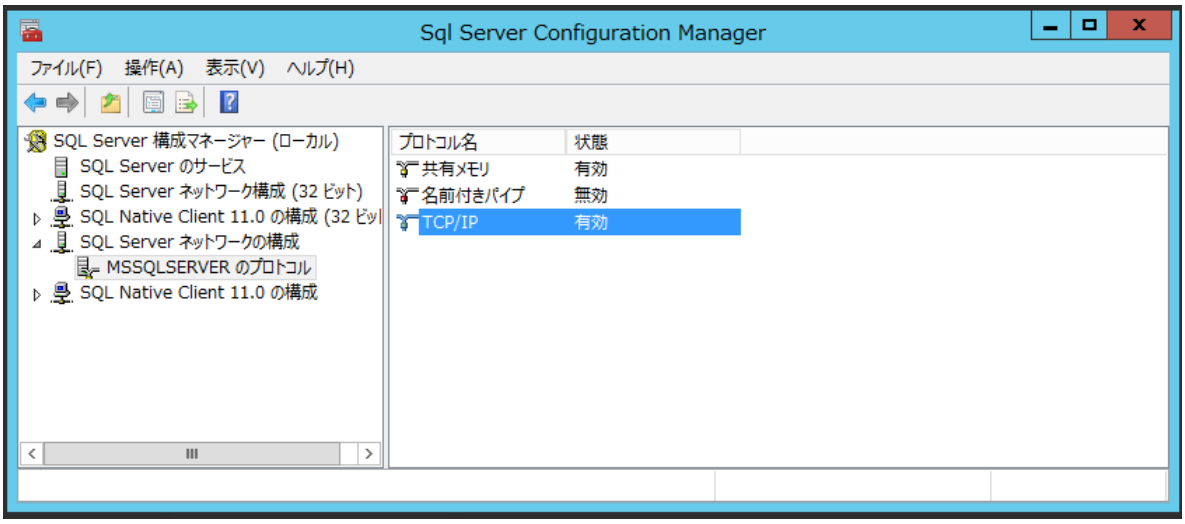


12) *[インストール]*をクリックする

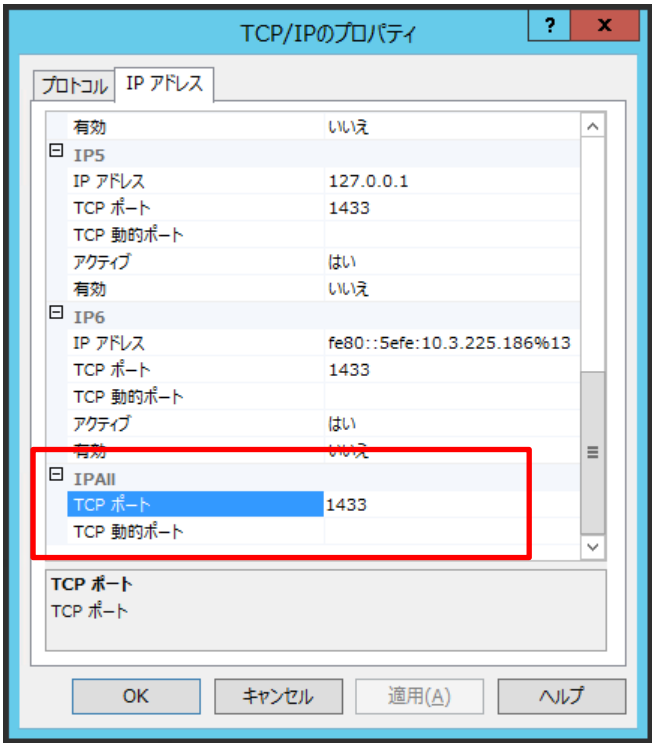
13) インストールが正常に完了したことを確認する



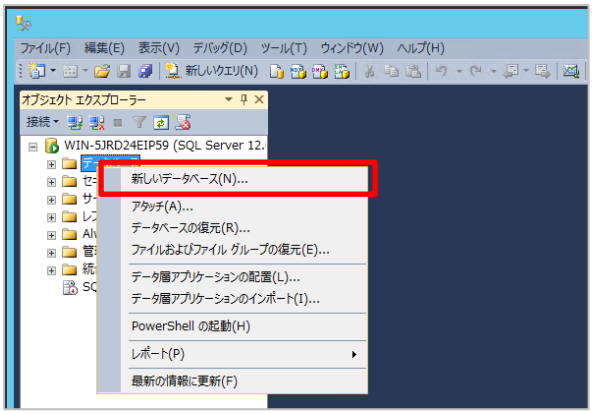
14) **SQL Server 構成マネージャ**にログインし、***[MSSQLSERVER のプロトコル]***から***[TCP/IP]***を選択する



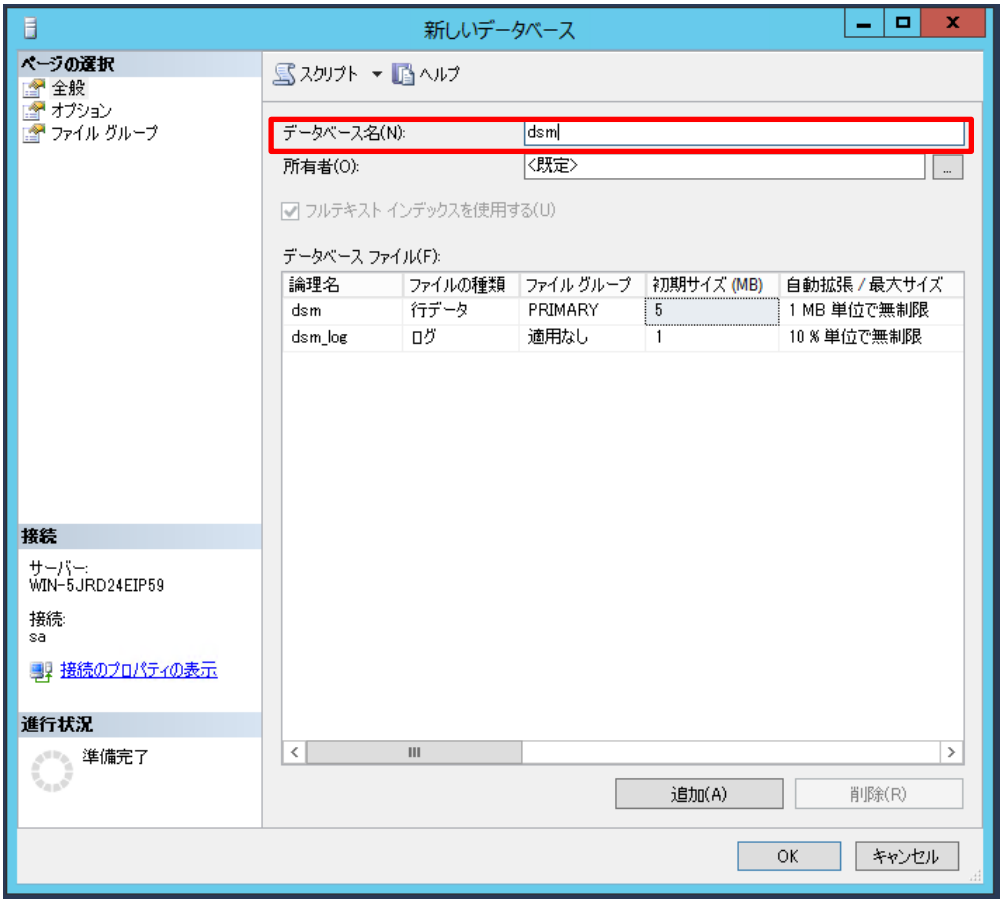
15) ***[TCP/IP のプロパティ]***で、***[IPALL]***の***ポート番号(1433)***を指定し、***[適用]***する



16) **SQL Management Studio** にログインし、*[オブジェクト エクスプローラ]* > *[データベース]*を右クリックして、*[新しいデータベース]*を選択する



17) *[データベース名]*に**データベース名**(dsm)を入力する



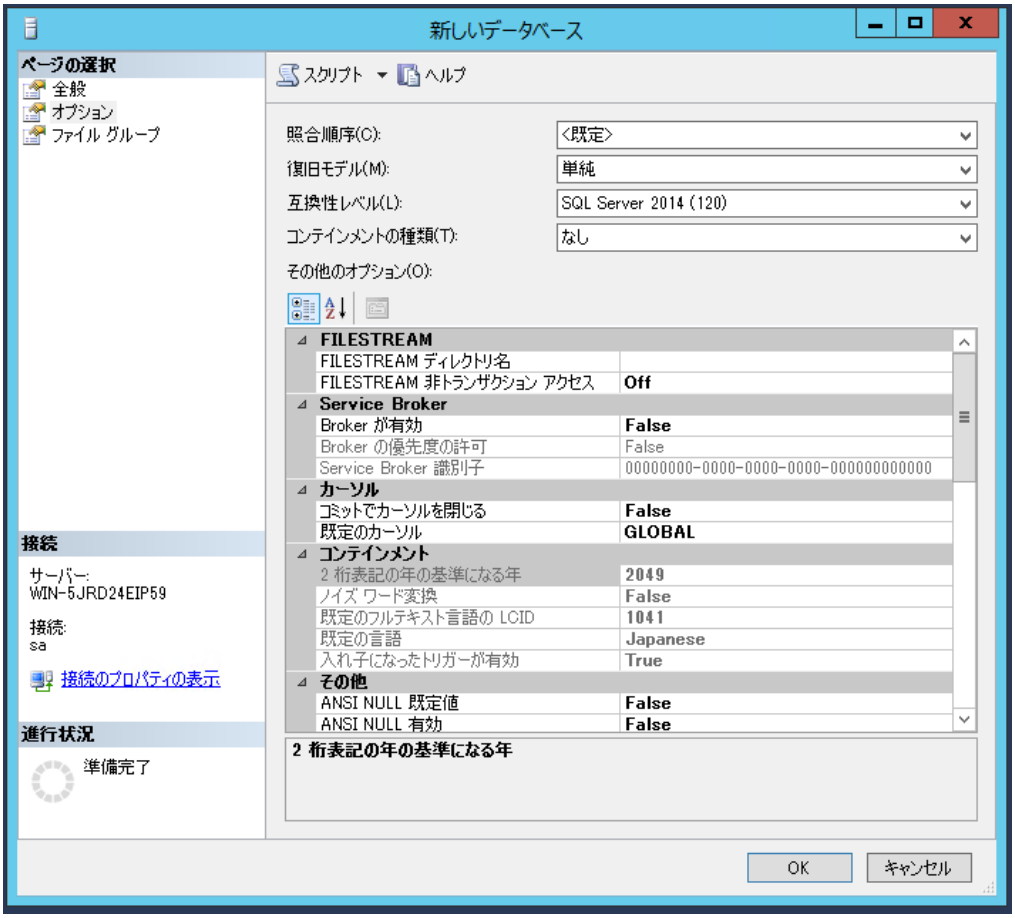
18) *[オプション]*で**復旧モデル**から*[単純]*を選択して、*[OK]*を選択する

【TIPS】

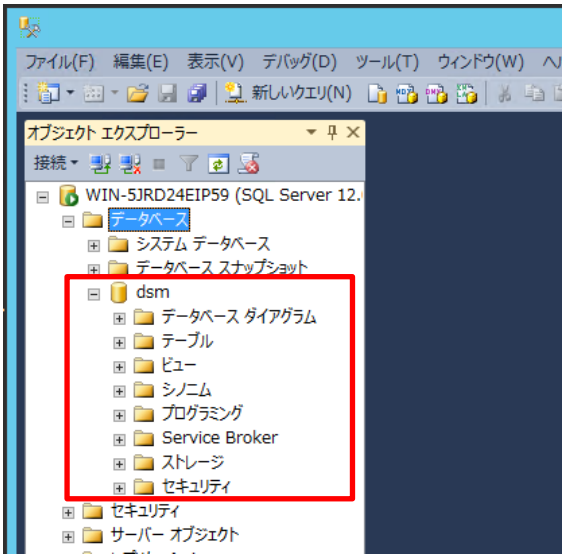
復旧モデルは、「完全」や「一括ログ」を選択することも可能ですが、データベースの肥大防止やメンテナンス負荷軽減の観点から、復旧モデルを[単純]にすることを推奨しています。

関連 FAQ：SQL Server の復旧モデルについて

http://esupport.trendmicro.com/solution/ja-JP/1112366.aspx

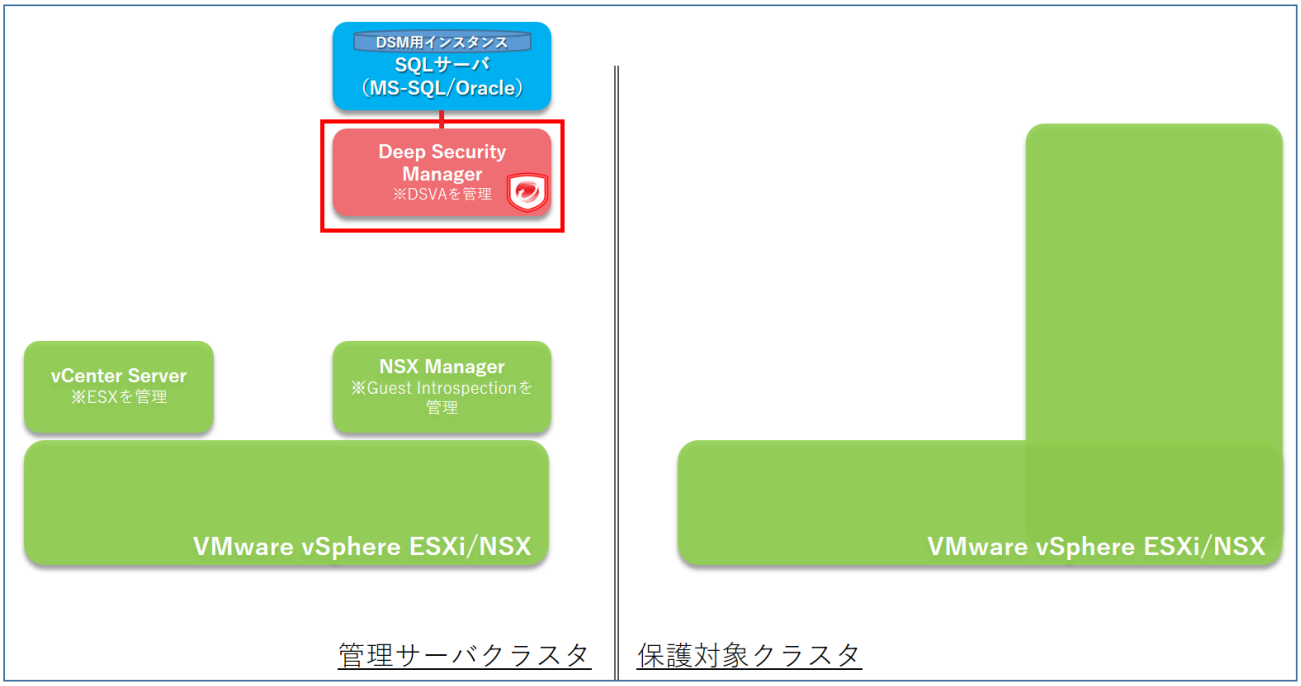


19) 新しいデータベースインスタンスができていることを確認する

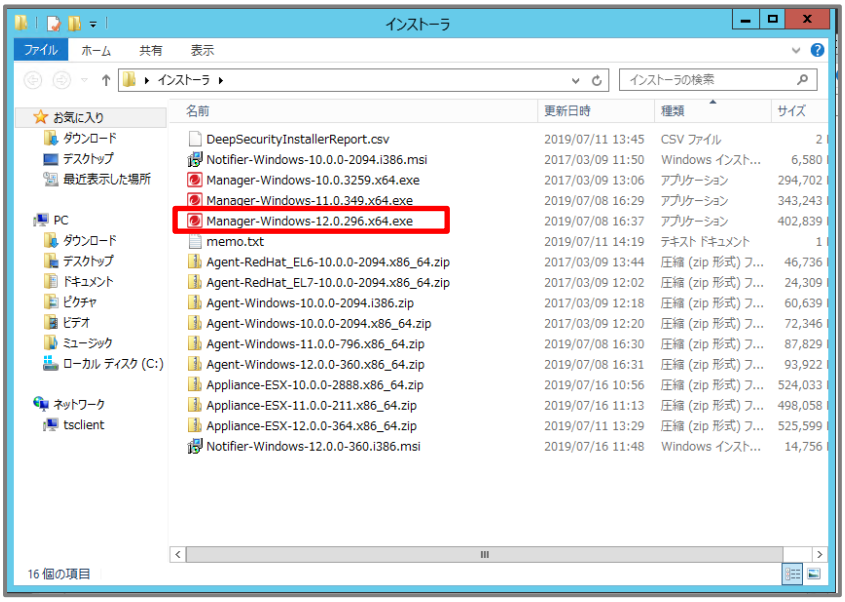


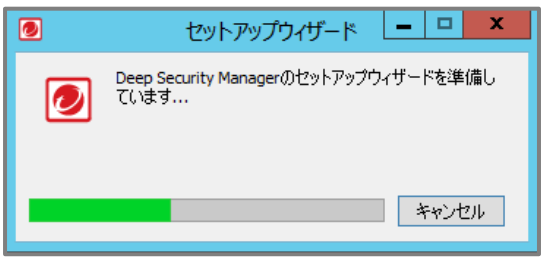
2-3-2. Deep Security Manager(DSM) インストール

DSM を Windows サーバにインストールし、DSM 用に設定した SQL サーバに接続します。



1) DSM 用サーバ上で Deep Security Manager のインストーラを実行する





【TIPS】

DSM をインストールする際に、インストーラと同一ディレクトリに DSA や DSVA などのインストールコンポーネントを配置しておくと、インストール時にコンポーネントを自動的に DSM にアップロードされます。

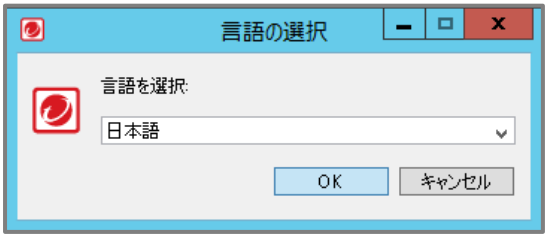
Deep Security では、管理対象となる防御用プログラム（DSA/DSVA）を DSM にインポートしておく必要があります。以下のコンポーネントをインストール時に準備しておくようにしてください。

- DSM の OS にあわせた DSA（DSR として利用するため）
- DSVA のソフトウェアパッケージについてはヘルプセンターに展開されている最新のビルドを利用してください。
- RHEL 7（x64）用 Deep Security Agent（DSVA Build 単位でのバージョンアップ用）
  - DSVA のソフトウェアパッケージは、メジャーリリース毎及び大幅なエンハンスメントが発生した場合にリリースされます。
  - 適宜リリースされる Update については、Redhat(64bit)版 DSA を利用してアップデートしたい Appliance バージョンのアップデートを行います。
    （実際は、DSVA OVF と該当の DSA を DSM ローカルにダウンロードしておくことで、NSX からの“デプロイ”時に自動的に指定された Build で展開されます。）
  - RHEL 7（x64）用 Deep Security Agent（DSVA Build 単位でのバージョンアップ用）
  - ソフトウェアパッケージの例

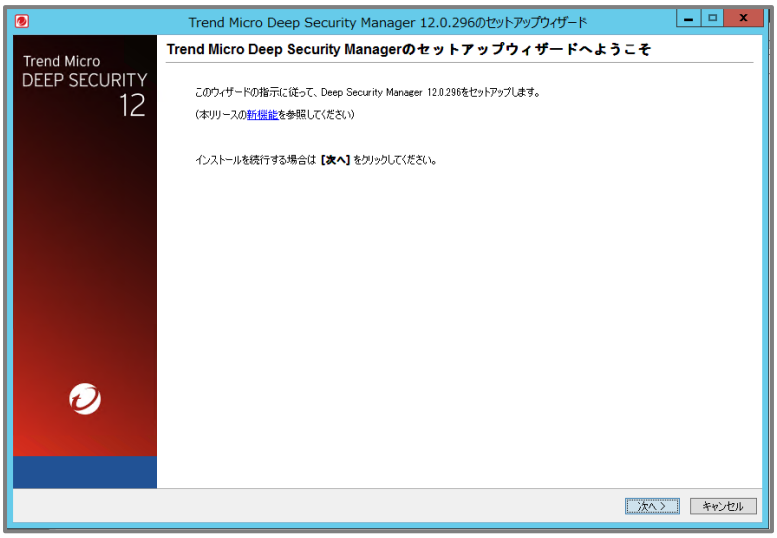
    Appliance-ESX-12.x.x-xxxx.x86-64.zip ：DSVA パッケージ本体（DS12.0 以降）
    Agent-RedHat-EL7-<version>-<build>.x86-64.zip ：DSVA を最新版で配置するための DSA
    Agent-Windows-<version>-<build>.x86_64.zip ：DSR 用 DSA（導入が Linux 版の場合は Linux 版 DSA）
  - DSVA 展開ビルドの指定方法（デフォルトでは DSM ローカルにアップロードされている DSVA と RHEL 7（x64）用 DSA の中で最新のビルドが選択）
    [管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]

また、ソフトウェアバージョンについては、VMware 各ソリューションとの互換性を確認の上、その中で最新のビルドを利用することを推奨します。

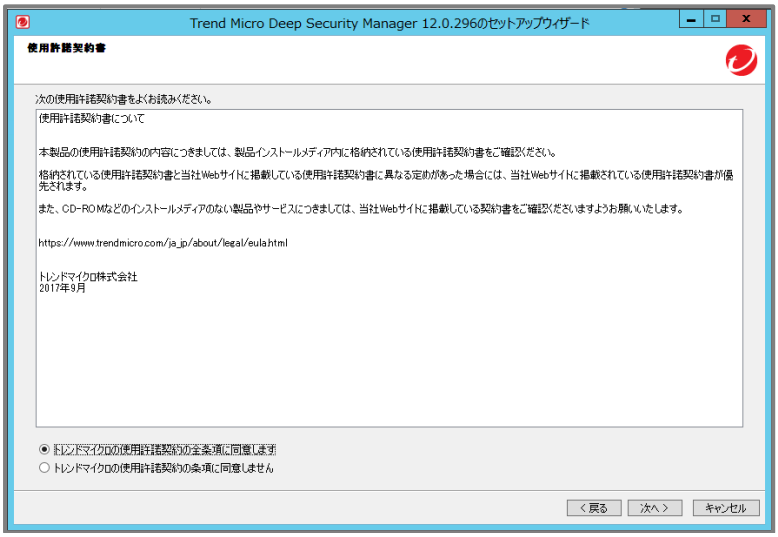
2） 言語選択を行う



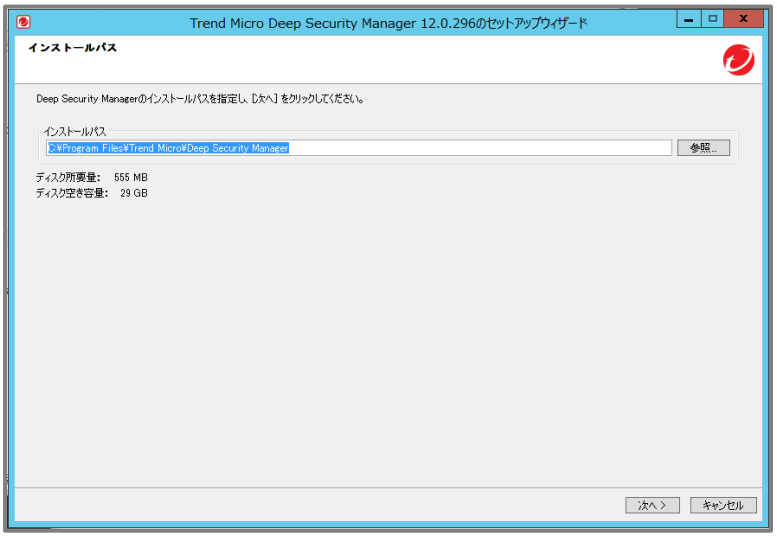
3) セットアップウィザードで*[次へ]*を選択する



4) 使用許諾契約に同意する

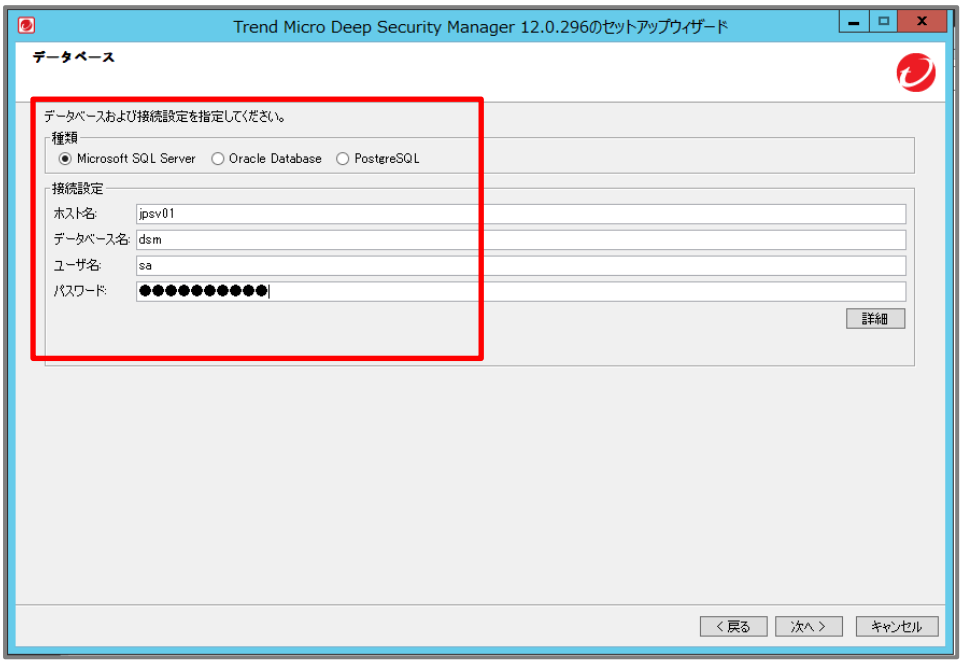


5) インストールパスを指定する

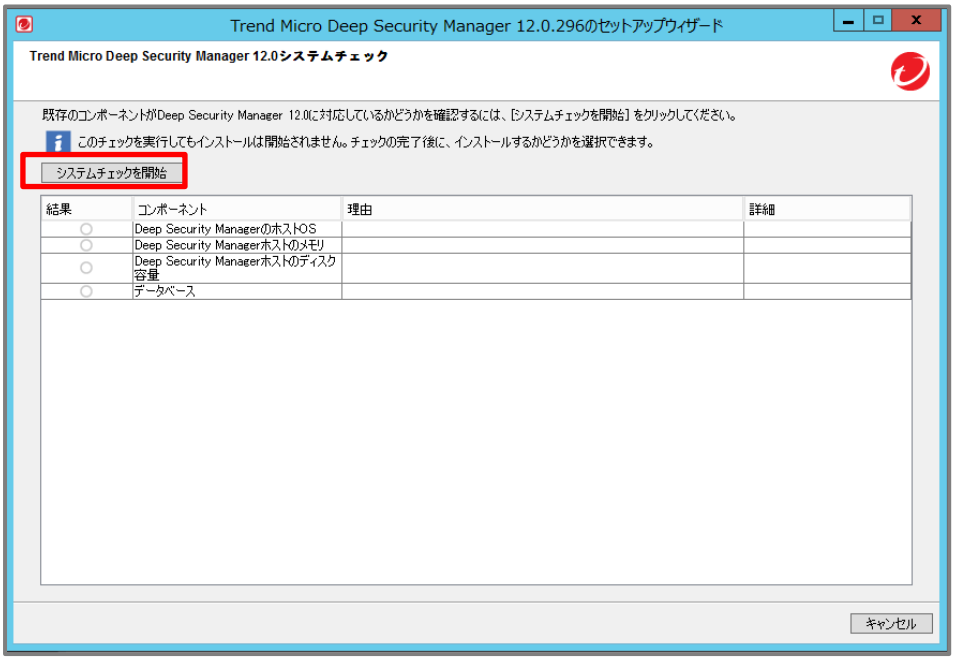


6）データベースの接続設定を行う

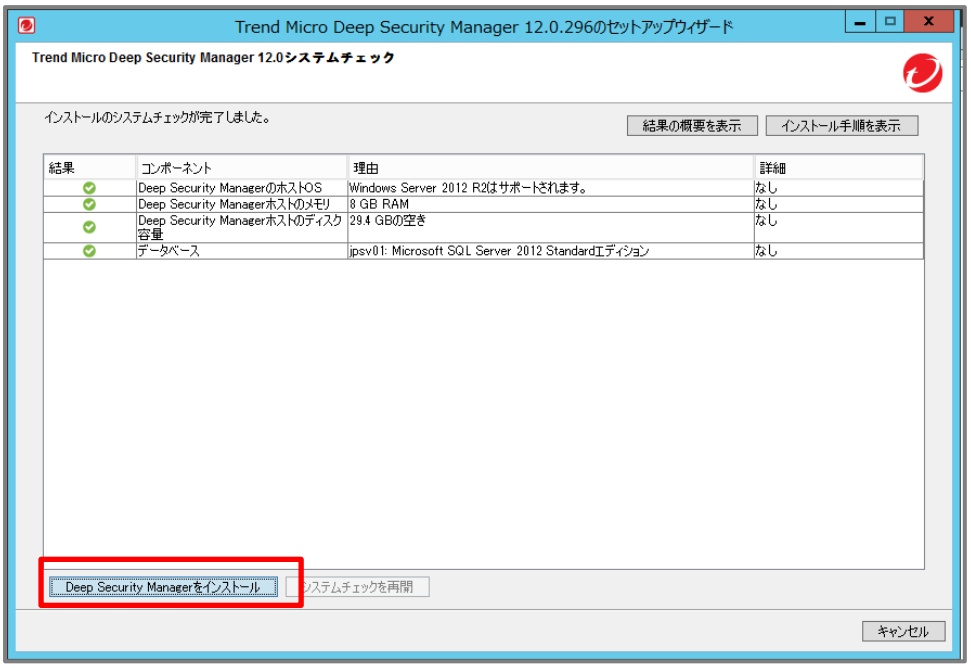
- **［オプション］**： データベース種類を選択
- **［接続設定］**： DSM 用 SQL の*[ホスト名][データベース名]*を指定
  トランスポートを*[TCP]*で設定
  データベースインスタンスに対する*[ユーザ名 (sa)] [パスワード]*を指定



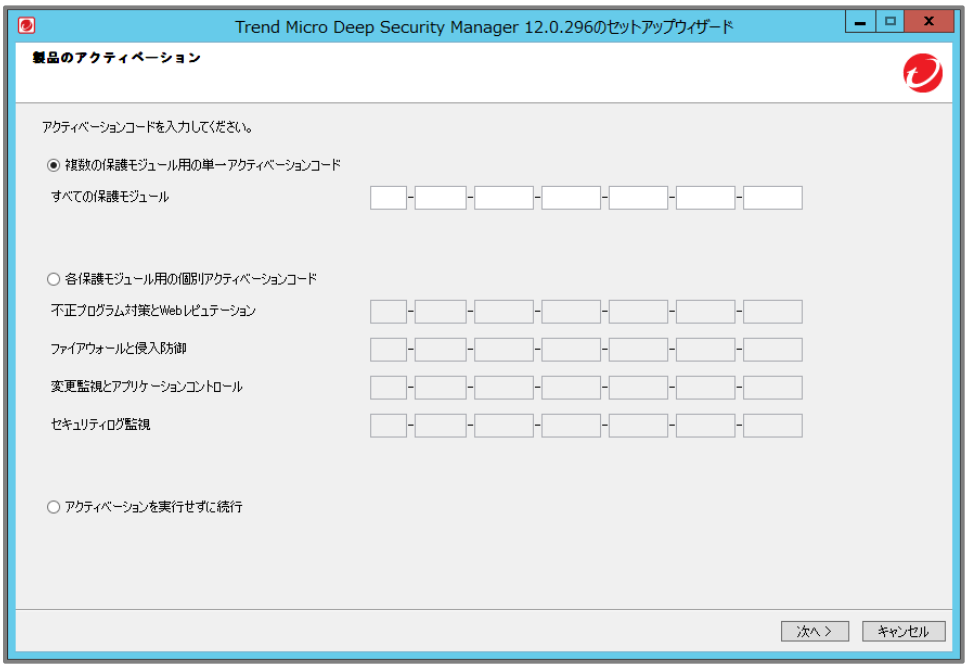
7）*[システムチェックを開始]*をクリックして、インストールチェックを行う



8) システムチェックの結果がすべてグリーンステータスとなることを確認して、
*[Deep Security Manager をインストール]*をクリックする

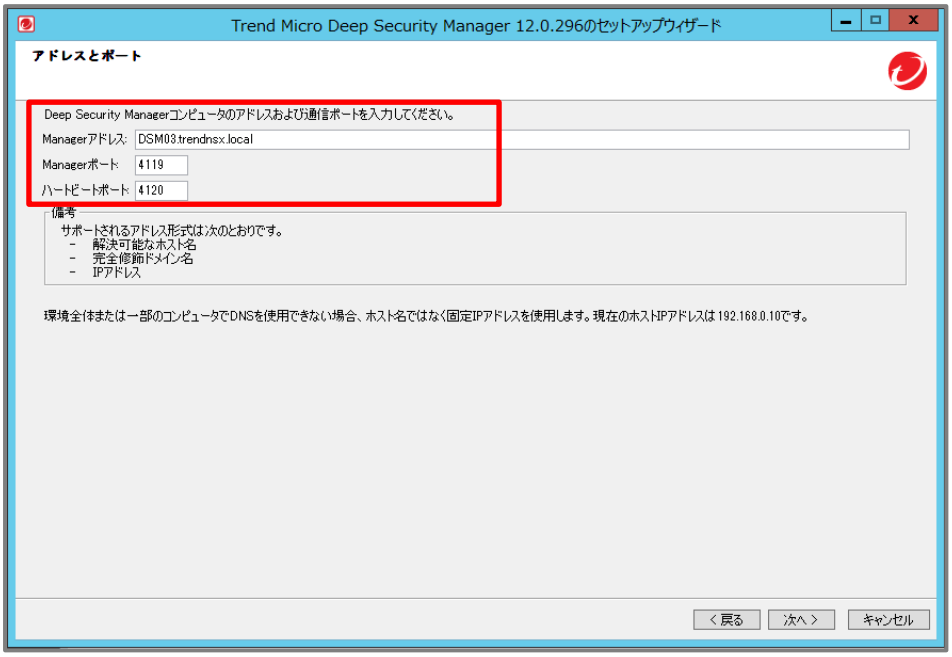


9) アクティベーションコードを入力する



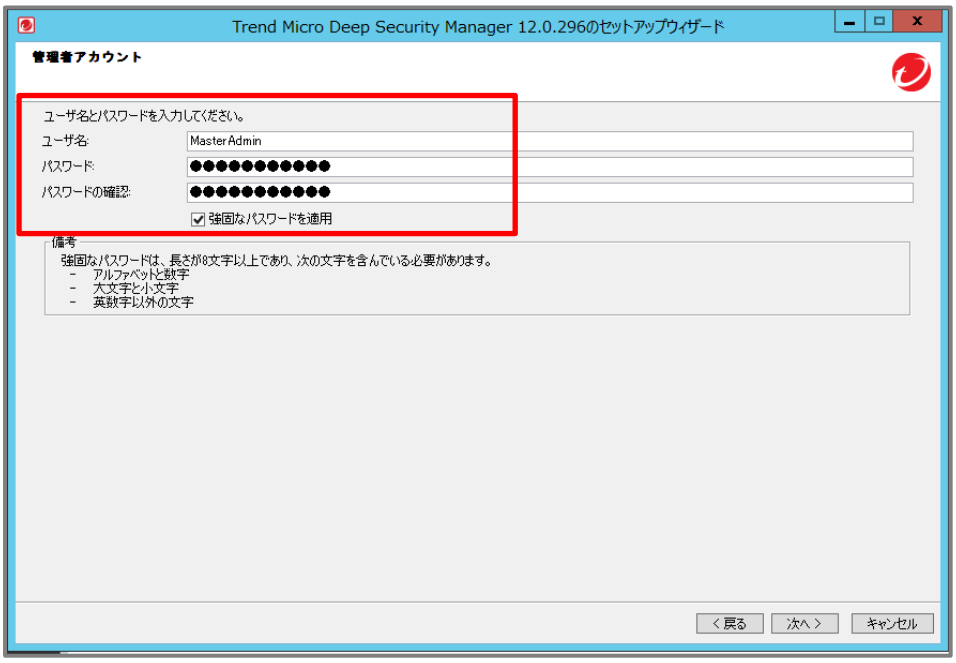
10) DSM のアドレス、ポート番号、ハートビートポートを設定する

- **[Manager アドレス]** : 名前解決可能なホスト名を設定
- **[Manager ポート]** : デフォルト **4119** を設定
- **[ハートビートポート]** : デフォルト **4220** を設定



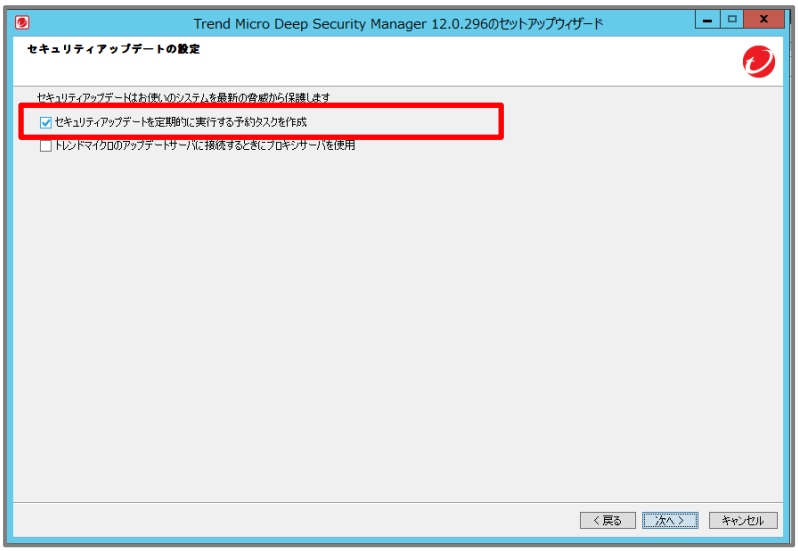
11) 管理者アカウントの設定を行う

- **[ユーザ名]** : 任意のユーザ名を設定
- **[パスワード]** : 任意のパスワードを設定



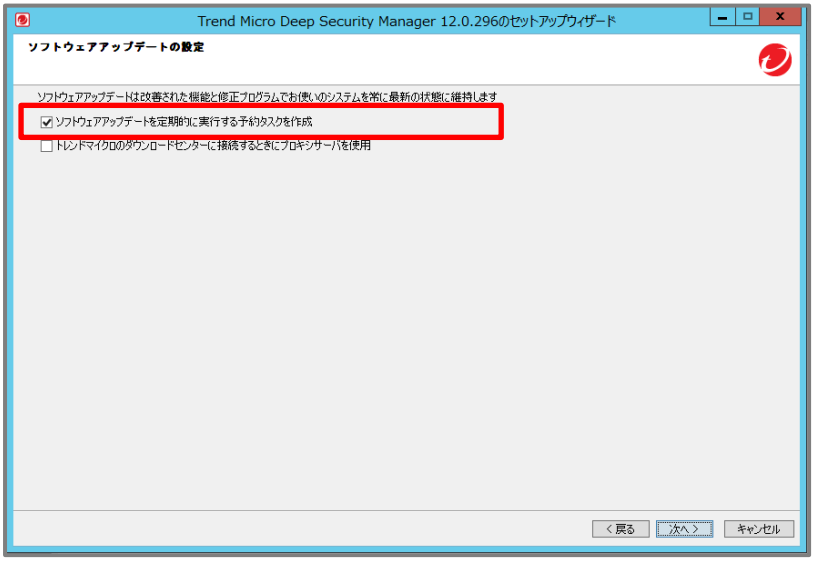
12) セキュリティアップデートの設定を行う

- ***[セキュリティアップデートを定期的に実行する予約タスクを作成する]*** :
  チェックボックスを入力
- ***[トレンドマイクロのアップデートサーバに接続するときにプロキシサーバを使用]*** :
  - プロキシサーバ経由でアクセスする場合にはチェックボックスを入力し、プロキシサーバの情報、認証情報(オプション)を入力
  - 対応するプロトコルは HTTP、SOCKS4、SOCKS5

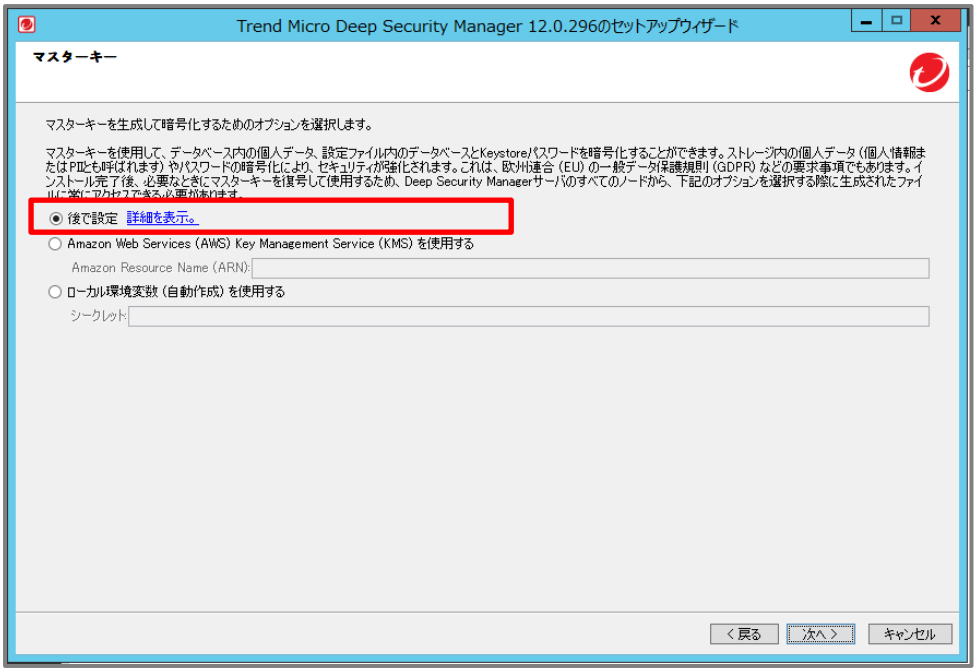


13) ソフトウェアアップデートの設定を行う

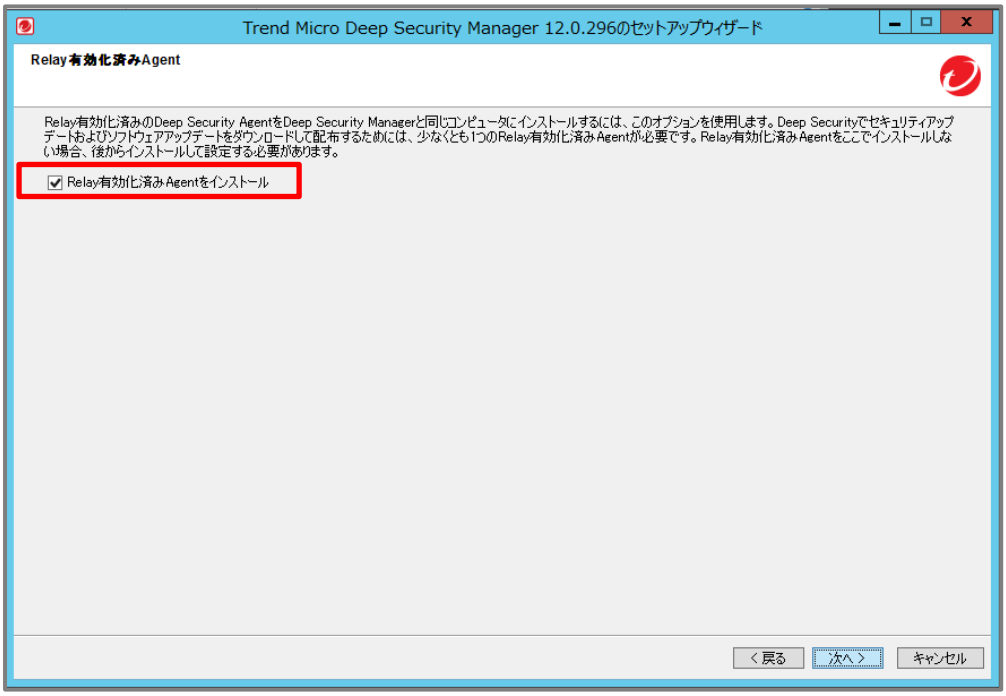
- ***[ソフトウェアアップデートを定期的に実行する予約タスクを作成する]*** :
  チェックボックスを入力
- ***[トレンドマイクロのダウンロードセンターに接続するときにプロキシサーバを使用]*** :
  プロキシサーバ経由でアクセスする場合にはチェックボックスを入力し、プロキシサーバの情報、認証情報(オプション)を入力
  - 対応するプロトコルは HTTP、SOCKS4、SOCKS5



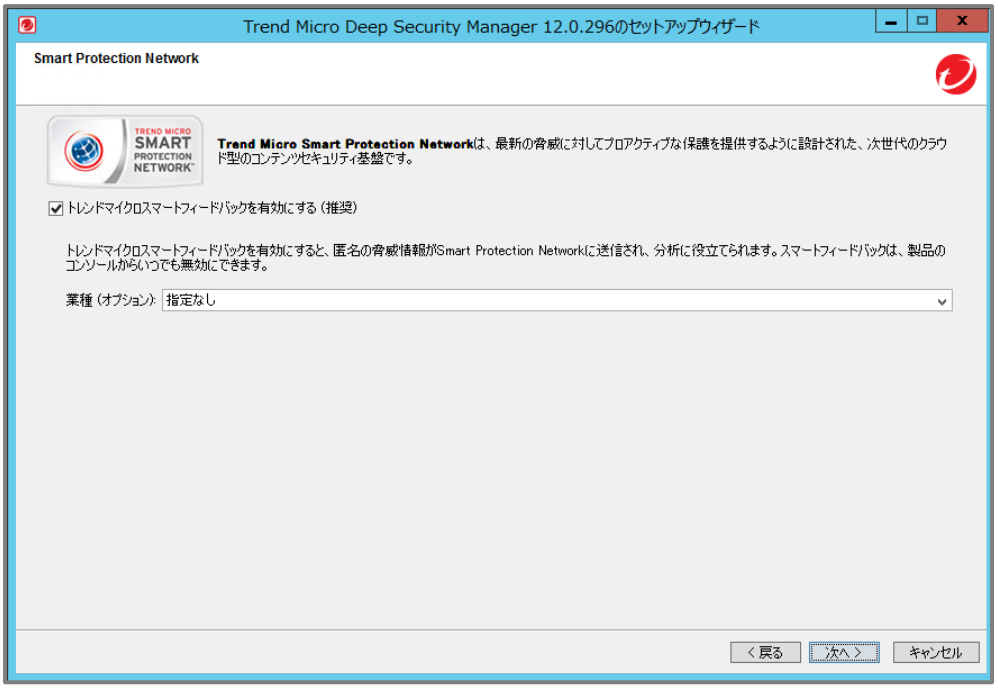
14) マスターキーを生成して暗号化するためのオプションについては***[後で設定]***を選択する



15) DSM に Relay サーバ（DSR）を同居させるため、***[Relay 有効化済み Agent をインストール]***にチェックを入れる

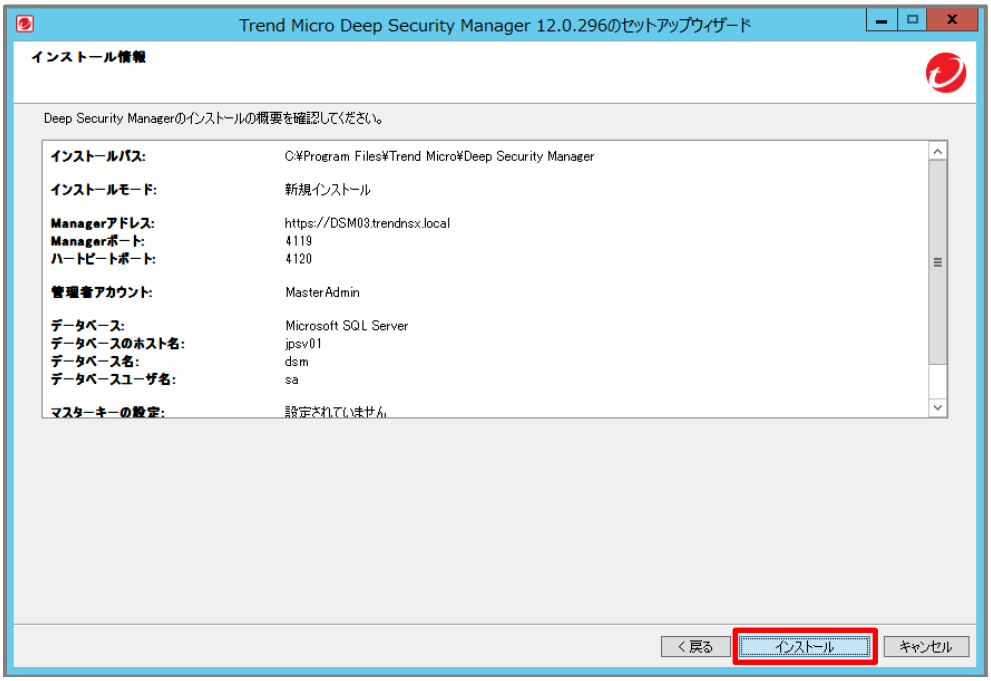


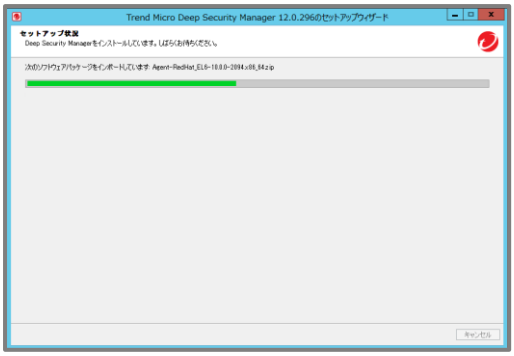
16) トレンドマイクロスマートフィードバックを有効にしたまま、業種情報を入力する（任意）



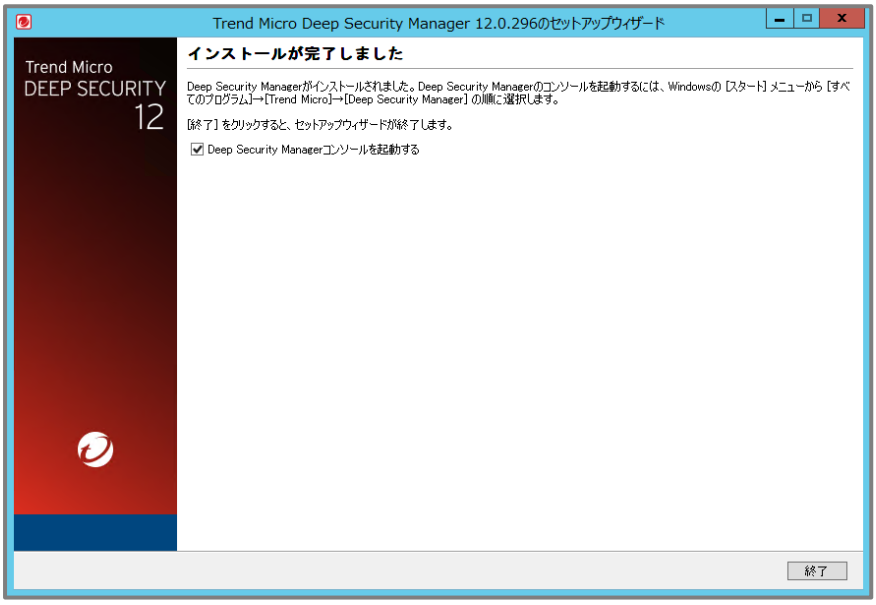
17) インストール情報を確認し、*[インストール]*ボタンをクリックする

インストールの完了まで 10 分程度かかります。





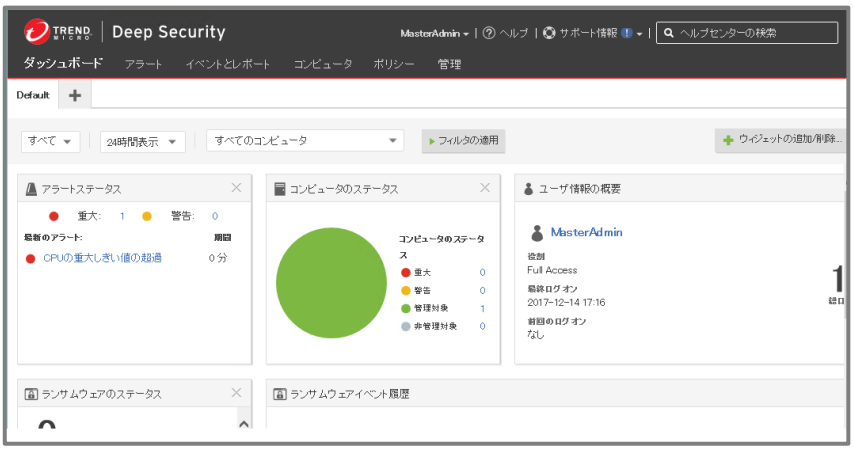
18) インストール完了を確認する



19) Deep Security Manager にログインできることを確認する

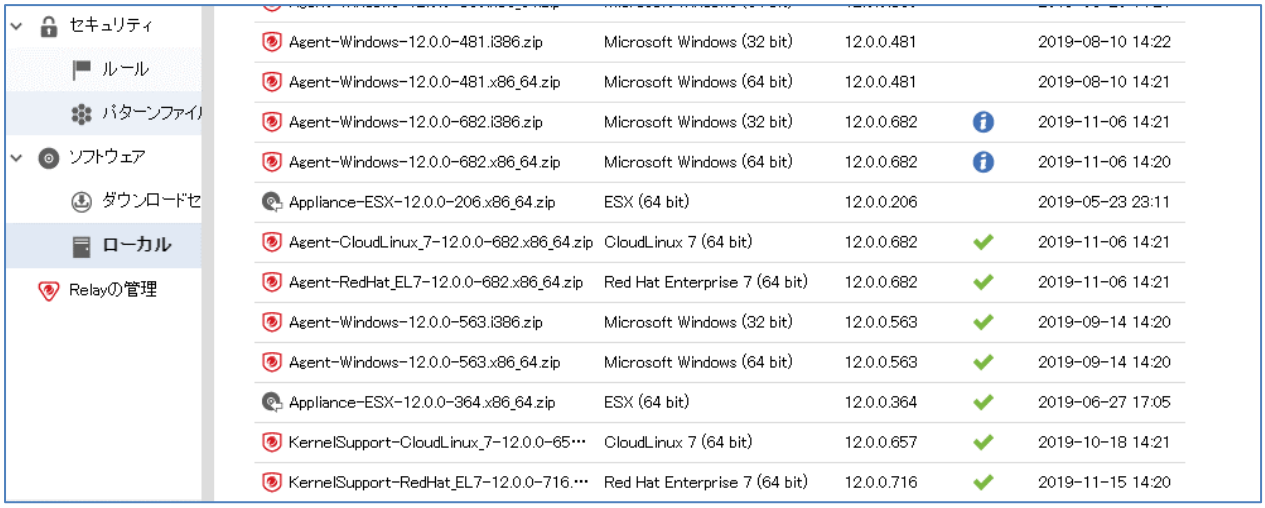
インストール完了画面からログインしない場合には、ブラウザにて以下の URL でアクセスしてトップ画面が表示されることを確認します。

https://＜DSM_Host_Name_or_IP＞:4119



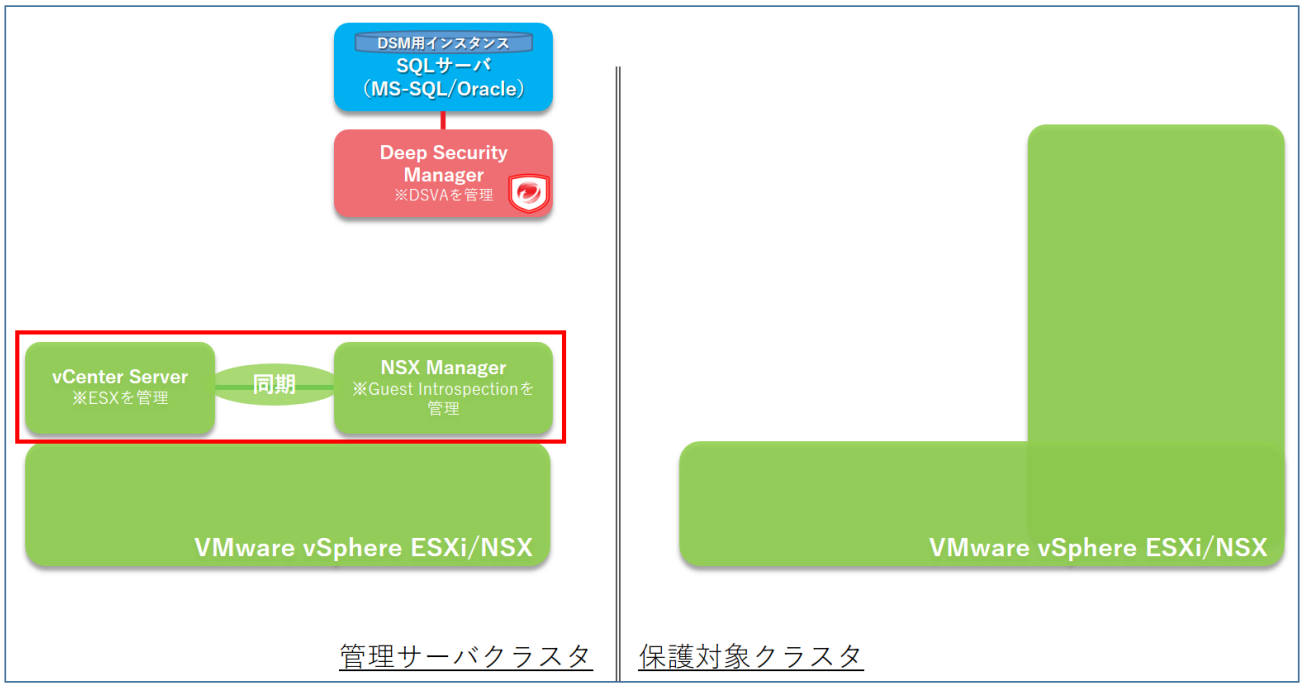
20）DSM に必要なパッケージがインポートされていることを確認する

[管理]>[ソフトウェア]>[ローカル]



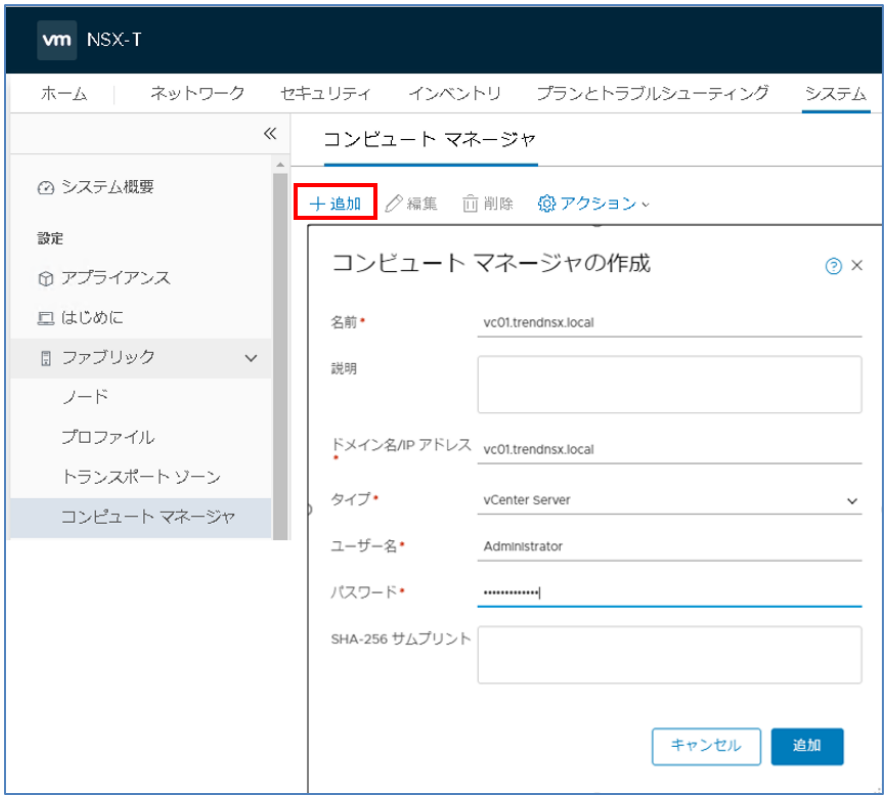
2-3-3. NSX ファブリック設定 － NSX Manager への vCenter Server の登録

NSX Manager から vCenter Server をコンピュートマネージャとして登録を行います。



1) NSX Manager にアクセスをして

*[システム]>[ファブリック]>[コンピュート マネージャ]*を選択して、*[追加]*を選択する



vCenter Server の接続情報を登録する

- **[名前]** : vCenter Server 名を設定
- **[ドメイン名/IP アドレス]** : vCenter Server のドメイン名または IP アドレスを設定
- **[タイプ]** : “vCenter Server”を選択
- **[ユーザ名]** : vCenter Server の管理者権限を持ったユーザ名を設定
- **[パスワード]** : 管理者権限を持ったユーザの管理者パスワード

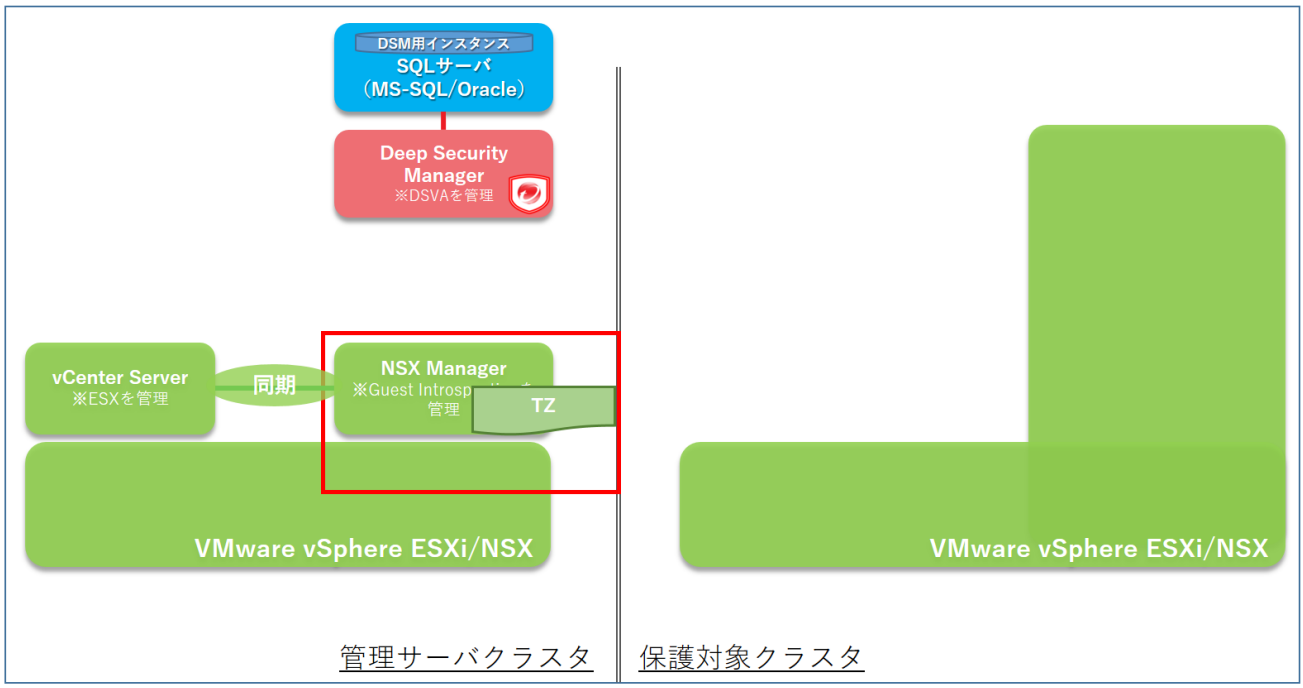
2) コンピュートマネージャとして vCenter Server が正常に登録されていることを確認する

- **[登録状態]** : “登録済み”となっていることを確認
- **[接続状態]** : “稼働中” となっていることを確認

2-3-4. NSX ファブリック設定 – トランスポートゾーンの設定

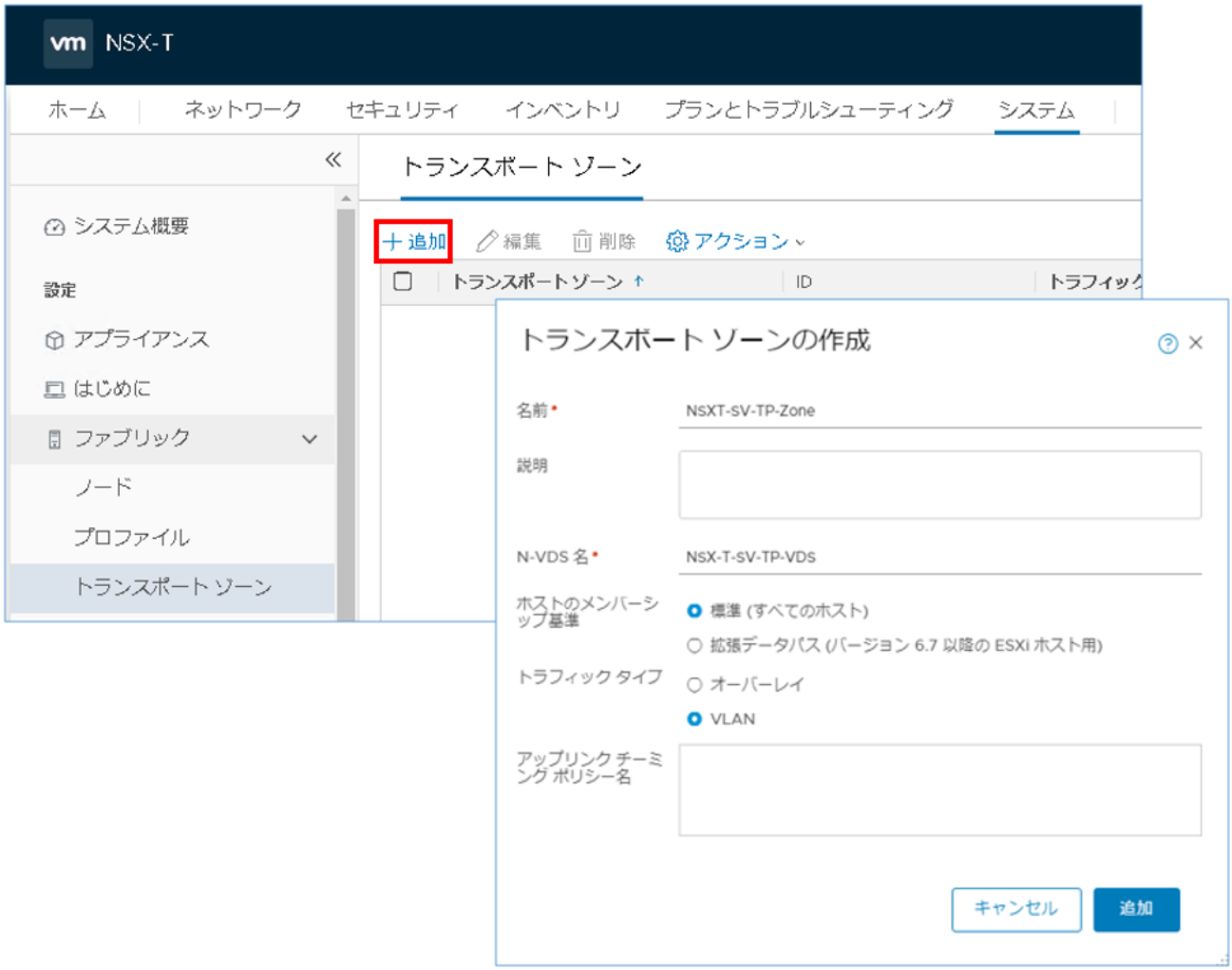
DSVA で保護を行う仮想マシンが展開される ESXi ホスト及びホスト上のネットワークを指定するための“トランスポートゾーン“を設定します。（すでに設定されている場合はスキップしてください。）

“トランスポートゾーン”は、vCenter Server 上のクラスタとは別の概念として設定されますが、ESXi ホストに展開される仮想マシンは vCenter Server で規定されるクラスタ・リソースプールに応じて vMotion/DRS が実行されることになります。DSVA によるセキュリティを担保するためには vCenter Server で規定されているクラスタに所属する ESXi ホストの範囲と同一となるように“トランスポートゾーン”を規定することを推奨します。



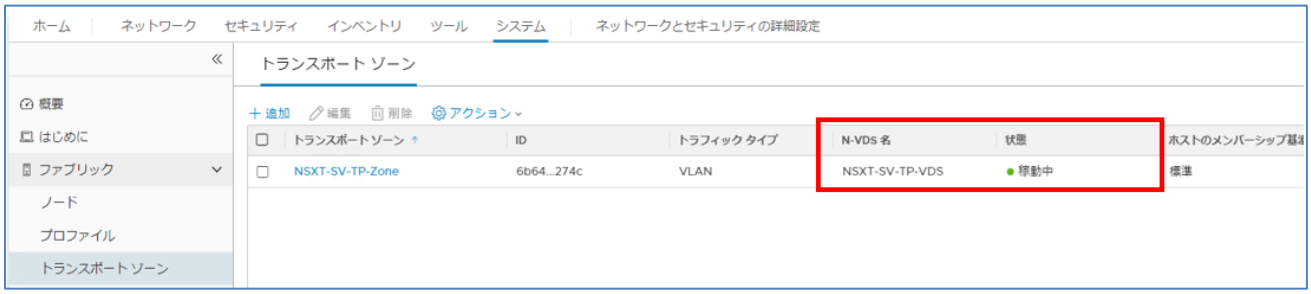
1) NSX Manager にアクセスをして

*[システム]>[ファブリック]>[トランスポート ゾーン]*を選択して、*[追加]*を選択する



- **[名前]** : トランスポートゾーン名を設定
- **[接続状態]** : N-VDS 名を設定
- **[ホストのメンバーシップ基準]** : “標準(すべてのホスト)”または“拡張データパス”を構成に従って選択
- **[トランスポートタイプ]** : **“オーバーレイ”または“VLAN”を構成に従って選択**

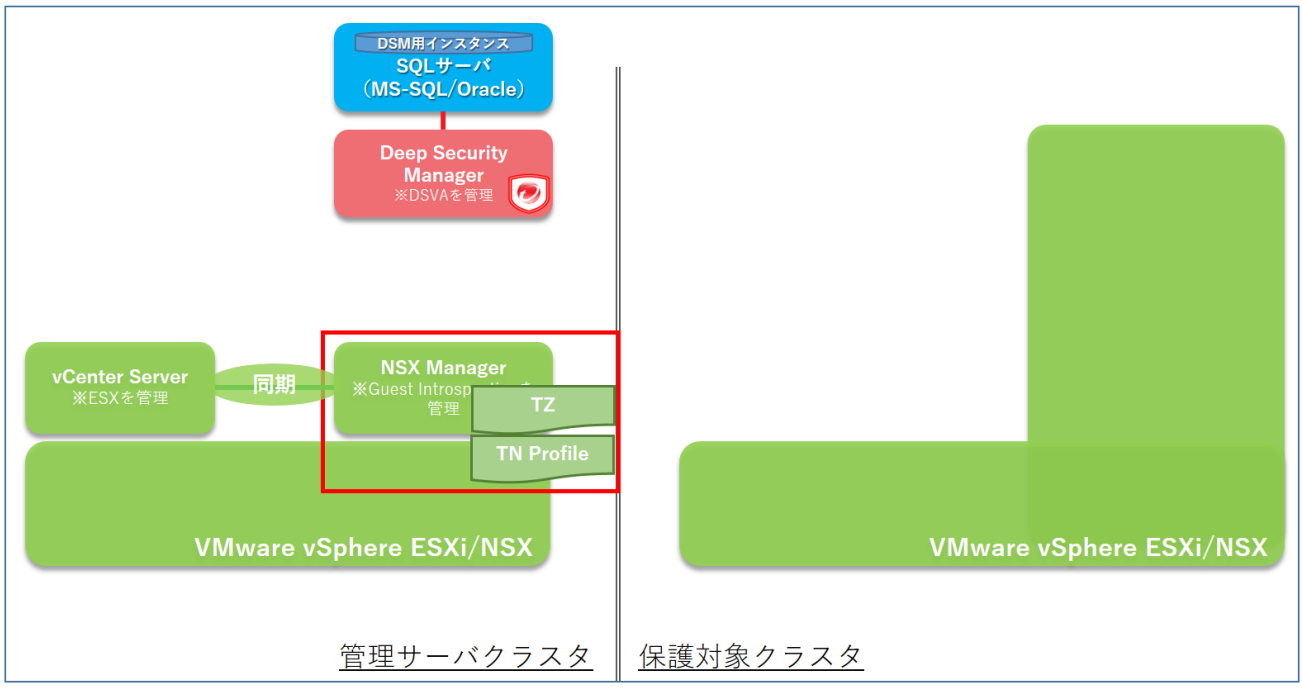
2) 設定したトランスポート ゾーンが正しく指定されていることを確認する



- **[N-VDS 名]** : 設定した N-VDS 名が指定されていることを確認
- **[状態]** : “稼働中” となっていることを確認

2-3-5. NSX ファブリック設定 – トランスポートノードプロファイルの設定

DSVA で保護を行う仮想マシンが展開される ESXi ホスト上のネットワーク設定するために、トランスポートゾーンプロファイルを設定する必要があります。(すでに設定されている場合はスキップしてください。)



1) NSX Manager にアクセスをして

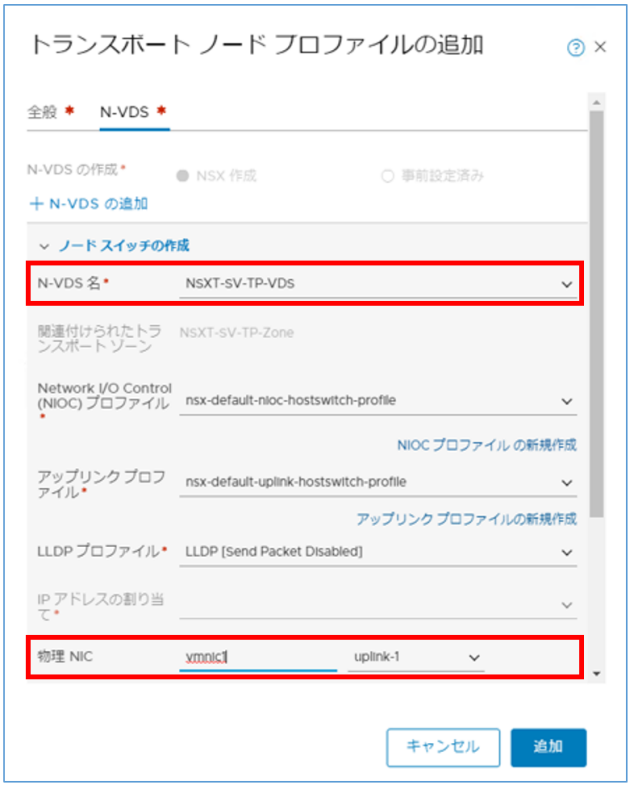
*[システム]>[ファブリック]>[プロファイル]>[トランスポート ノード プロファイル]*を選択して、

*[追加]*を選択する

2) *[全般]*タブでトランスポートノードの概要設定を行う

- **[名前]** : プロファイル名を指定
- **[トランスポートゾーン]** : 先ほど作成したトランスポートゾーンを選択

3) *[詳細]*タブでトランスポートノードに展開する N-VDS のプロファイル設定を行う



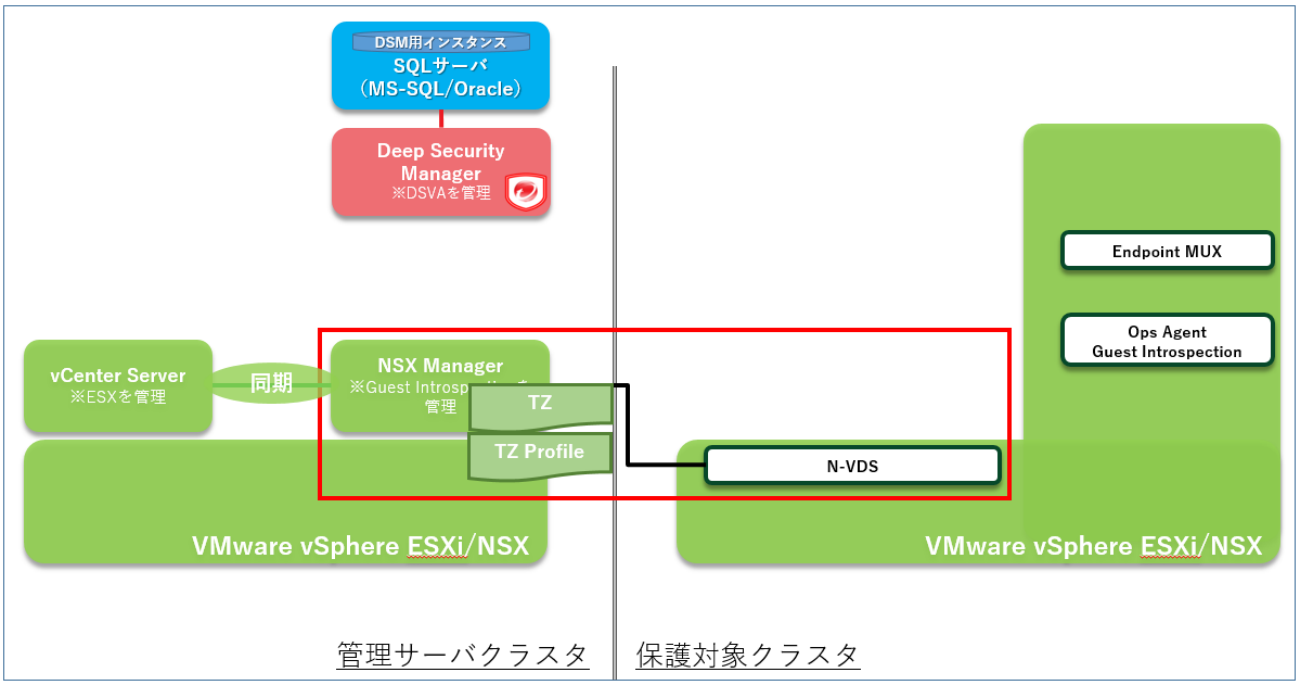
- **[N-VDS 名]** ： 2.3.4 のトランスポートゾーンの設定で指定した N-VDS 名を設定
- **[NIOC プロファイル]** ： "nsx-default-nioc-hostswitch-profile"を選択
- **[アップリンク プロファイル]** ： "nsx-default-uplink-hostswitch-profile" を選択
- **[LLDP プロファイル]** ： "LLDP [Send Packet Enabled]"を選択
- **[IP アドレスの割り当て** ：必要に応じて"IP プールを使用" or "DHCP を使用"を選択
  [IP プールを使用] が表示されている場合は、
  [新規 IP プールの作成と仕様] をクリックし、DSVA 用の IP プールを作成して、それを [IP プール] の値として使用します。
- **[物理 NIC]** ： 展開する ESXi ホストの環境に応じてアップリンクポートを指定

※プロファイル情報を含めて構築されている環境に応じて、適切なパラメータを設定してください。

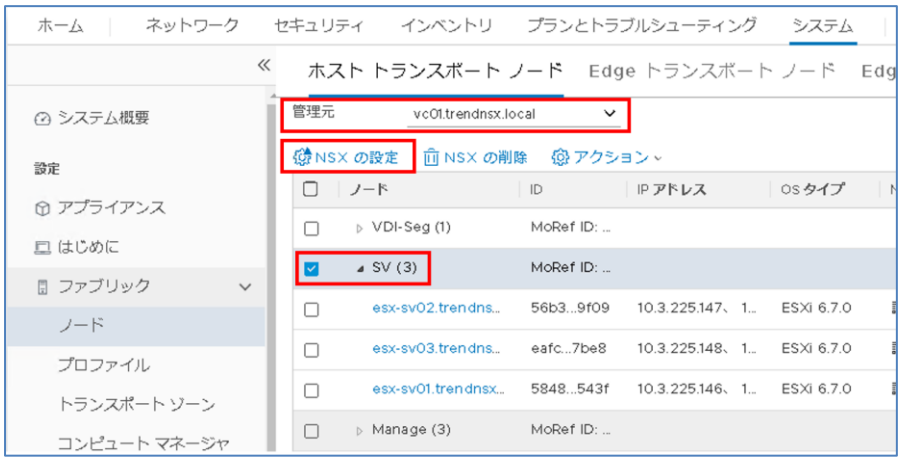
4) トランスポートノードプロファイルが作成されていることを確認する

2-3-6. NSX ファブリック設定 – トランスポートノードプロファイルの vSphere クラスタへの適用

トランスポートノードプロファイルを DSVA が展開される ESXi ホスト（vCenter Server 上のクラスタ単位で指定）に対して適用します。

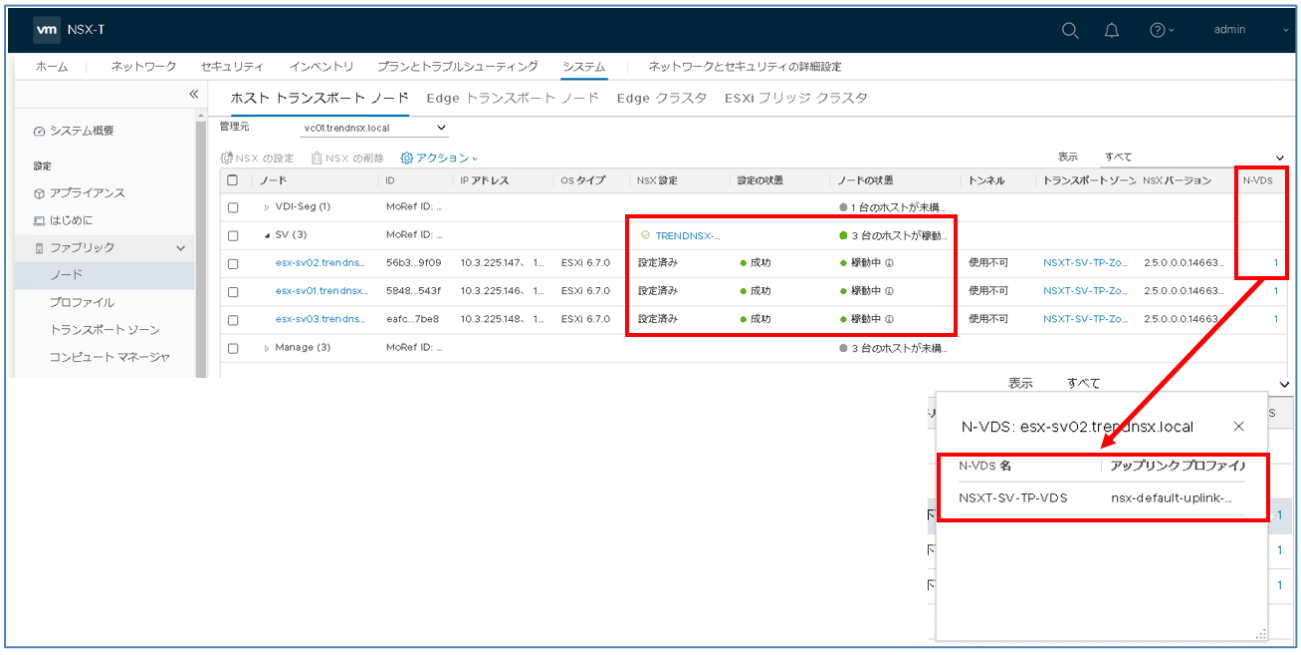


1) *[システム]>[ファブリック]>[ノード]>[ホストトランスポートノード]*から*[管理元]*から登録した vCenter Server を選択
NSX を展開するクラスタを選択して*[NSX の設定]*を選択



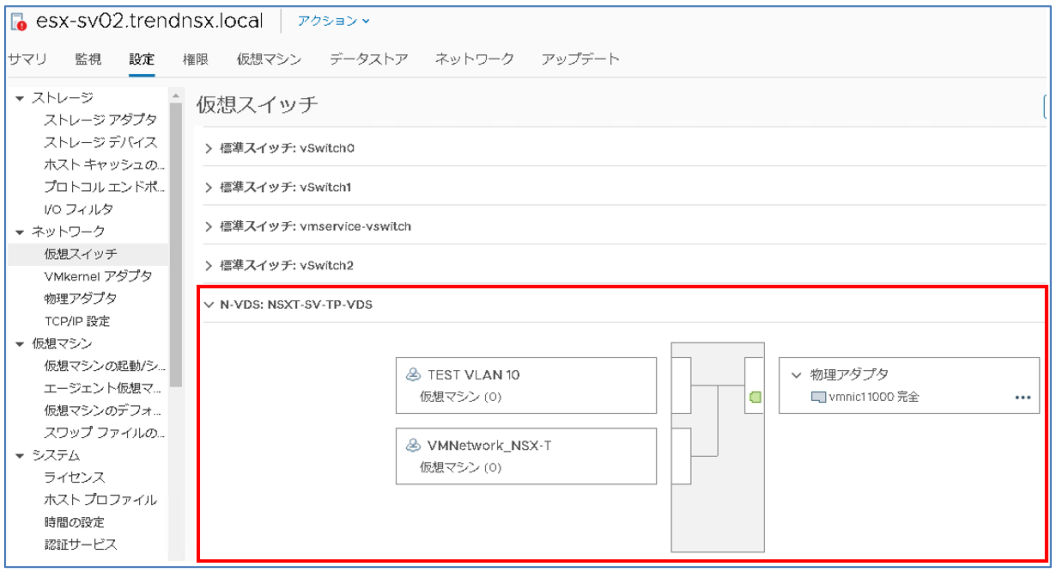
2) 先ほど設定したトランスポートノードプロファイルを展開プロファイルとして選択して保存をする

3) 配信先のクラスタに対してトランスポートノードプロファイルが正常に展開されているかを確認する



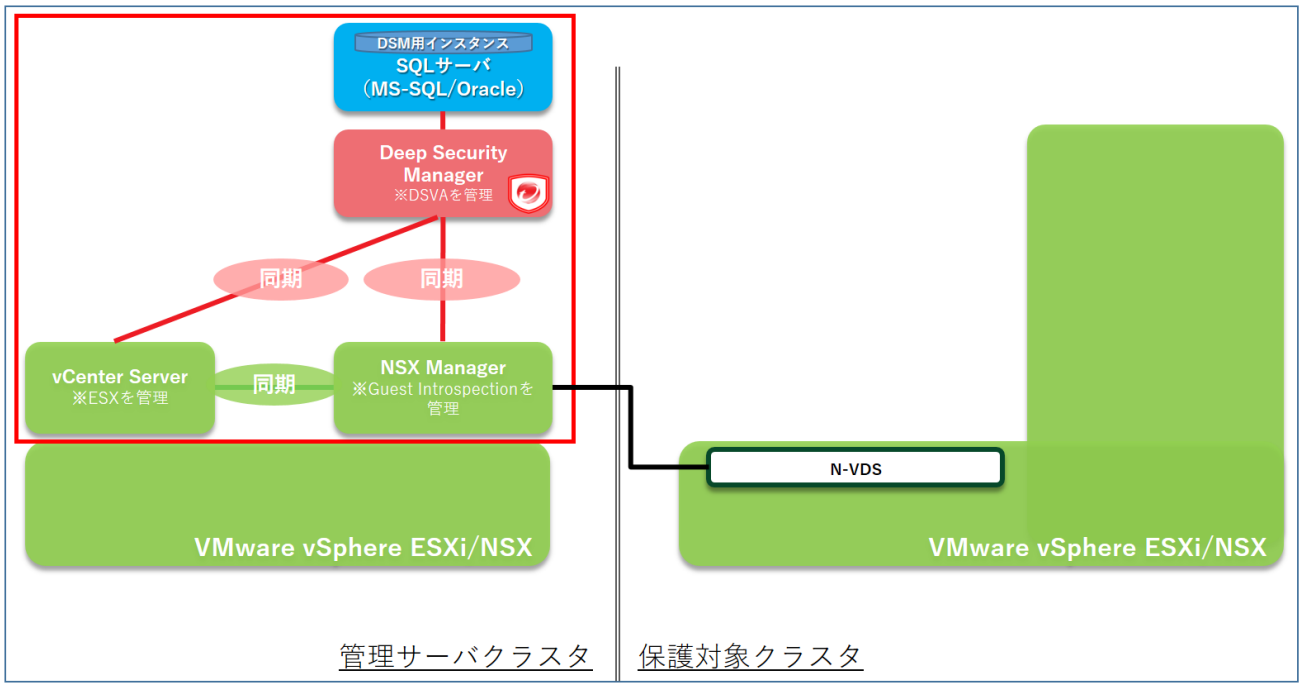
- **[NSX 設定]** ：クラスタに対して適用したトランスポートノードプロファイルが適用されており、
  “x台のホストが稼働中”となっていることを確認
  また、各ホストでは“設定済み”となっていることも確認
- **[設定の状態]** ： 各ホストの状態が“成功”となっていることを確認
- **[ノードの状態]** ： 各ホストの状態が“稼働中”となっていることを確認
- **[N-VDS]** ： トランスポートノードプロファイルで指定した N-VDS の展開を確認する

また、vCenter Server 上でも各ホスト上で N-VDS が展開されていることを確認する



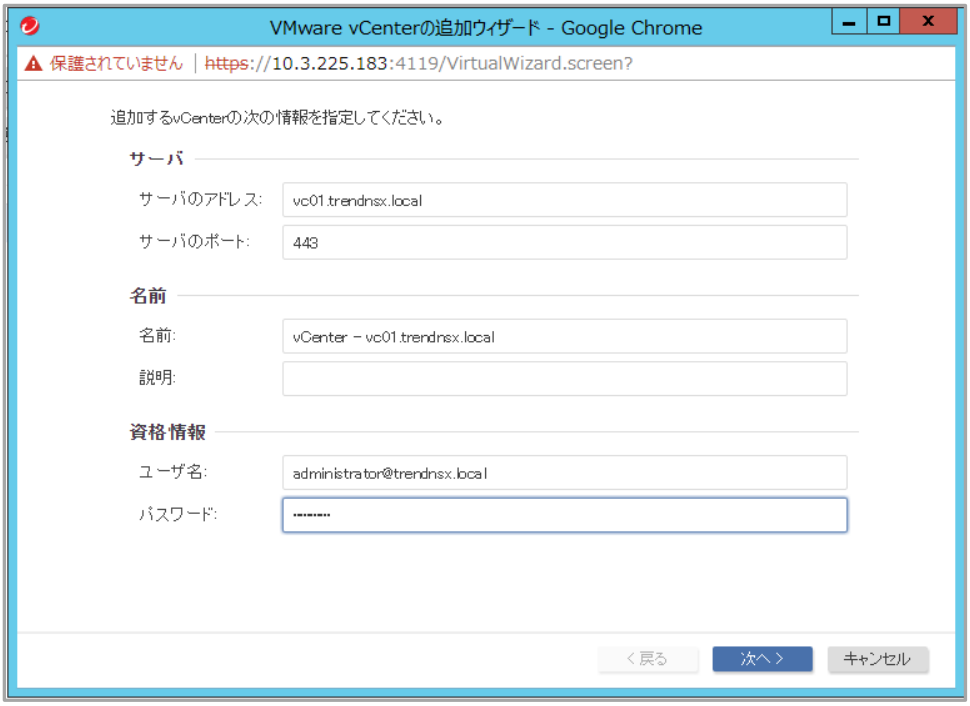
2-3-7. DSM＆vCenter Server・NSX Manager 連携設定

DSM にてvCenter Server 及び NSX Manager の連携設定を行い、インベントリ情報/セキュリティポリシーの同期、DSVA のデプロイが行えるようにします。



1) **[コンピュータ]**タブから右側ペインの**[コンピュータ]**を右クリックして、**[VMware vCenter の追加]**を選択する

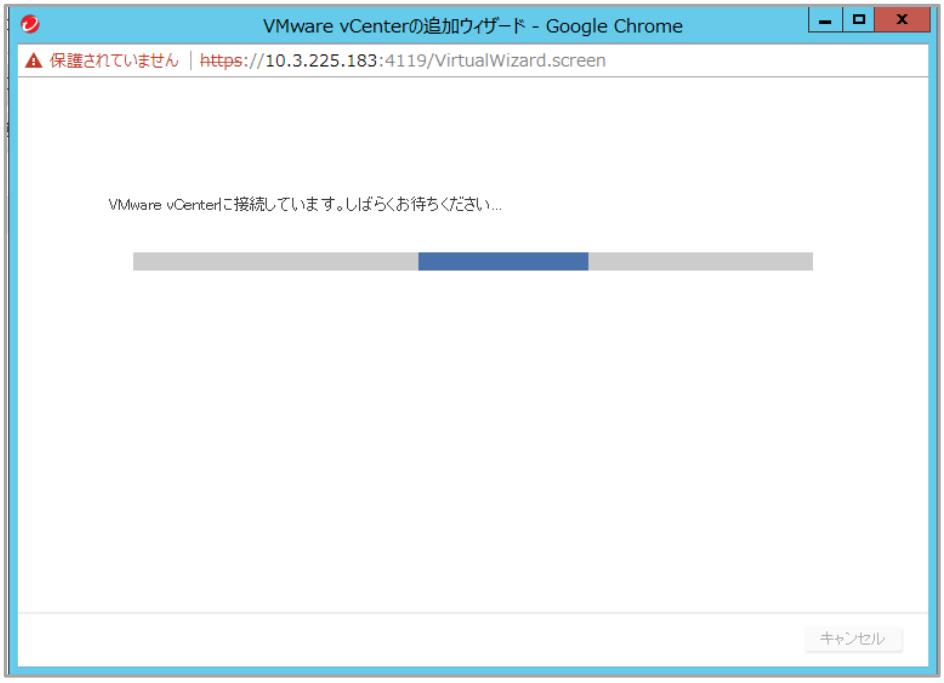
2) 接続する vCenter Server の情報を設定する



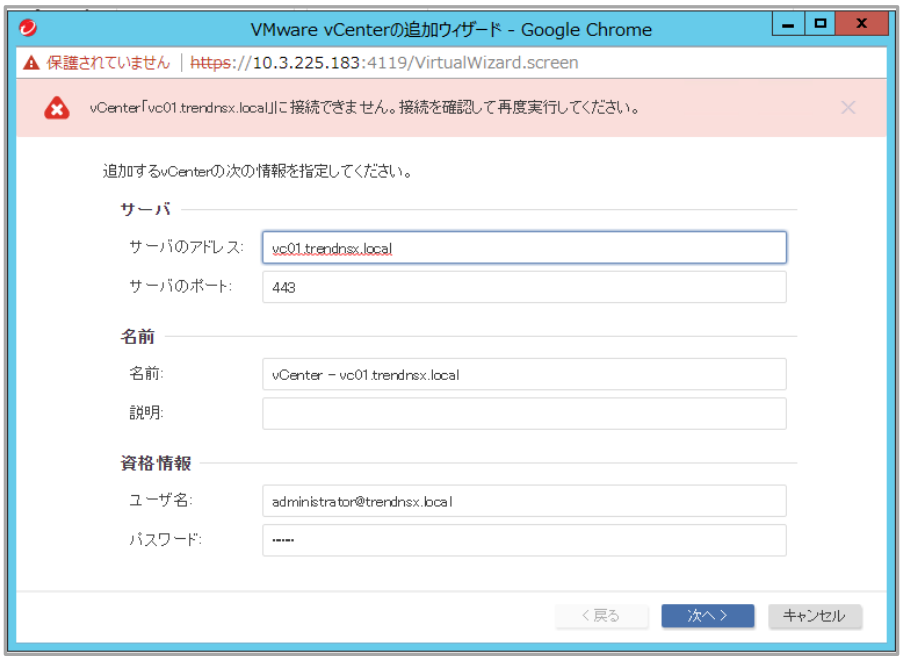
- **[サーバのアドレス]** : vCenter Server サーバ名
- **[サーバのポート]** : 443
- **[ユーザ名]** : 管理者権限を持ったユーザ名
- **[パスワード]** : パスワード

3) *[次へ]*を押して、vCenter Server の接続を確認する

SSL 証明書を受け入れるかどうかの確認があった場合には*[受け入れる]*を選択します。



※vCenter Server へのアクセスができない場合には、以下のようなエラーメッセージが表示されるため、vCenter Server へのアクセス情報を再確認します。



4) 接続する NSX Manager の情報を設定する

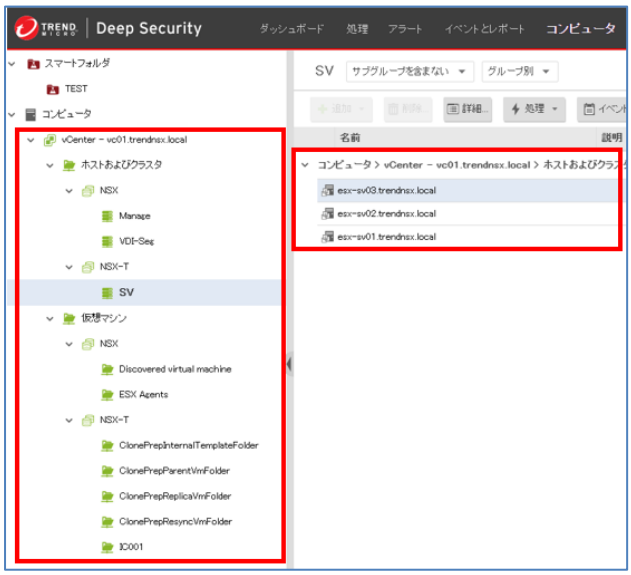
本番環境においては、NSX Manager は 3 台構成にすることを構成要件となっています。vCenter Server から設定する NSX Manager については NSX Manager で設定している Cluster VIP を必ず指定してください。

- **[Manager のアドレス]** : NSX Manager サーバ名
- **[Manager のポート]** : 443
- **[ユーザ名]** : NSX Manager 管理者権限を持ったユーザ名
- **[パスワード]** : パスワード

5) ***[次へ]***を押して、NSX Manager の接続を確認する

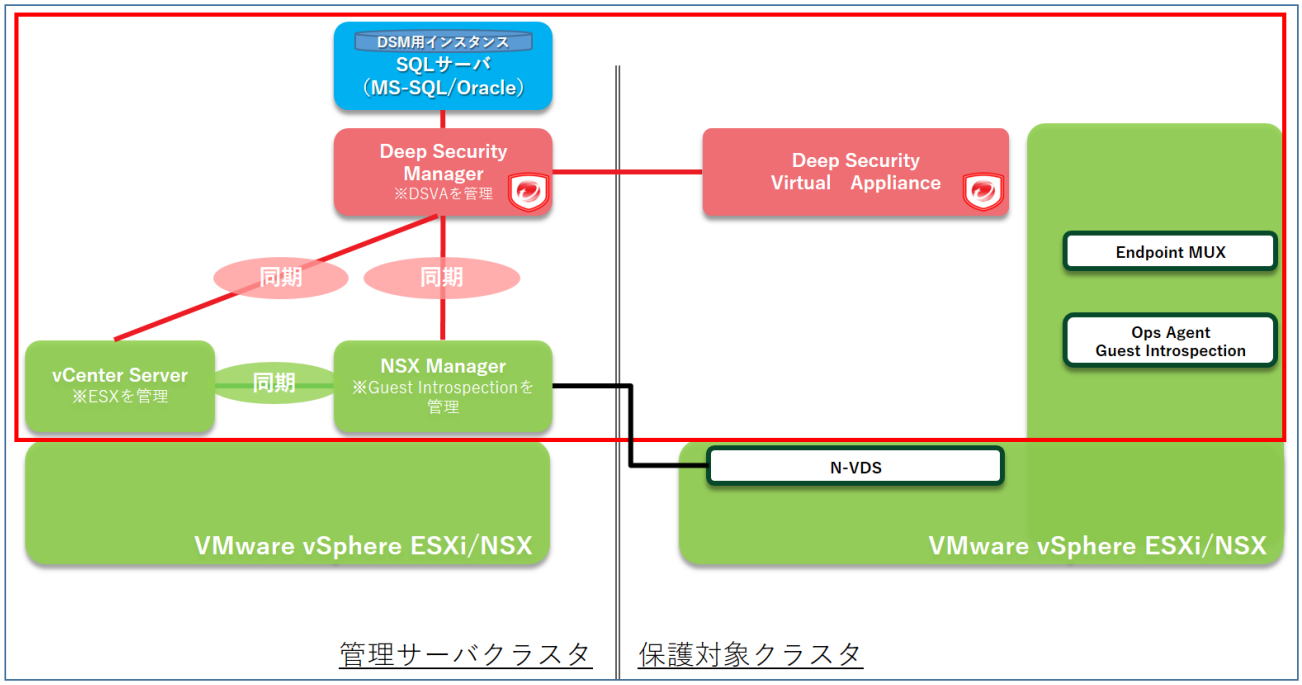
SSL 証明書を受け入れるかどうかの確認があった場合には***[受け入れる]***を選択します。

6) ***[コンピュータ]***タブで右側ペインに vCenter Server のインベントリ情報が連携されていることを確認する



2-3-8. DSVA デプロイ

保護対象クラスタの各 ESXi ホストに対して DSVA を配信します。



NSX 環境においては、DSVA は NSX Manager からデプロイを行います。NSX Manager 経由で DSM または指定された外部 Web サーバに格納されるソフトウェアパッケージに含まれる OVF ファイルを指定して、各 ESXi ホストに対するデプロイを行う仕様となっています。
DSM を vCenter Server・NSX Manager と連携することにより、DSM ローカルに配置される DSVA ソフトウェアパッケージの URL(デフォルト)または、任意に指定した外部 Web サーバの DSVA ソフトウェアパッケージの URL が NSX Manager にリアルタイムに通知され、DSVA デプロイ時に使用する OVF URL が自動的に指定されます。

DSVA は NSX に管理されたセキュリティ VM として ESX Agent Manager(EAM)に管理されたセキュリティアプライアンスとして扱われます。EAM により管理されたセキュリティ VM は、NSX Manager が vCenter Server 上で配信対象のクラスタの配下に生成する“ESX Agents”フォルダの配下に配置されます。

➢ **DSVA ソフトウェアパッケージとデプロイに必要なコンポーネント**

DSVA のメジャーリリース(Long Term Support)毎に GM(初期リリース)版 OVF がリリースされます。メジャーリリースで適宜リリースされる Update については、Redhat(64bit)版 DSA を利用してアップデートしたい Appliance バージョンのアップデートを行います。
(実際は、DSVA ソフトウェアパッケージと該当の DSA を DSM ローカルにダウンロードしておくことで、NSX からの“デプロイ”時に自動的に実行されます。)
※仕様変更などにより GM 以外でもメジャーリリース中に DSVA ソフトウェアパッケージがリリースされることがあります。できる限り最新のソフトウェアパッケージを利用することを推奨します。
(以下は 2019 年 12 月末時点の DS12.0 DSVA ソフトウェアパッケージ)

Appliance

ソフトウェア	リリースの種類	ビルド	リリース詳細	リリース日	ダウンロード
Deep Security Appliance 12.0.0-682 for ESX-x86_64 (12 LTS Update 3)	LTS	12.0.0-682	LTS	Dec 5, 2019	
Deep Security Appliance 12.0.0-364 for ESX-x86_64 (12 LTS)	LTS	12.0.0-364	GA	Jun 19, 2019	

DSVA の配信にあたっては、以下のコンポーネントを事前に DSM へアップロードされている必要があります。

【DS12.0】

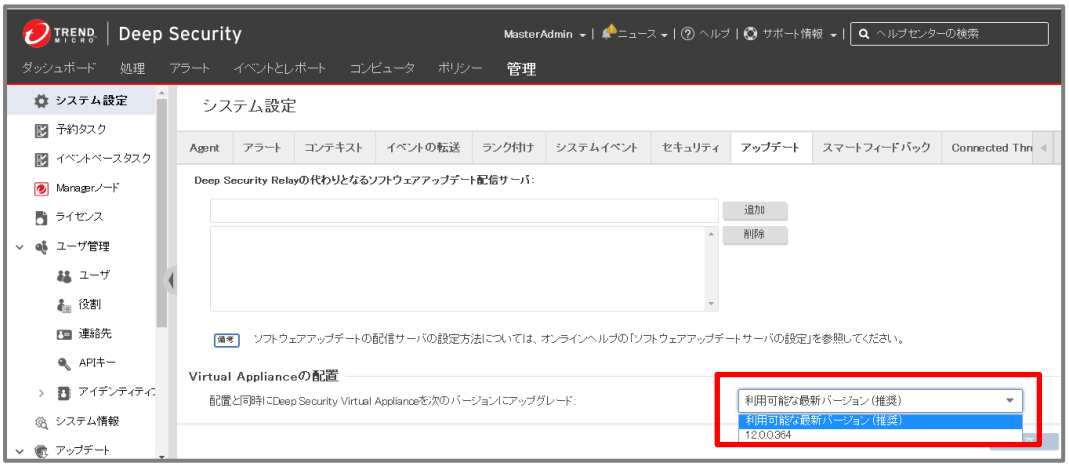
DSM に以下の 2 つのコンポーネントをアップロードして、NSX から配信

- Deep Security Appliance 12.0.0-XXX for ESX-x86_64 (12 LTS Update 3)
  “Appliance-ESX-12.0.0-XXX.x86_64.zip”(XXX はビルド番号)
- RHEL 7 (x64) 用 Deep Security Agent

実際に配信したい Appliance バージョンについては、以下の設定画面から指定することが可能です。

(プルダウンには、DSM ローカルにアップロードした Appliance OVF と RHEL7 (x64) 用 Deep Security Agent のバージョンにより指定可能な DSVA 配信バージョンが表示されます。

[管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]



➢ デプロイする DSVA のリソース設定

NSX-T2.4 までは、DSM へ DSVA OVF をアップロード後、DSM インストールフォルダ配下の以下のフォルダに格納される dsva.ovf ファイルの中の以下のパラメータを修正することで変更が可能です。

<DSM_Install>¥temp¥Appliance-ESX-<appliance_version>

```
<Item>
  <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
  <rasd:Description>Number of virtual CPUs</rasd:Description>
  <rasd:ElementName xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">4 virtual CPU</rasd:ElementN
  <rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">1</rasd:InstanceID>
  <rasd:ResourceType>3</rasd:ResourceType>
  <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
</Item>
<Item>
  <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
  <rasd:Description>Memory Size</rasd:Description>
  <rasd:ElementName xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">6144 MB of memory</rasd:Elem
  <rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">2</rasd:InstanceID>
  <rasd:Reservation>6144</rasd:Reservation>
  <rasd:ResourceType>4</rasd:ResourceType>
  <rasd:VirtualQuantity>6144</rasd:VirtualQuantity>
</Item>
```

NSX-T2.5 以降の環境では、セクション 1.4.6 で記載の通り、NSX の仕様の変更に伴い、DSVA など 3rd Party Security VM を各ホストへデプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチェックを実行するプロセスが追加されています（ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署名が付与されます）。
NSX-T2.5 以降では、VMware 社によるデジタル署名が付与されている Deep Security 12.0 Update 3 以降の OVF パッケージを必ず使用する必要があり、DSVA に割り振るリソースに応じて以下の 4 種類の OVF ファイルから選択をする必要があります。

OVF Files	vCPU	Memory
dsva.ovf	2	4096MB
dsva-small.ovf	2	8192MB
dsva-medium.ovf	4	16384MB
dsva-large.ovf	6	24576MB

NSX-T2.5.0 以降の環境での DSVA ソフトウェアパッケージの扱い、デプロイの方法の詳細は**セクション 1.4.6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更** を参照してください。

1) NSX Manager にアクセスし、*[システム]＞[サービス展開]＞[展開]*を選択し、セキュリティ VM を新規にデプロイする設定を行う

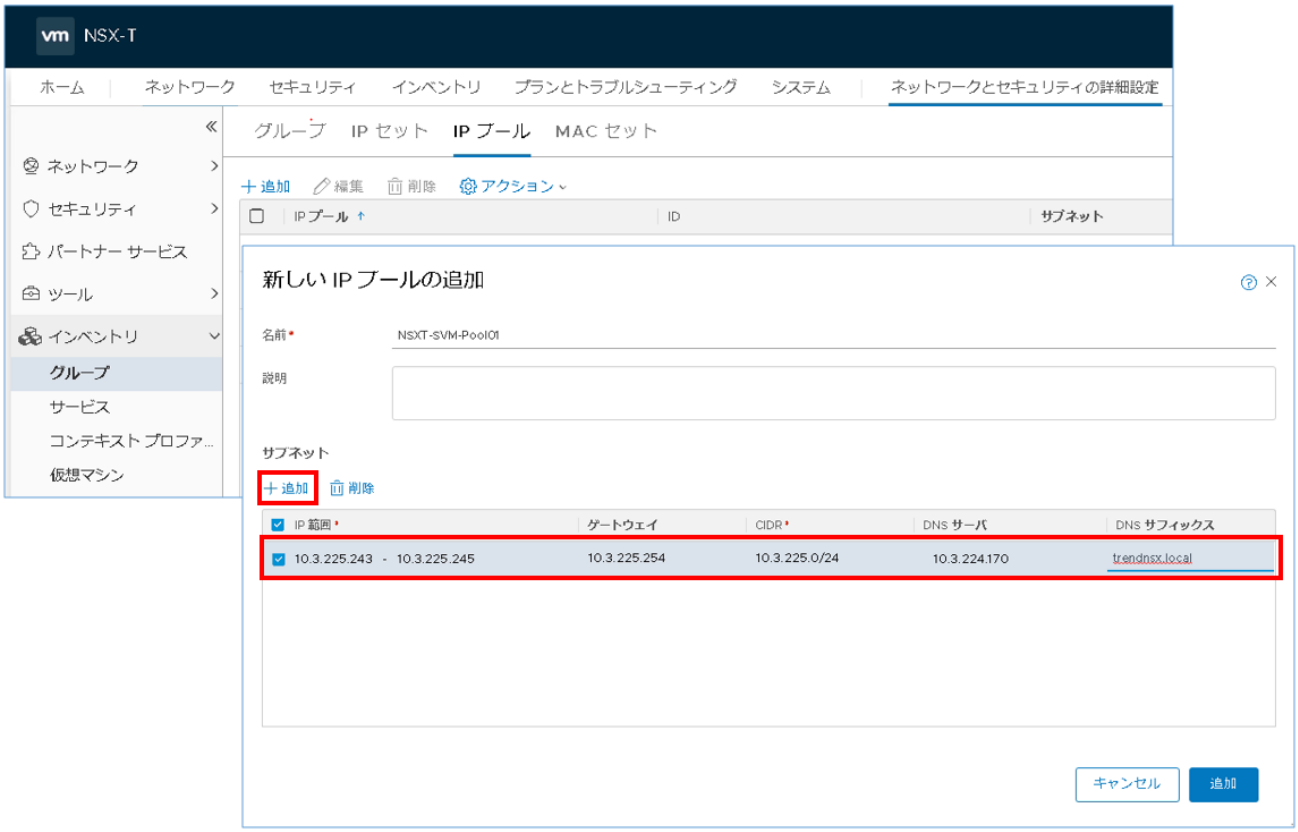
配信するセキュリティ VM をパートナーサービスから選択を行い、[DEPLOY SERVICE]を選択

- **[パートナーサービス]** ： **プルダウンから”Trend Micro Deep Security”を選択**

展開する DSVA の基本設定（vCenter Server 上の配信先のクラスタ、配信するデータストア、DSVA の管理ポートが所属するネットワーク、配信する DSVA の仕様など）を選択する

- **[サービス展開名]** ： 任意の名称を設定
- **[コンピュート マネージャ]** ： DSVA を配信するクラスタが所属する vCenter Server を指定
- **[クラスタ]** ： DSVA を配信するクラスタを指定
- **[データ ストア]** ： DSVA を配信するデータストアを指定。“ホストで指定済み”または任意のストレージデータストア
- **[ネットワーク]** ： “詳細の編集”を選択“IP Pool”（推奨）または“DHCP”を選択

① IP プールを利用する場合で IP プールの設定がされていない場合には、“IP プールの管理”を選択して、*[ネットワークとセキュリティの詳細設定]>[インベントリ]>[グループ]>[IP プール]*へ移動
*[追加]*ボタンを押して、“新しい IP プールの追加”を行う



- **[IP 範囲]** : DSVA に設定する管理 IP の範囲を指定
  （最低 DSVA を配信する ESXi ホスト数を設定）
- **[ゲートウェイ]** : DSVA に設定するデフォルトゲートウェイを設定
- **[CIDR]** : DSVA の管理 IP が所属するサブネットを CIDR 形式で設定
  （例） 10.3.225.0/24
- **[DNS サーバ]** : DSVA が参照するローカル DNS サーバを設定
- **[DNS サフィックス]** : DNS サーバで指定しているドメインを設定

② IP プールが正しく設定されていることを確認する

[TIPS]

DSVA を配信するデータストア、ネットワークがプルダウンから表示されない場合には、vCenter Server にて配信先のホストの***[設定]>[仮想マシン]>[エージェント仮想マシンの設定]***からデプロイしたいデータストア、ネットワークを指定する必要があります（このパラメータが NULL/空欄の場合には DSVA のデプロイに失敗します）。

2) すべての設定が終わったら***[保存]***ボタンを選択して、DSVA のデプロイを開始する

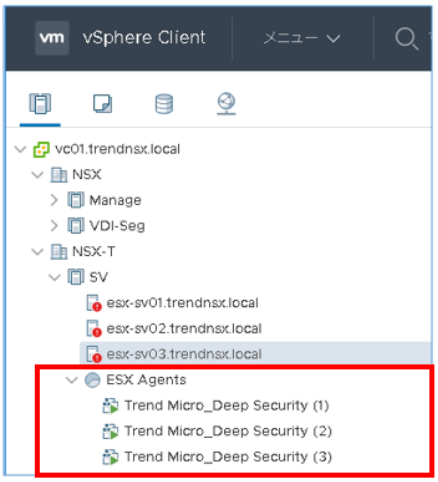
- デプロイの状態が“進行中”になっていることを確認して、デプロイの完了を待つ（数分かかります。適宜 Web Client GUI のリロードを行って状態を確認してください。）

- 進行中の状態にならず、配信が失敗する場合には NSX Manager が正しく DSVA のソフトウェアパッケージが認識できない、またはデプロイに必要なパラメータに不足または修正が必要な状態であると考えられるため、エラー状態の確認・修正の上、DSVA を再度デプロイする必要があります。

3) DSVA が正常にデプロイされたことを確認する

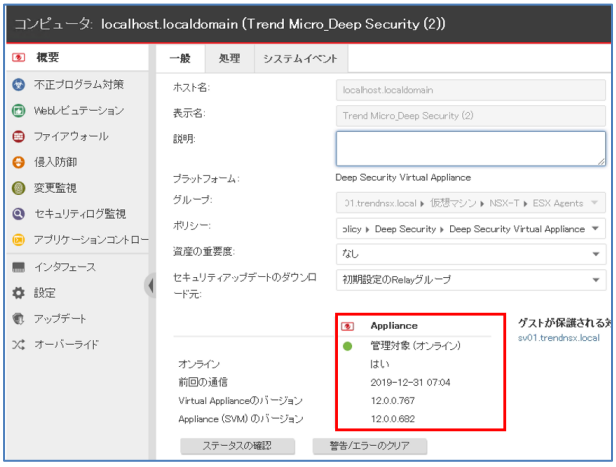
- **［状態］** ： 稼働中

また、該当クラスタ配下の[ESX Agents]に対象となる ESXi ホスト台数分の DSVA が配信されていることを確認してください。



合わせて、DSM 上で DSVA の“ステータス”が“管理対象（オンライン）”になっていることを確認する必要があります。

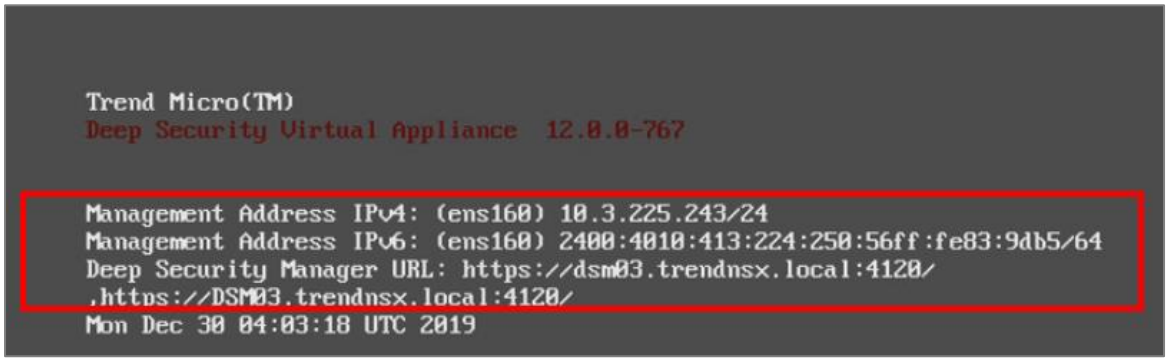
また、DSVA の**“Virtual Appliance のバージョン”**が **“DSVA ソフトウェアパッケージとデプロイに必要なコンポーネント”で前述をした*[管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]***で指定したバージョンと同じバージョンとなっていることを確認します。**“Appliance（SVM）のバージョン”**と同じままの場合などには、DSVA がセキュリティ VM としては配信されているものの、適切なバージョンにアップデートされていないものと考えられるため、DSA パッケージが正常にダウンロードできる状態になっているか、DSM と DSVA が適切に通信できているかどうかを確認する必要があります。



DSVA のステータスが“管理対象(オンライン)”とならず、何らかのエラーが発生している場合には、以下のような原因が考えられます(これ以外の原因がある場合も考えられます)。適切なシステム環境となっていることを確認して、一旦 DSVA のデプロイを解除(削除)を行い、再度デプロイを設定する必要があります。

- DSVA のデプロイに必要な適切なソフトウェアパッケージが DSM または外部 Web サーバにインポートされていない
- DSVA の管理 IP が DSM と正常に通信するために必要なネットワークの設定または IP プールまたは DHCP で割り当てたネットワークレンジ、デフォルトゲートウェイ、DNS サーバなどの設定に不備がある
- DSM と DSVA 間で適切なファイアウォールルールの開放または適切な DNS 名前解決ができない
- 上記の要因などにより DSVA が正しく DSM を認識できていない

vCenter Server から DSVA に対して Web コンソールでアクセスした際のトップ画面で下記のように DSM の情報が常時されず、何も表示されない場合には、DSVA は正しくデプロイされていない状態となります。また、合わせて割り当てたネットワークレンジから DSVA の管理 IP が割り振られていることも確認してください。



2-3-9. Deep Security 基本設定とセキュリティポリシーの策定

DSM から Deep Security を運用する上で必要な基本設定およびセキュリティポリシーの策定を行います。

- **Relay グループの設定の確認**

  デフォルトでは DSM は、インストール時に生成される***[初期設定の Relay グループ]***に所属します。通常は、***[初期設定の Relay グループ]***を利用することで問題はありません。

[初期設定の Relay グループ]に DSR となるサーバが一台も所属していない状態の場合には、***[新規 Relay グループ...]***から DSR とする DSA サーバを指定する必要があります。通常は DSM サーバに DSA をインストールして DSR として導入してください。

Relay を多段構成で構成したい場合などには Relay グループを追加で設定することが可能です。
詳細は以下のヘルプセンターの情報を参照してください。
https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/Set-Up-Relays.html?redirected=true&Highlight=Relay
また、DSM がインターネットに接続できないオフライン環境でアップデートを行う方法については以下の FAQ を参照して運用方法を検討ください。
https://success.trendmicro.com/jp/solution/1096762

- **予約タスクの設定**

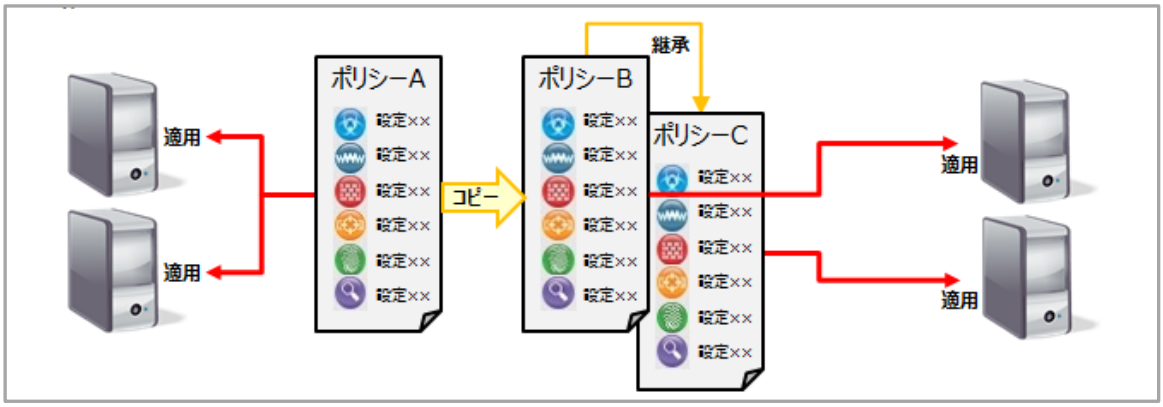
必要に応じて、定期的に実行するタスクを設定することができます。セキュリティの観点から最低限以下の予約タスクが設定されているかを確認し、設定されていない場合は予約タスクの新規作成を行ってください。また、適宜、タスクの実行間隔、実行するコンピュータの調整をしてください。(以下の 2 つの予約タスクはインストール時に自動的に設定されています。)

- セキュリティアップデートの確認
- ソフトウェアアップデート確認

また、不正プログラム対策で予約検索を行う場合には、[コンピュータの不正プログラムを検索]も設定する必要があります。
詳細は以下のヘルプセンターの情報を参照してください。
https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/scheduled-tasks.html

- **Deep Security セキュリティポリシーの作成**

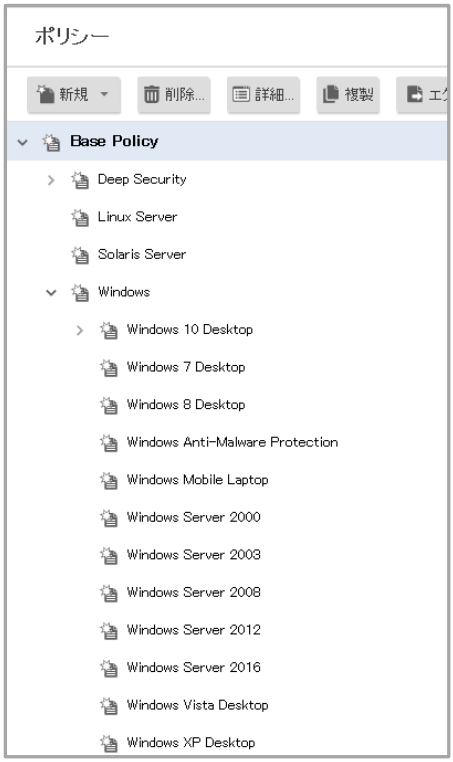
Deep Security の各機能では詳細な設定が可能です。
それらの設定を、保護対象のコンピュータに個別に設定するのではなく、まずは設定をセットにした「ポリシー」を作成し、コンピュータに対してはどのポリシーで保護するのかを選択して適用します。
ポリシー作成は、新規作成することも、既存のポリシーをコピーして部分的に修正することも可能です。また、「継承」オプションを利用することにより親子関係のポリシーを作ることも可能です。親ポリシーを継承した子ポリシーを作成した場合、親ポリシーの変更は子ポリシーにも自動的に反映されます。また、子ポリシーにて個別設定を行った場合には、該当の設定項目だけが変更(継承から除外される)されて、それ以外の設定項目は親ポリシーに準じる、といった柔軟なセキュリティポリシーの適用が可能となります。



➢ 継承に関する詳細は以下のヘプルセンターを参照してください。

https://help.deepsecurity.trendmicro.com/ja-jp/policies-inheritance-overrides.html

Deep Security では、予めいくつかのポリシーがプリセットされています。
ポリシーは新規に 1 から作成することもできますが、OS 毎にトレンドマイクロが定義したポリシーをベースに個別にカスタマイズをすることも可能です。



仮想デスクトップとして利用する仮想マシンを保護する場合には、以下の点を参考にポリシー作成をしてみてください。（以下の内容によって必ずしもセキュリティリスクのすべてを回避できるわけではないことを予めご了承ください。）

- 不正プログラム対策を有効にしてください。
- 不正プログラム対策の予約検索については、仮想デスクトップの展開方法、セキュリティポリシーに応じて実施の必要性の検討、実施間隔の設定を行ってください。
- Web レピュテーション、侵入防御については、NSX-T2.4 及び 2.5 環境において DSVA で提供することはできません。（2019 年 12 月現在）

サーバ OS を保護する場合には、上記に加えて Web レピュテーション、侵入防御、変更監視、セキュリティログ監視、アプリケーションコントロールなどの機能を DSA で併用して適用することを検討してください。

- 侵入防御機能については推奨設定の検索を利用することで効率的なルール運用が可能となります。推奨設定の検索の詳細については、Deep Security ヘプルセンターを参照してください。
- 変更監視、セキュリティログ監視の利用にあたっては、ルールに対してユーザ、システム固有のパラメータ設定する必要がある“設定可能ルール”（ルールマークに歯車マークがついているルール）が多く存在しま

す。ルール適用にあたっては、推奨設定の検索の利用とあわせて適用するサーバの情報を確認した上で行うことを推奨します。

- 変更監視を有効化する場合には、ベースラインの再構築、予約タスクの実行などの設定をあわせて行ってください。

本セクションでは、以下のシチュエーションを想定した設定を行っていきます。
実際の環境では、利用される環境及びセキュリティポリシーに応じて設定を行ってください。

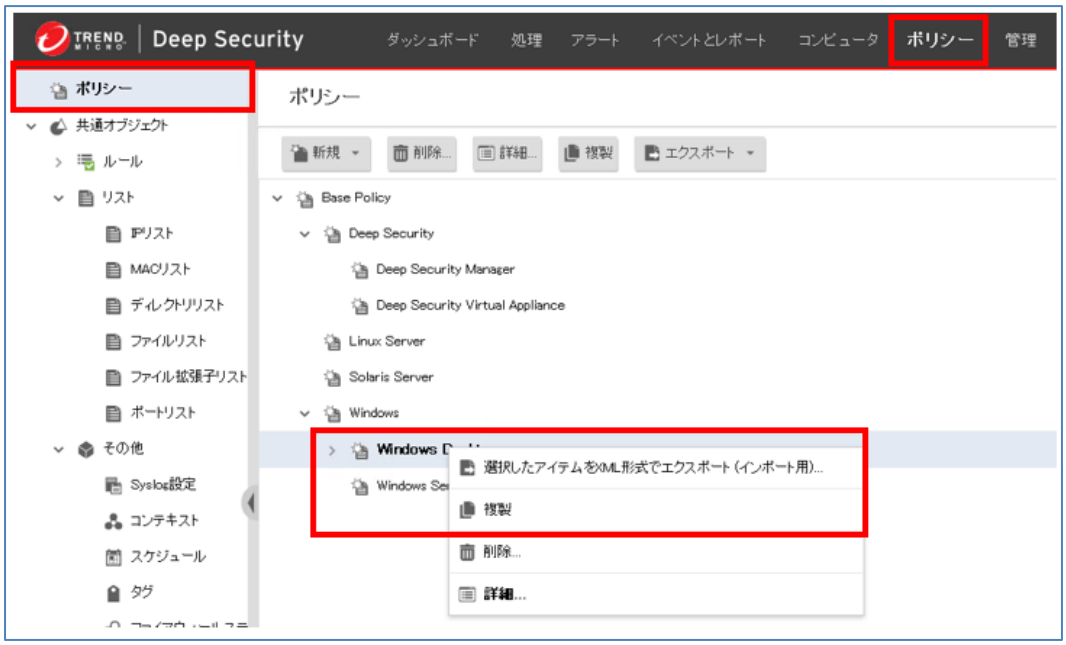
- Horizon にて仮想マシン（VDI 用 Windows クライアント）が展開される環境
- 仮想マシンに対して、Deep Security の不正プログラム対策を有効化
- Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと連携した自動隔離ができるように隔離用セキュリティグループも設定
- 不正プログラム対策イベント検出時に付与する NSX セキュリティタグを **“ANTI_VIRUS.VirusFound.threat=high”**に設定
- 本セクションでは、ポリシーを以下のとおり指定

  Deep Security セキュリティポリシー ： VDI_Windows Desktop_Demo01

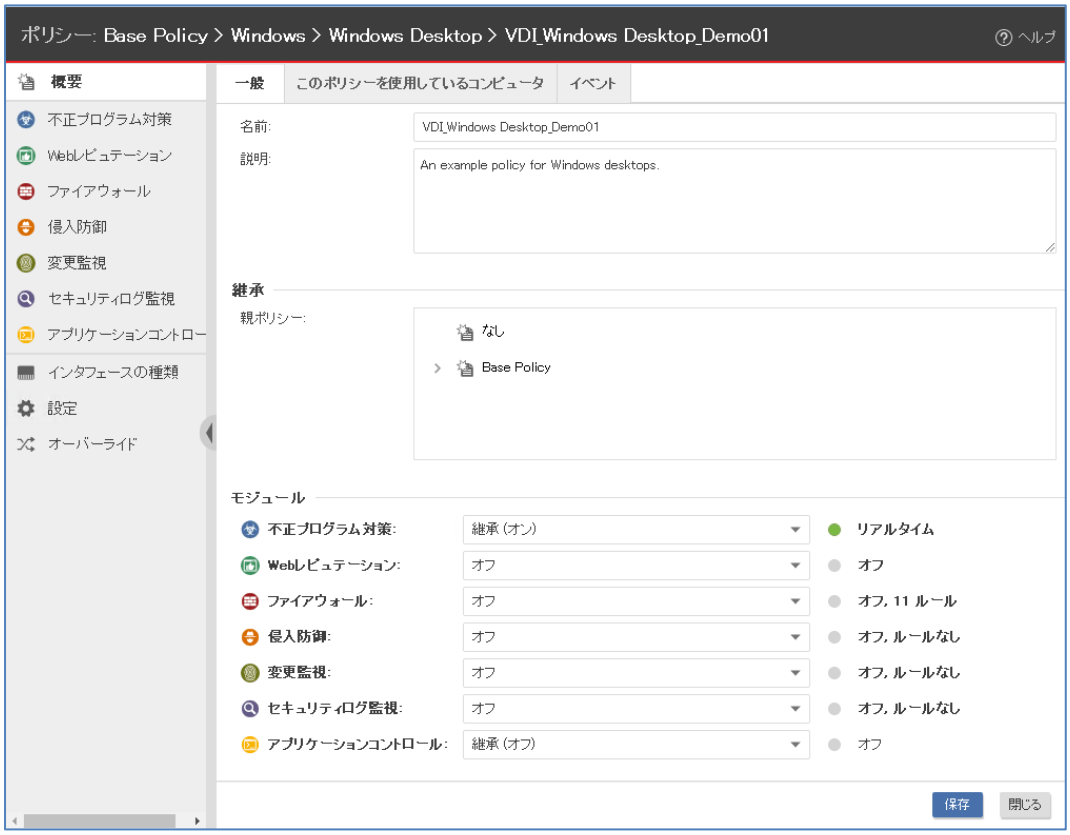
  トレンドマイクロが提供するデフォルトのポリシーである“Windows Desktop”を継承してカスタマイズし、以下の機能を有効化

  - 不正プログラム対策

1) DSM から*[ポリシー]>[ポリシー]*から定義済のポリシーである**[Windows Desktop]**を選択して、複製する



2) 複製したポリシーをカスタマイズして、保存



- **[名前]** : **VDI_Windows Desktop_Demo01**
- **[継承:親ポリシー]** : **Windows Desktop**
- **[不正プログラム対策]** : 継承(オン)

- **[Web レピュテーション]** : オフ＜変更＞
- **[ファイアウォール]** : オフ＜変更＞
- **[侵入防御]** : オフ＜変更＞
- **[変更監視]** : オフ＜変更＞
- **[セキュリティログ監視]** : オフ＜変更＞
- **[アプリケーションコントロール]** : 継承（オフ）

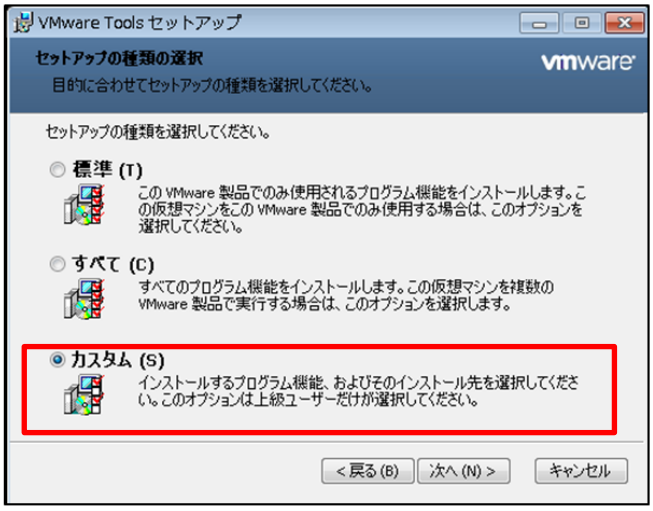
2-3-10. 保護対象仮想マシンへの VMware Tools 及び Notifier のインストール

エージェントレスによるセキュリティ機能を提供するためには、仮想マシンに VMware Tools を導入することで、仮想マシンで発生したトランザクションを ESXi ホスト経由で DSVA が受け取れる必要があります。また、エージェントが導入されないため、イベントが発生した場合に仮想マシンのユーザがそれに気づくことが困難です。仮想デスクトップなどのユーザがログインをして利用する仮想マシンについては、Trend Micro が提供する通知ツール Notifier を導入しておくことを推奨しています。

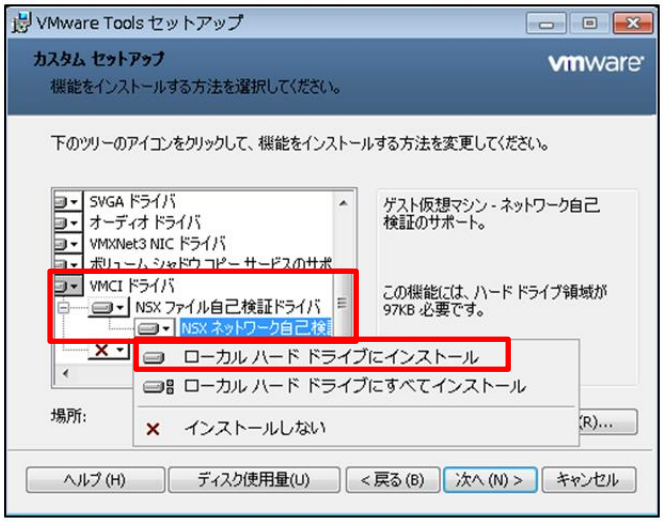
仮想デスクトップ環境においては、マスターイメージに VMware Tools、Notifier をあらかじめインストールしておくことによりスムーズな展開が可能です。

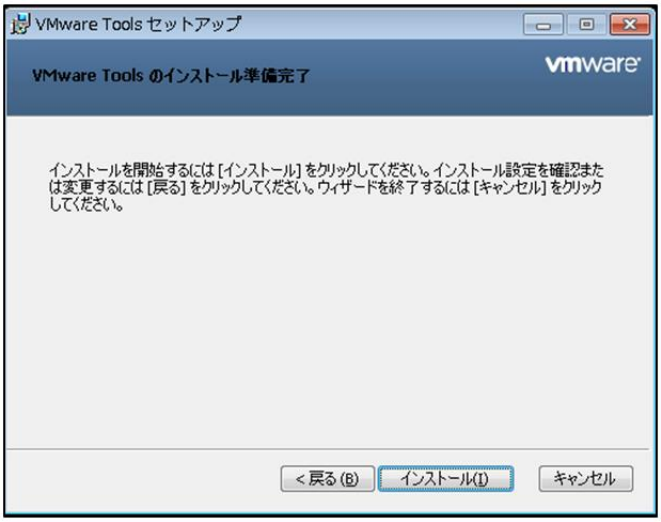
➢ **VMware Tools のインストール**

1）仮想マシン上で VMware Tools のセットアップファイルを実行し、セットアップウィザードを進める
*[セットアップの種類の選択]*で*[カスタム]*を選択する



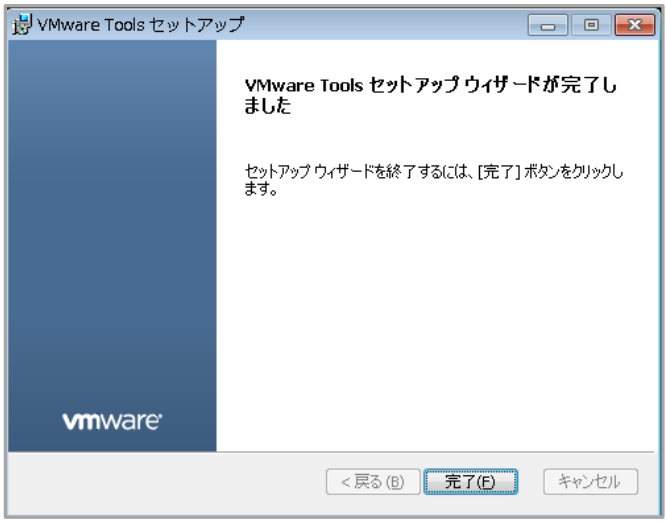
2) *[カスタム セットアップ]*で*[VMCI ドライバ]*から以下のドライバを*[ローカル ハード ドライブにインストール]*を選択して、インストールを行う





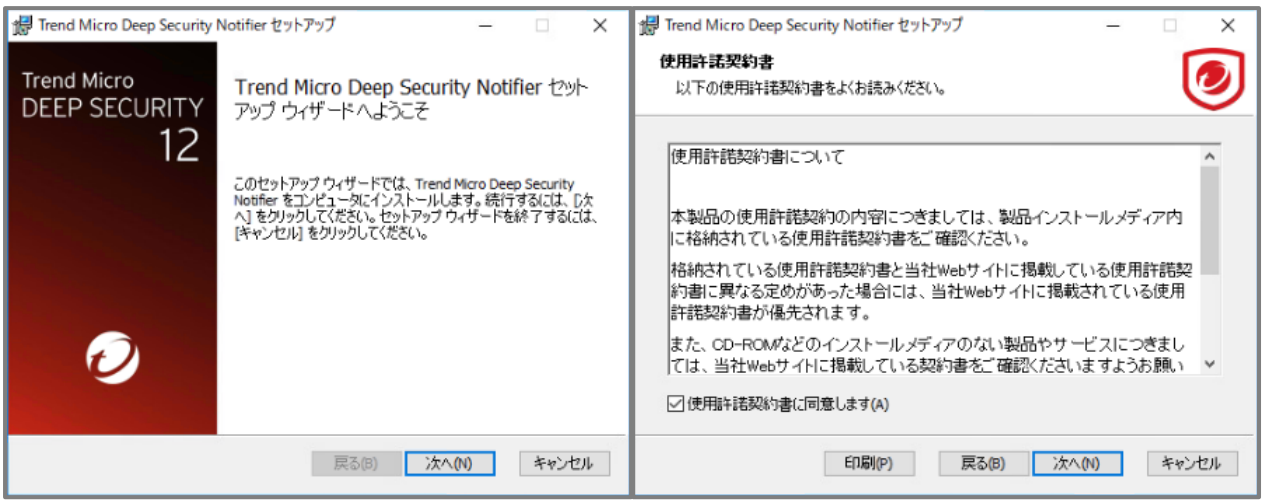
- **“NSX ファイル自己検証ドライバ”を選択**
  ※NSX ネットワーク自己検証ドライバについては選択しない

3) インストールを完了する

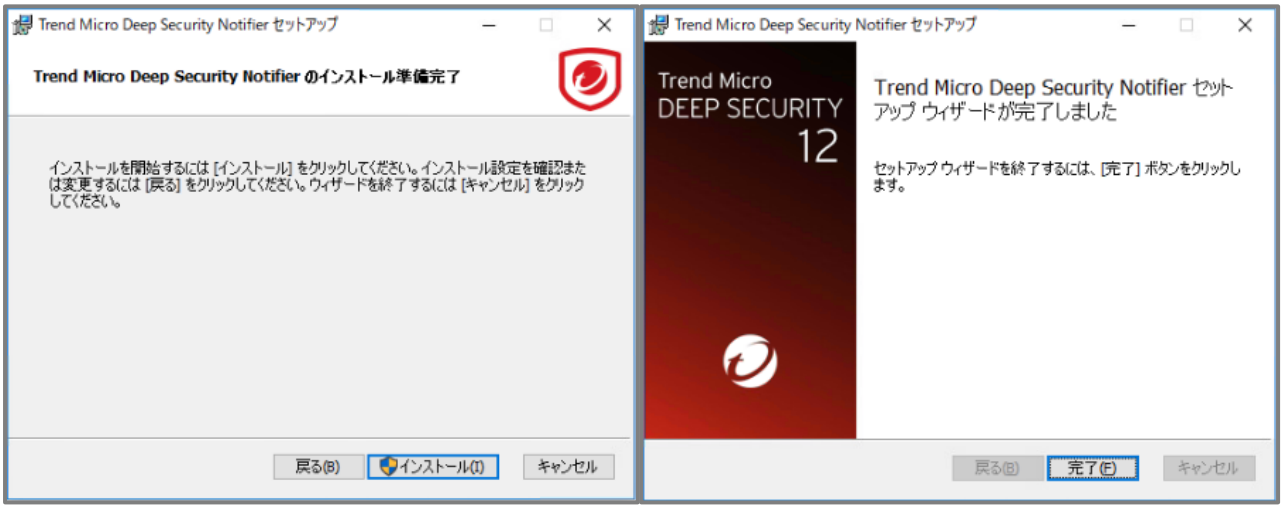


➢ Notifier のインストール

1）仮想マシン上で Notifier のセットアップファイルを実行し、セットアップウィザードを進め、使用許諾に同意する

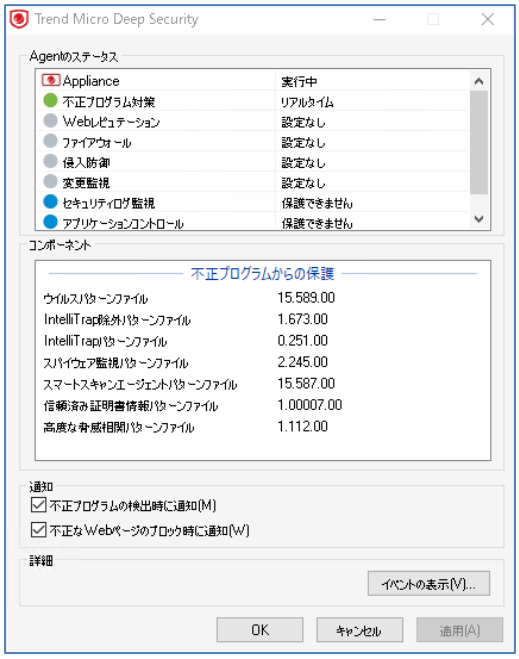


2）インストールを実行する



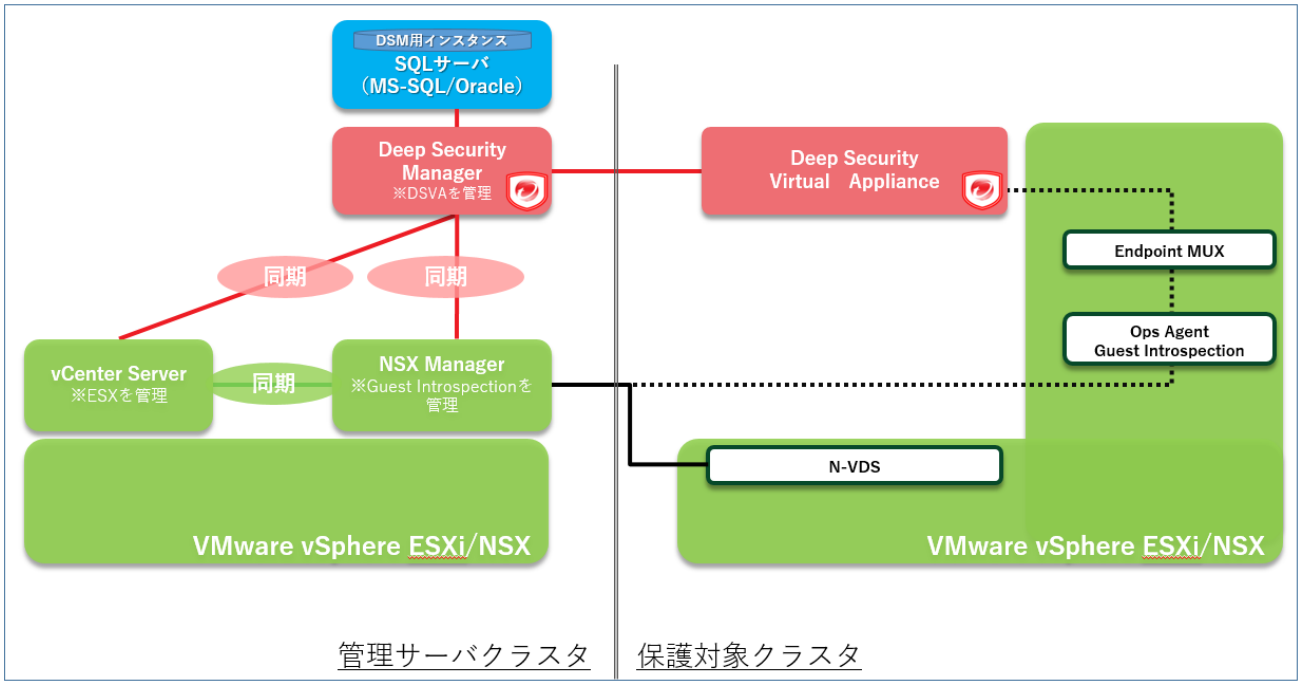
3）仮想マシンのデスクトップに Deep Security のアイコンが表示されることを確認する

Notifier では仮想マシンに適用されているセキュリティ機能の概要と検出したイベントが表示されます。
（以下のキャプチャは、DSVA にポリシーが配信された後のステータスを表示したものです。）



2-3-11. エンドポイントの保護を設定 NSX セキュリティポリシー・セキュリティグループ作成

ESXi ホスト上に展開される仮想マシンに適用する Deep Security セキュリティポリシーを定義するために、NSX セキュリティグループ、セキュリティポリシーの作成を行います。また、Deep Security で検出したセキュリティイベントに応じて仮想マシンを自動隔離する場合には、隔離用のセキュリティグループも作成をしておきます。



セキュリティグループの作成

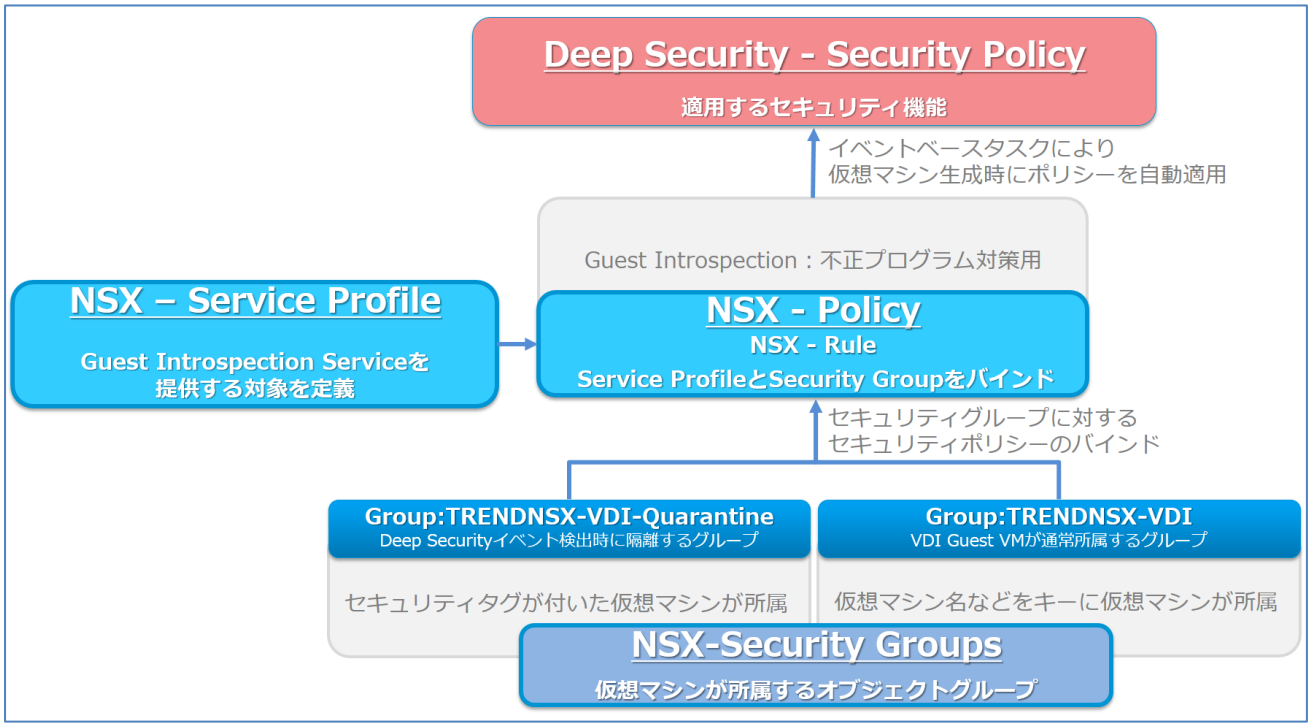
1. VDIドメインセキュリティグループの作成
2. 隔離用セキュリティグループの作成
   - Deep Securityのイベントに応じて自動隔離を行う場合

サービスプロファイルの作成

3. サービスプロファイルの作成
   - ゲストインロスペクションサービスをDeep Securityで利用するための定義

エンドポイントの保護のためのルール作成

4-1. VDIドメイン用ルールの作成
4-2. 隔離用ルールの作成
4-3. ルールの発行



この設定を行うことにより、仮想マシンが新たに生成された際に、セキュリティポリシーに従って自動的に Deep Security のセキュリティポリシーが適用され、セキュリティ機能を有効化することができます。

本セクションでは、以下のシチュエーションを想定した設定を行っていきます。
実際の環境では、利用される環境及びセキュリティポリシーに応じて設定を行ってください。

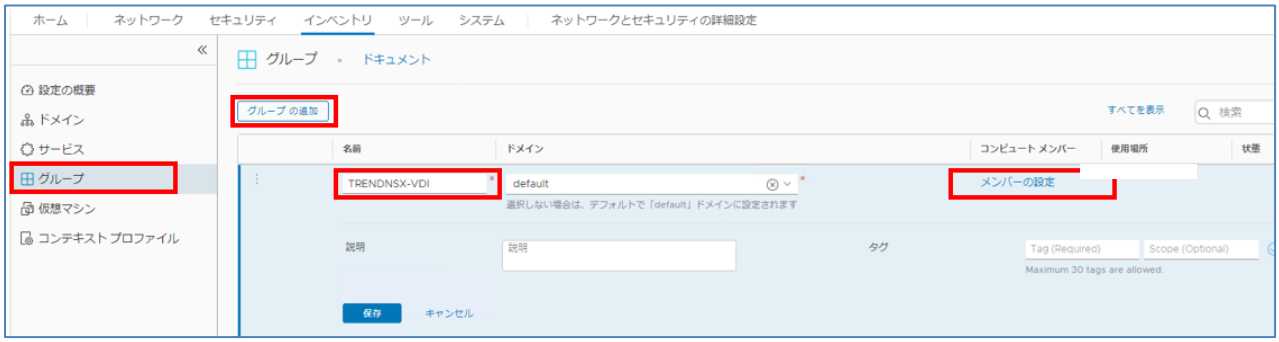
- Horizon にて仮想マシン（VDI 用 Windows クライアント）が展開される環境
- 仮想マシンに対して、Deep Security の不正プログラム対策、侵入防御、Web レピュテーション機能を有効化
- Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと連携した自動隔離ができるように隔離用セキュリティグループも設定
- 不正プログラム対策イベント検出時に付与する NSX セキュリティタグを **“ANTI_VIRUS.VirusFound.threat=high”**に設定
- 本セクションでは、各設定の名称を以下のとおり指定

・ **Deep Security セキュリティポリシー** ： **VDI_Windows Desktop_Demo01**
（セクション 2-3-7 で作成したセキュリティポリシー）
・ **NSX セキュリティポリシー** ： **Win-VDI-Policy**
・ **NSX セキュリティプロファイル** ： **Win-VDI-Profile**
・ **NSX セキュリティグループ** ： **TRENDNSX-VDI**（VDI ドメインセキュリティグループ：正常時）
TRENDNSX-VDI-Quarantine（隔離用セキュリティグループ）

[1] VDI ドメインセキュリティグループの作成

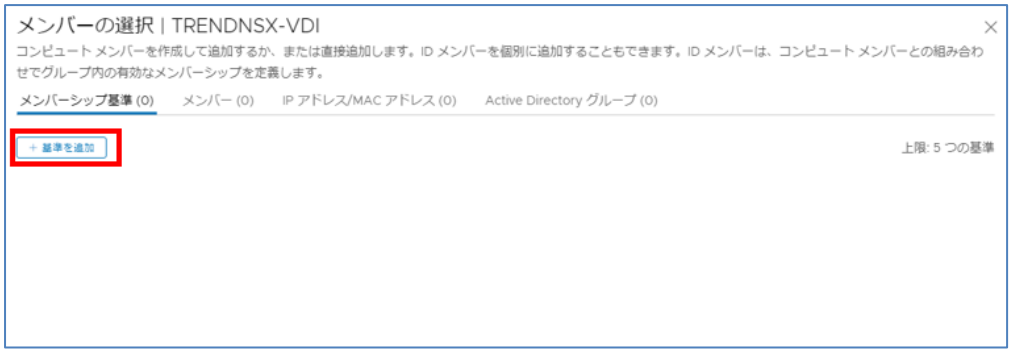
正常時に仮想マシンが所属するセキュリティグループを作成します。

1） NSX Manager にアクセスし、***[インベントリ]＞[グループ]***を選択し、***[グループの追加]***をクリックする

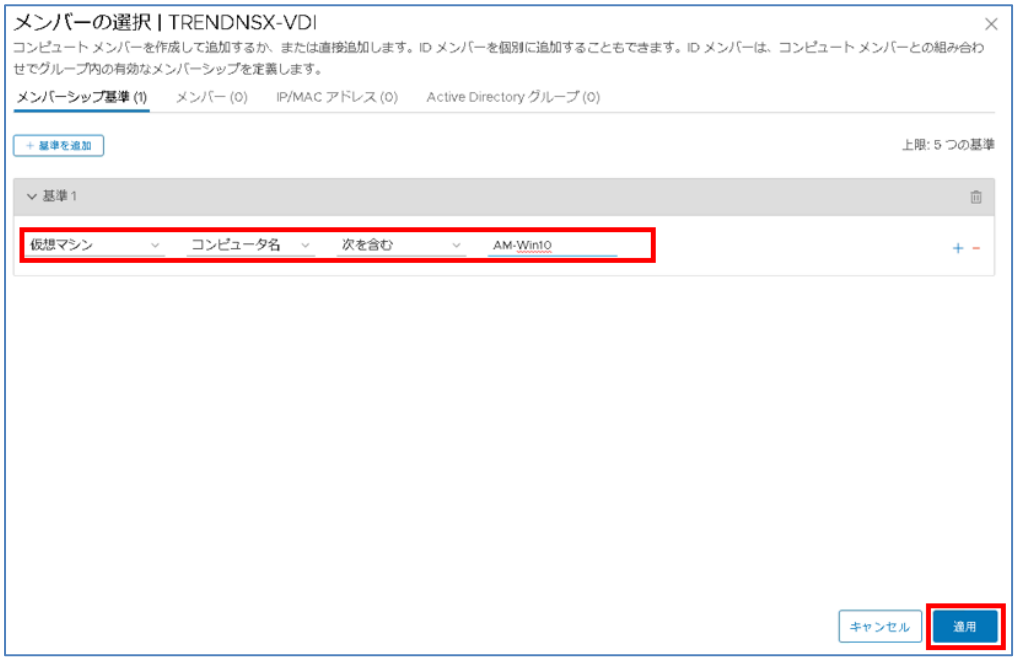


・ **名前** ： VDI ドメインセキュリティグループ名を設定（**“TRENDNSX-VDI”**）

2) **“コンピュートメンバー”**で**“メンバーの設定”**をクリックして、**“基準の追加“**を選択する



3) **”仮想マシン名”**の**”コンピュータ名”**が**“次を含む”**＝**“AM-Win10”**だった場合に TRENDNSX-VDI グループに所属するためのメンバーシップ基準を設定して適用する



4) ***[グループの追加]***で**“保存”**する

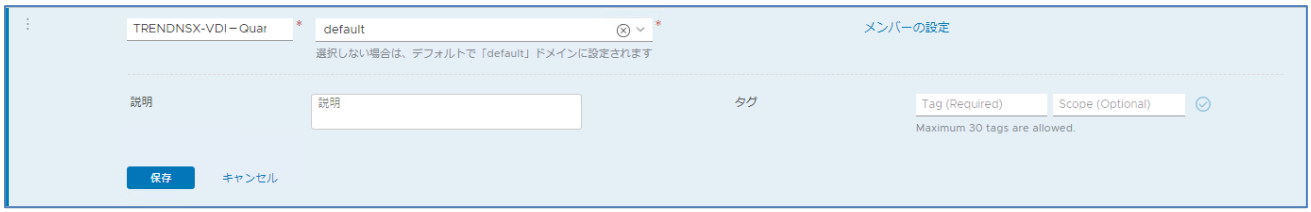
[2] 隔離セキュリティグループの作成

Deep Security で不正プログラム対策イベントを検出した際に仮想マシンが隔離されるセキュリティグループを作成します。

※自動隔離を行わない場合、設定は不要です。

1) VDI ドメインセキュリティグループ同様に、***[インベントリ]＞[グループ]***を選択し、***[グループの追加]***をクリックする

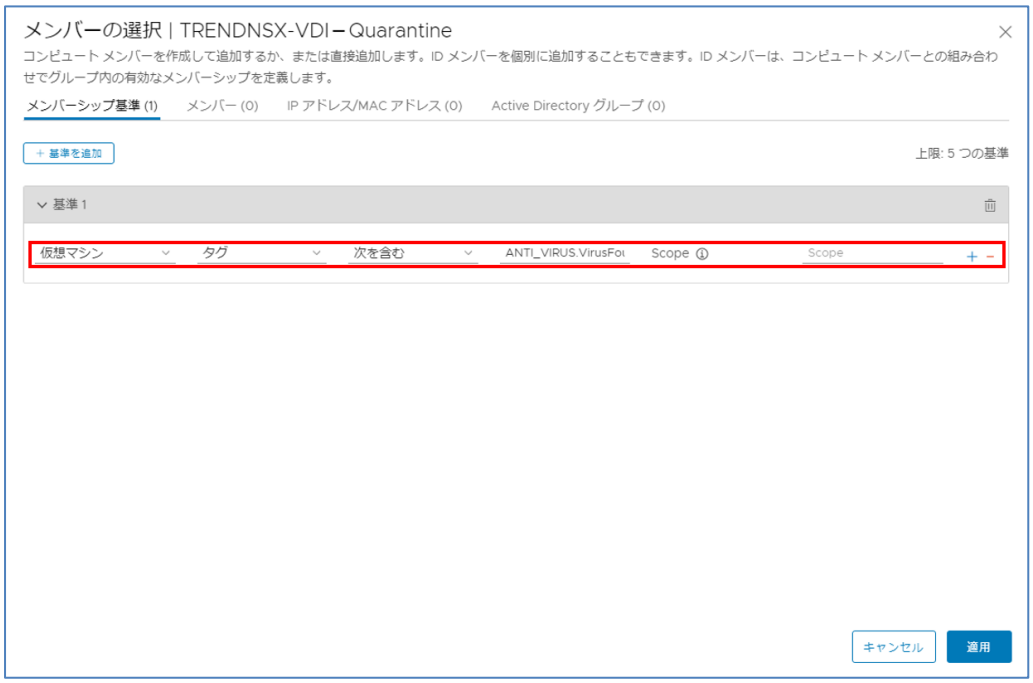
2) セキュリティグループの名前**“TRENDNSX-VDI-Quarantine”**を設定する



・ **名前** ： 隔離用セキュリティグループ名を設定（**“TRENDNSX-VDI-Quarantine”**）

3) **“コンピュートメンバー”**で**“メンバーの設定”**をクリックして、**“基準の追加“**を選択する

4) **”仮想マシン名”**に付与される**“タグ”**として**“次を含む”**＝**“ANTI_VIRUS.VirusFound.threat”**だった場合に TRENDNSX-VDI-Quarantine グループに所属するためのメンバーシップ基準を設定して適用する



5 ）*[グループの追加]*で**“保存”**する

6) セキュリティグループが 2 つ作成されていることを確認する

[3] サービスプロファイルの作成

NSX 環境において Deep Security によりエージェントレス型セキュリティを実現するための定義をプロファイルとして設定します。

1) NSX Manager にアクセスし、*[セキュリティ]＞[エンドポイントの保護]＞[サービスプロファイル]*へ移動し、*[パートナーサービス]*で *"Trend Micro Deep Security"を選択した上で、"*"**サービスプロファイルの追加"**をクリックする

2) サービスプロファイル名を指定し、ベンダープレートを選択して**"保存す"**る

- **サービスプロファイル名** ： サービスプロファイル名を設定（**"Win-VDI-Profile"**）
- **ベンダーテンプレート** ： **"Default(EBT)"**を選択する
  → Deep Security のイベントンベースタスク（EBT）により仮想マシン生成時を vCenter Server から通知された際にその仮想マシンに対して Deep Security のポリシーを自動的に適用させることを宣言

3) サービスプロファイルが設定されていることを確認する

[4] エンドポイントの保護のためのルールの作成

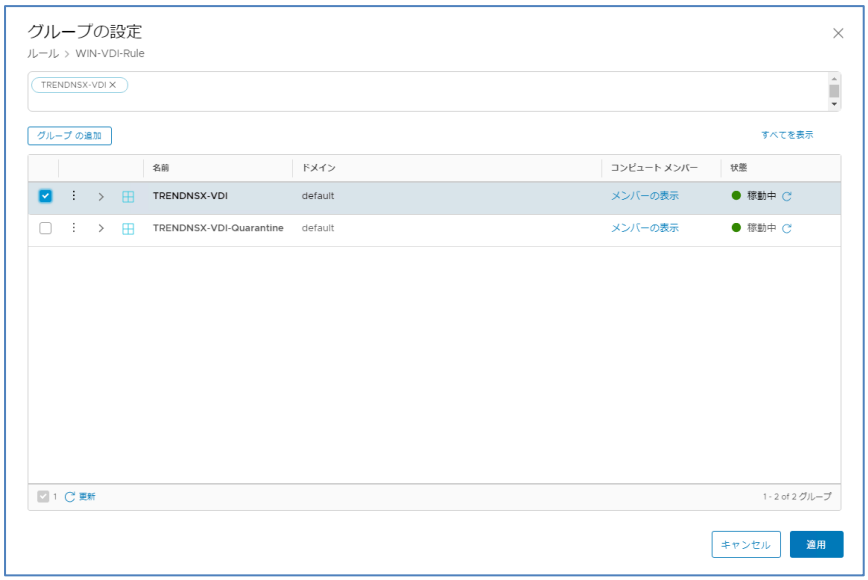
[4-1]エンドポイントの保護のための VDI ドメイン用ルールを作成する

VDI ドメイン用セキュリティグループとサービスプロファイルを紐づけるためにルールを作成します。

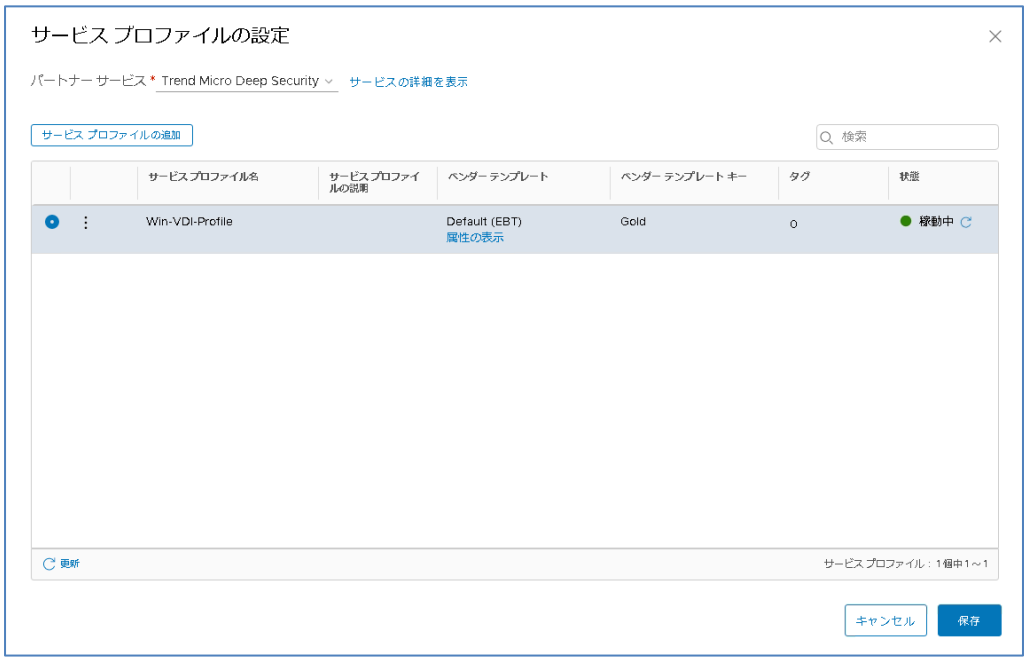
1) NSX Manager にアクセスし、*[セキュリティ]＞[エンドポイントの保護]＞[ルール]*へ移動して*[ポリシーの追加]*をクリックし、**[名前]** 列で、“New Policy” をクリックして名前を変更する（***“Win-VDI-Policy”***）

2) 作成したポリシーの横にあるチェックボックスをオンにし、*[ルールを追加]* をクリックする
作成したポリシーの下に表示されたルールの**[名前]** 列で、“New Rule” をクリックして名前を変更する（***“Win-VDI-Rule”***）

3) ***[グループ列]***で***[グループの選択]***を選択し、VDIドメインセキュリティグループを(***"TRENDNSX-VDI"***)選択して***[適用]***する。



4) ***[サービスプロファイル]列***で***[サービスプロファイルの選択]***を選択し、サービスプロファイル(***"Win-VDI-Profile"***)を選択して***[保存]***する。



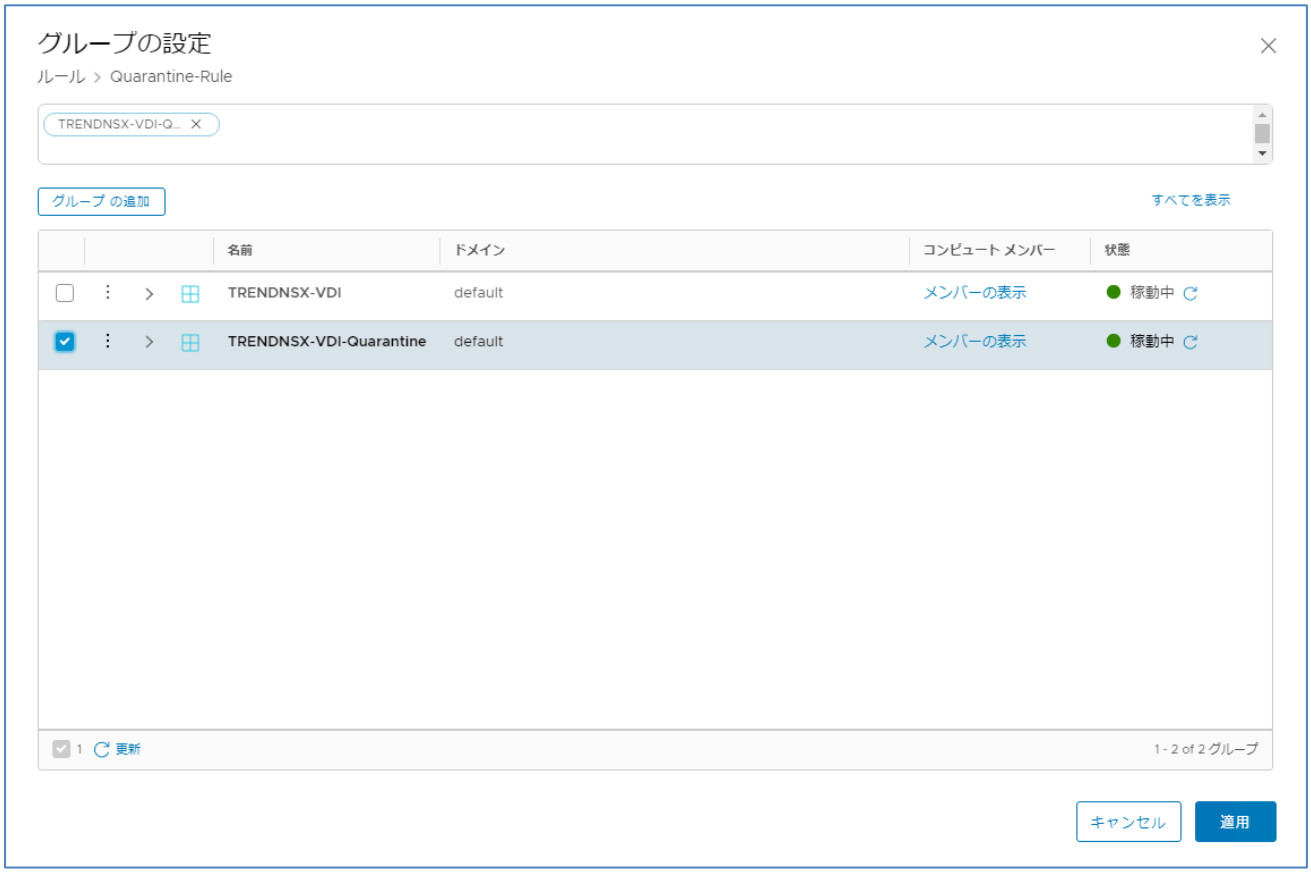
[4-2]　エンドポイントの保護のための隔離用ルールを作成する

隔離用セキュリティグループとサービスプロファイルを紐づけるためにルールを作成します。
※自動隔離を実施しない場合は作成する必要はありません。

1)　[4-1]の手順と同様に***[セキュリティ]＞[エンドポイントの保護]＞[ルール]***へ移動し、***[ポリシーの追加]***をクリックして、**[名前]** 列で、"New Policy" をクリックして名前を変更する(***"Quarantine-Policy"***)

2) 作成したポリシーの横にあるチェックボックスをオンにし、*[ルールを追加]*をクリックする
作成したポリシーの下に表示されたルールの**[名前]** 列で、“New Rule” をクリックして名前を変更する
（*“Quarantine-Rule”*）

3) *[グループ列]*で*[グループの選択]*を選択し、隔離用セキュリティグループを（*“TRENDNSX-VDI”*）選択して*[適用]*する。



4) [4-1]と同様、*[サービスプロファイル]列*で*[サービスプロファイルの選択]*を選択し、サービスプロファイル（*“Win-VDI-Profile”*）を選択して*[保存]*する。

[4-3] エンドポイントの保護のためのルールの発行

設定したルールを各 ESXi ホストに適用するために発行を行います。

1) 作成した VDI ドメイン用ルールと隔離用ルールの順番の設定

後段で設定する分散ファイアウォールと連携して自動隔離を行う場合、通常運用時には仮想デスクトップは VDI ドメイン用ルールに所属します。この状態で Deep Security にて不正プログラム対策イベントを検出すると DSM は NSX Manager に対してセキュリティタグ情報を連携します。これにより該当仮想デスクトップを隔離用セキュリティグループへ所属させるための NSX セキュリティタグが付与されますが、VDI ドメイン用セキュリティグループと隔離用セキュリティグループの両方に所属することになります。

エンドポイントの保護におけるポリシー、ルールについては、上位に配置されているものが優先して適用されます。ある仮想マシンが、複数のセキュリティグループに所属している状態になった場合には、上位に配置されているルールが優先して適用されます。

自動隔離を行う場合には、必ず隔離用セキュリティグループが適用されているポリシー、ルールが上位になるように設定してください。

ポリシーの順番を変える場合には、該当のポリシーをマウスで選択して移動したい位置へ移動します。

2) ルールの ESXi ホストへの配信の実行

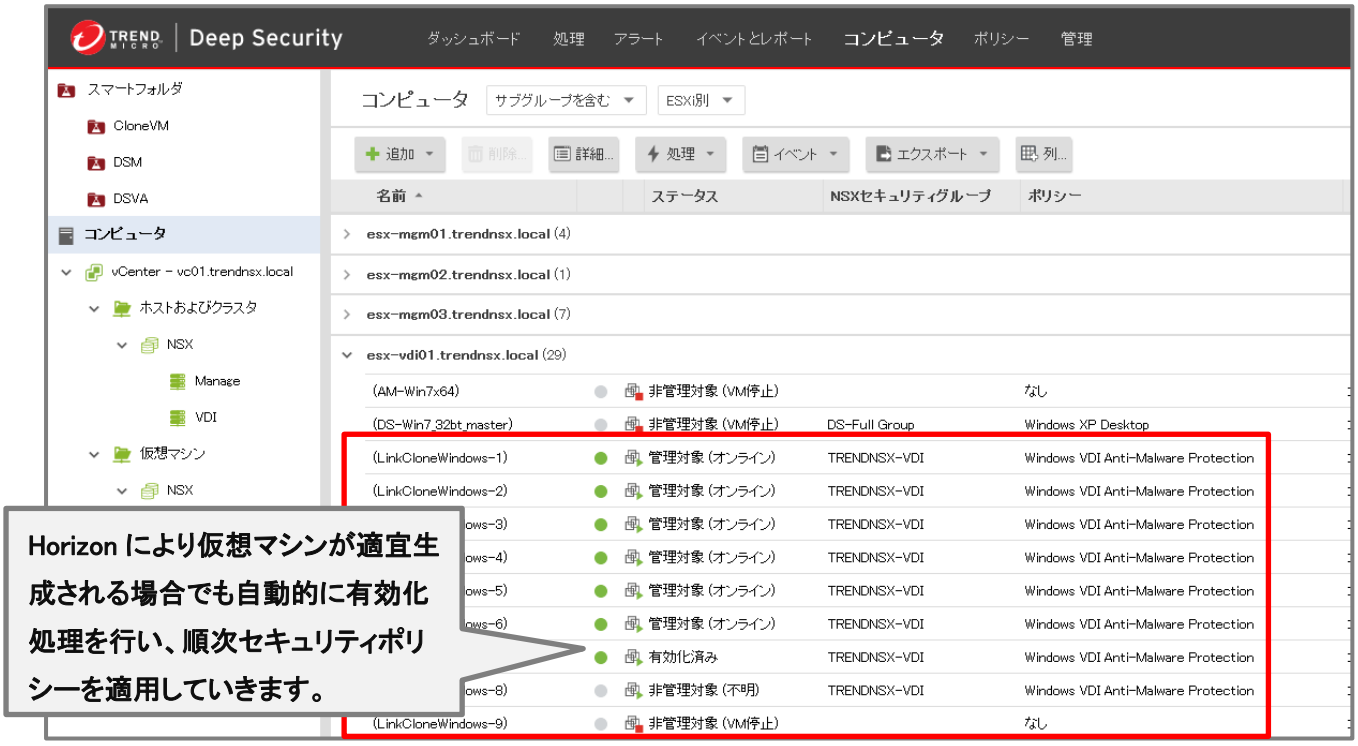
作成したポリシー、ルールを各 ESXi ホストへ適用するためにルール一覧の右上にある[発行]ボタンを押す
(“未発行の変更の合計”が作成したポリシーとルールの総計になることを予め確認する)

3) ルールの確認

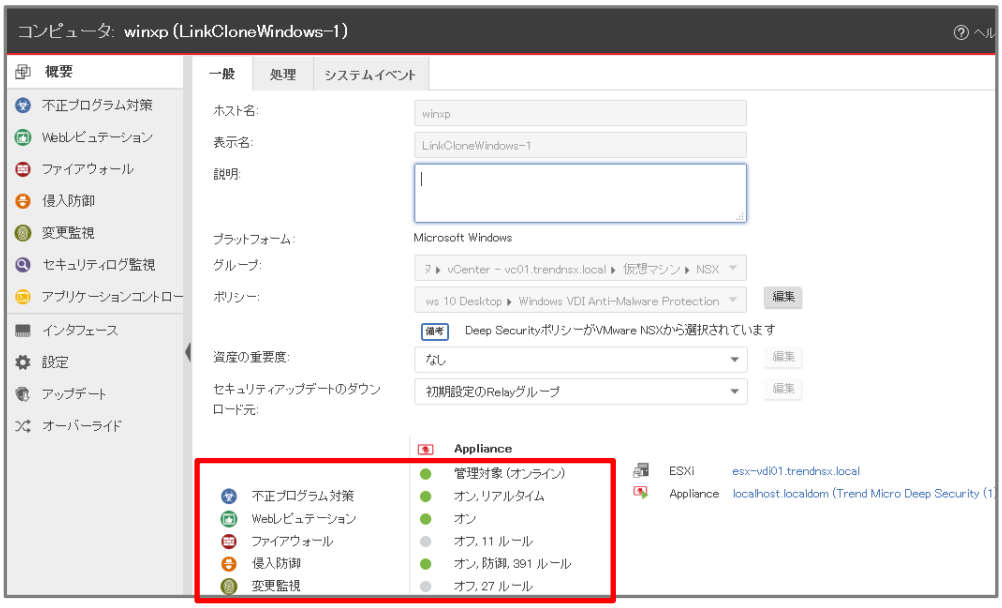
2-3-12. 仮想マシン展開時の有効化の確認とセキュリティ機能の検証

➢ Deep Security 有効化ステータスの確認

Deep Security の仮想マシン保護においては、保護対象となる仮想マシンが、DSM の管理対象下にある必要があります。仮想マシンが管理対象下に入ると、引き続き DSVA による保護が行われている ESXi ホスト上で仮想マシン毎に NSX セキュリティグループに紐付くセキュリティポリシーが自動的に配信、適用されます。
セキュリティポリシーの配信が完了して、正常にセキュリティ機能が提供されている状態となると、各仮想マシンのステータスは**[管理対象(オンライン)]**という状態となります。
[管理対象(オンライン)]の状態に移行する一連の処理を Deep Security では**"有効化"**と呼びます。



ステータスが**[管理対象(オンライン)]**であれば、各仮想マシンのセキュリティ機能も有効に機能していることを示しています。



有効化により何かしらのエラーが発生している場合には、意図したセキュリティ機能が提供できていない可能性がありますので、エラー原因を特定して対処する必要があります。

※自動的に有効化を行わない場合には、DSM 上から個別に仮想マシンの有効化を行う、または、イベントベースタスク(EBT)を設定する必要があります。イベントベースタスクを設定する場合には、NSX セキュリティポリシーのセキュリティプロファイルを**[Default(EBT)]**に設定しておく必要があります。
(NSX for vShield Endpoint、NSX for vSphere Standard を利用している場合にもサービスプロファイルを**[Default(EBT)]**に指定する必要があります。)

➢ **Deep Security 有効化ステータスの確認**

各セキュリティ機能における実際の動作確認については、以下の方法で実施することが可能です。実際には環境に応じて必要な検証を実施してください。不正プログラム対策については、DSVA のファイル検出機能(Guest Introspection に依存)が正常に動作をしているか、Web レピュテーションについては、ネットワーク検出機能(Network Introspection に依存)が正常に動作しているかを確認することができます。

- **不正プログラム対策**
  保護対象仮想マシンからテスト用ウイルスファイル(EICAR)をダウンロードして不正プログラム対策イベントが発報するかを確認する。
  詳細及びテスト用ウイルスファイルの取得については、以下の FAQ を参照してください。
  http://esupport.trendmicro.com/solution/ja-JP/1114066.aspx
- **Web レピュテーション**
  保護対象仮想マシンからトレンドマイクロが用意するテスト用サイトへアクセスを行い、Web レピュテーションイベントが発報するかを確認する。
  詳細及びテストサイトの情報は、以下の FAQ を参照してください。
  http://esupport.trendmicro.com/solution/ja-JP/1114067.aspx

2-4. セキュリティタグを利用した自動隔離の考え方と設定手順

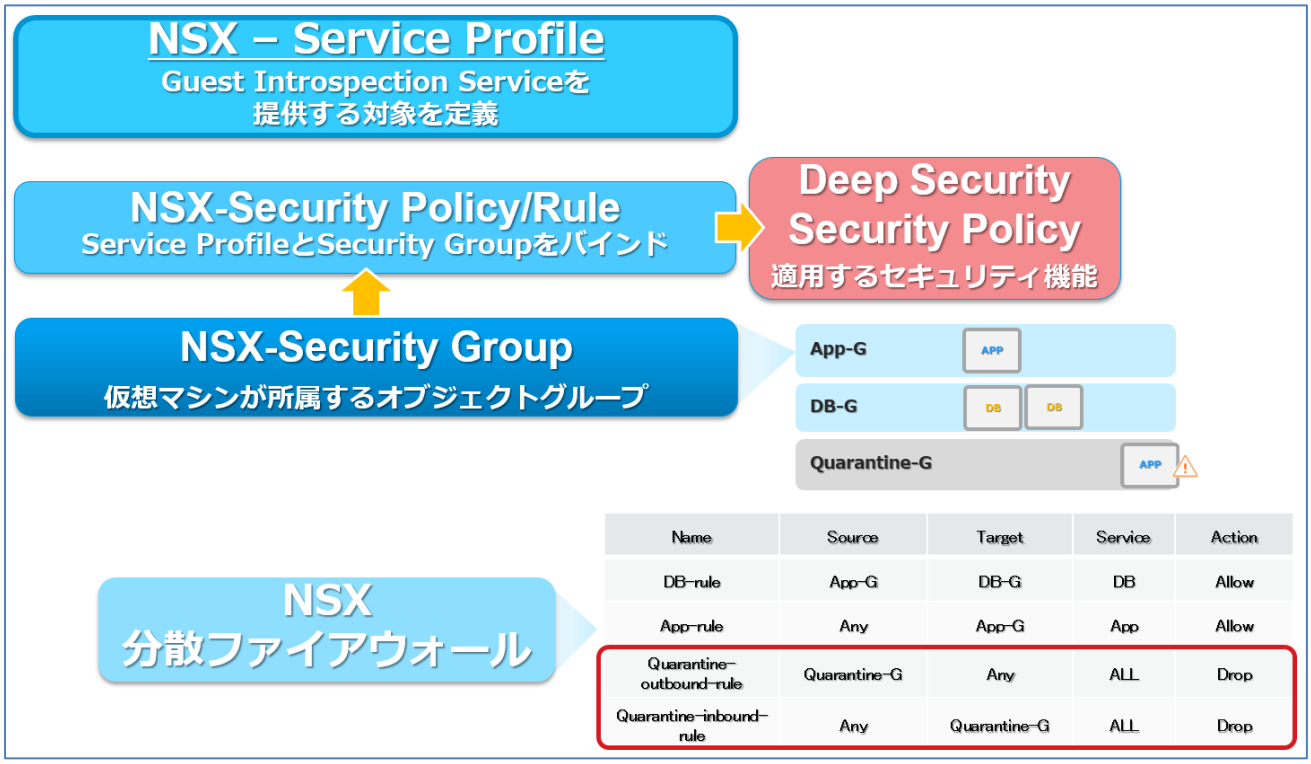
セクション 2-3 のエージェントレスによる仮想マシン保護を行うことでセキュリティレベルを一定レベルに維持することが可能となりました。このセクションでは、分散ファイアウォールを利用して DSVA で保護されている仮想マシンで検出されたセキュリティイベントをトリガーに該当の仮想マシンを他のネットワークと通信できないように自動隔離する設定を行います。

2-4-1. セキュリティタグと分散ファイアウォールを利用した自動隔離の仕組み

分散ファイアウォールによるアクセス制御を行うためには、仮想マシンを NSX セキュリティグループに紐付け、それをオブジェクトとしてファイアウォールルールの設定を行います。

セキュリティグループの設定を行う際に、グループのメンバーシップに所属させる基準として、コンピュータ名やオブジェクトタイプ（クラスタなど）とあわせてセキュリティタグを利用することによって、Deep Security のセキュリティイベントをトリガーとして該当の仮想マシンの所属するセキュリティグループを動的に変更することが可能となります。その結果として、適用される分散ファイアウォールルールを変更されることとなります。

セキュリティタグが付与された仮想マシンが所属するセキュリティグループに対して他のネットワークと通信不能なファイアウォールルールを適用することによって、仮想マシンがあたかもネットワーク設定が変更されて隔離ネットワークに移行したような効果を適用することができます（実際は仮想マシンのネットワーク設定は変更されません。）



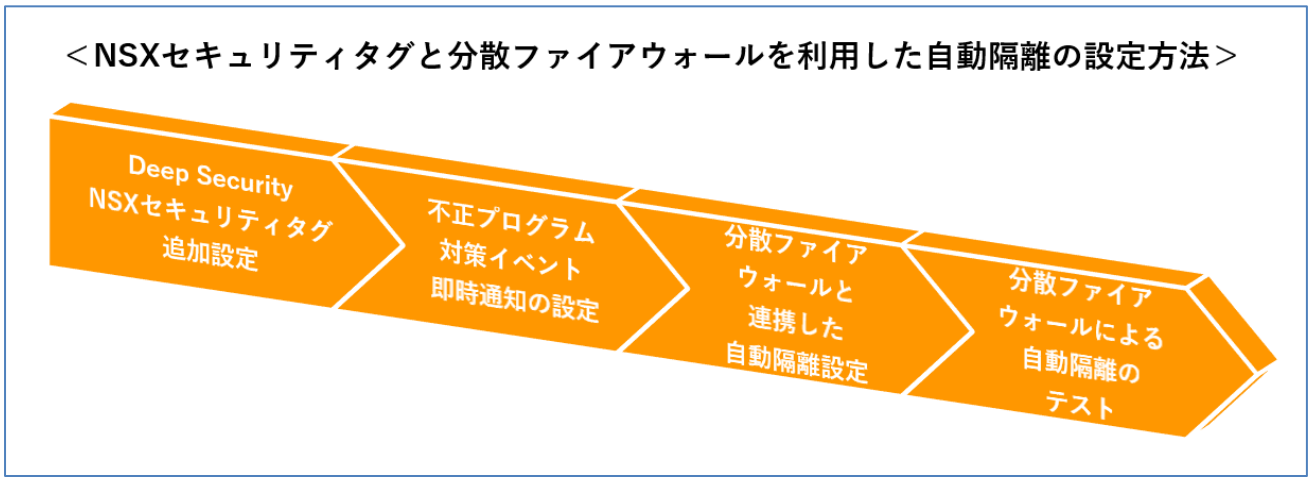
※上記のルールの記載は本ガイドのサンプルの設定内容とは合致していません。

本セッションでは、セクション 2-3-11 で設定したサービスプロファイル及びセキュリティグループを利用して、分散ファイアウォールによる自動隔離の設定を行います。

分散ファイアウォールのポリシーは以下のルールを設定しています。
（実際のルール設定を行う場合には、適用する環境のセキュリティポリシーにしたがってルール設計を行ってください。）

ポリシー/ルール名	送信元	送信先	サービス	アクション
Quarantine				
TRENDNSX-VDI-Quarantine-outbound	TRENDNSX-VDI-Quarantine	Any	Any	Block
TRENDNSX-VDI-Quarantine-Inbound	Any	TRENDNSX-VDI-Quarantine	Any	Block
TRENDNSX-VDItoVDI				
VDItoVDI	TRENDNSX-VDI	TRENDNSX-VDI	Any	Block
All Permit-Rule				
All Permit-Rule	Any	Any	Any	Permit

NSX セキュリティタグと分散ファイアウォールを利用した自動隔離の設定は以下の流れで行います。



2-4-2. Deep Security NSX セキュリティタグ追加設定

不正プログラム対策イベントを検出した際に NSX セキュリティタグを付与する設定を行います。

1） DSM から**[ポリシー]**>**[ポリシー]**から **[VDI_Windows Desktop_Demo01]**を選択し、**[不正プログラム対策]**の**[詳細]**タブを選択する
[NSX セキュリティのタグ付け]で以下の設定を行う

- **[NSX セキュリティのタグ付け]** : オン(“継承”のチェックボックスを外す)
- **[NSX セキュリティタグ]** : **ANTI_VIRUS.VirusFound.threat=high**
- **[修復処理に失敗した場合にのみ、NSX セキュリティタグを適用します。]** :
  チェックボックスを外す
- **[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用された NSX セキュリティタグは削除されます。]** :
  チェックボックスを入れる

※[修復処理に失敗した場合にのみ、NSX セキュリティタグを適用します。] のチェックボックスを入れた場合、不正プログラムを検出した際に修復処理が成功した場合には、NSX セキュリティタグは付与されず、自動隔離は行われません。

修復処理の詳細については、以下のヘルプセンターを参照してください。
https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/Protection-Modules/Intrusion-Prevention/nsx-security-tags.html#Configur

※[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用された NSX セキュリティタグは削除されます。] のチェックボックスを外した場合、自動隔離後に不正プログラム検索を手動で実施した際に不正プログラム対策イベントが検出されない場合でも NSX セキュリティタグは外れることはなく、NSX Manager 上で直接セキュリティタグを外す必要があります。

2-4-3. 不正プログラム対策イベント 即時通知の設定

自動隔離が実行される流れは、以下のとおりです。

DSVA にて不正プログラムを検出

↓

DSM⇔DSVA のハートビート間隔で DSM へイベントを通知

↓

DSM から vCenter Server へ該当仮想マシンに対するセキュリティタグ付与を実行

↓

仮想マシンを自動隔離

デフォルトの設定では、DSVA⇔DSM のハートビート間隔が 10 分（最短 1 分に設定可能）のため、DSVA で不正プログラムイベントが検出されてから、DSM に通知＝NSX セキュリティタグの付与まで最大 10 分を要する可能性があります。ハートビートを待たずに、DSVA が不正プログラム対策を検知した時点で即時イベントを DSM で検知できるように設定を行います。

1） DSM サーバにアクセスして、Windows コマンドプロンプトを立ち上げ、Deep Security Manager のインストールディレクトリから以下のコマンドを実行

```
C:¥Program Files¥Trend Micro¥Deep Security Manager>dsm_c.exe -action changesetting -name
com.trendmicro.ds.antimalware:settings.operational.AMNotifyEventImmediate -value true

Stopping Trend Micro Deep Security Manager...
System Setting: com.trendmicro.ds.antimalware:settings.operational.AMNotifyEvent
Immediate Value: true saved
Complete
Starting Trend Micro Deep Security Manager...

C:¥Program Files¥Trend Micro¥Deep Security Manager>
```

※コマンドを実行すると、DSM プロセスの再起動が発生します。
※DSM サーバが複数ノードある場合でも 1 台の DSM サーバで実行すれば変更は反映されます。

2) 設定を各 DSVA に反映させるため、DSVA に対するポリシーの配信を行う

2-4-4. 分散ファイアウォールと連携した自動隔離設定

TRENDNSX-VDI グループに所属する仮想マシン、NSX セキュリティタグが付与され自動隔離された仮想マシンに適用するファイアウォールポリシーを作成します。

1) NSX Manager にアクセスし、*[セキュリティ]>[East-West のセキュリティ]>[分散ファイアウォール]*を選択し、*[カテゴリ固有のルール]*を選択し、*[ポリシーの追加]*を行う

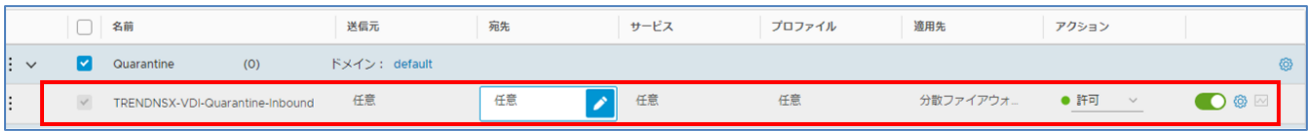
2) 隔離用ポリシーを作成する

2-1) **[名前]**列の“New Policy” をクリックして名前を変更 “Quarantine”して、さらに*[ルールの追加]*を行う

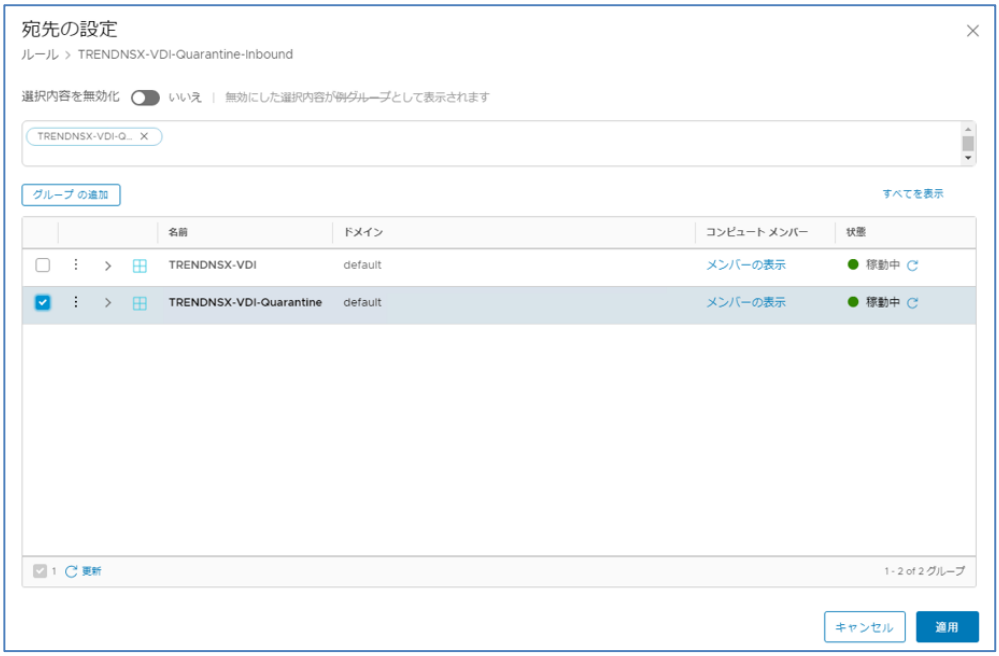
2-2）隔離用ルールを作成する

作成したポリシー の横にあるチェックボックスをオンにして[ルールを追加] する

ポリシーの下に新規に追加されたルールを以下の通り設定してアウトバウンドのブロックルールを作成する



- **名前** ： ルール名を任意に設定“TRENDNSX-VDI-Quarantine-Outbound”
- **送信元** ： 任意（デフォルト）
- **宛先** ： 宛先カラムをダブルクリックして“宛先の設定”から隔離用グループ“TRENDNSX-VDI-Quarantine”を選択する

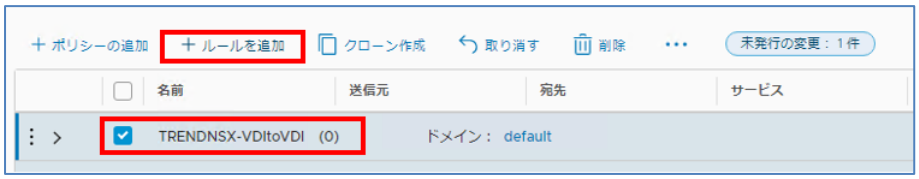


- **サービス** ： 任意（デフォルト）
- **プロファイル** ： 任意（デフォルト）
- **適用例** ： 分散ファイアウォール（デフォルト）
- **アクション** ： ドロップ

同様にインバウンドのブロックルールを作成し、2 つの隔離用ルールが作成できていることを確認する

3) VDIドメイン用ポリシーを作成する

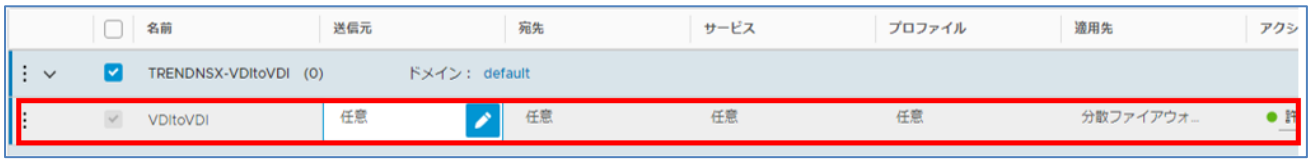
3-1) 1)と同様に新規ポリシーを作成し、**[名前]**列の“New Policy” をクリックして名前を変更 “TRENDNSX-VDItoVDI”して、さらに***[ルールの追加]***を行う



3-2) VDI 仮想マシン間のアクセスをドロップするルールを作成する

作成したポリシー の横にあるチェックボックスをオンにして[ルールを追加] する

ポリシーの下に新規に追加されたルールを以下の通り設定して VDI 仮想マシン間のブロックルールを作成する



- **名前** ： ルール名を任意に設定“VDItoVDI”
- **送信元** ： 宛先カラムをダブルクリックして“宛先の設定”から VDIドメイン用グループ “TRENDNSX-VDI”を選択する
- **宛先** ： 宛先カラムをダブルクリックして“宛先の設定”から VDIドメイン用グループ “TRENDNSX-VDI”を選択する
- **サービス** ： 任意（デフォルト）
- **プロファイル** ： 任意（デフォルト）
- **適用例** ： 分散ファイアウォール（デフォルト）
- **アクション** ： ドロップ

ルールが作成できていることを確認する

4) VDIドメインからその他のネットワークに対する通信をすべて許可するルールを同様に作成する

- ポリシー
  - **名前** ： ポリシー名を任意に設定“All Permit-Rule”
- ルール
  - **名前** ： ルール名を任意に設定“All Permit-Rule”

- **送信元** ： 任意（デフォルト）
- **宛先** ： 任意（デフォルト）
- **サービス** ： 任意（デフォルト）
- **プロファイル** ： 任意（デフォルト）
- **適用例** ： 分散ファイアウォール（デフォルト）
- **アクション** ： 許可

5）ルールの各 ESXi ホストへの配信

5-1）ルールの設定が完了したら各 ESXi ホスト上の分散ファイアウォールモジュールにルールを反映させるため、*[発行]*を選択する

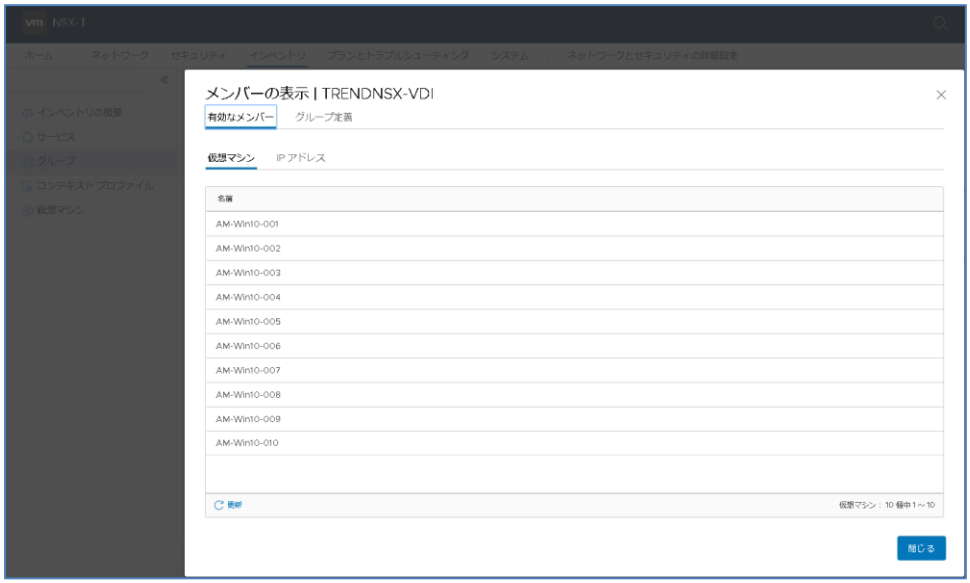
※ポリシーを発行する前に必ず隔離用ポリシーが VDI ドメイン用ポリシーの上位に配置されるかを確認してください。セキュリティグループの特性上、1 つのオブジェクトが複数のグループに所属している場合、分散ファイアウォールでは、上位にあるグループのポリシーが適用されます。隔離用ポリシーが下位にある場合には自動隔離がされなくなるため注意してください。（NSX for vSphere ではセキュリティグループの設定に除外項目がありましたが、NSX-T ではありません。）

5-2）各ポリシーが**“稼働中”**となっていることを確認する

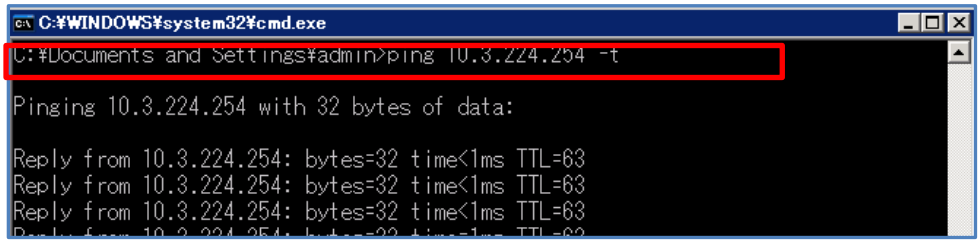
2-4-5. 分散ファイアウォールによる自動隔離のテスト

仮想マシンで不正プログラム対策イベントを検出した際に、セキュリティタグが付与されて該当端末の通信ができなくなることを確認します。

1) NSX Manager にアクセスし、*[インベントリ]>[グループ]*を開く
“TRENDNSX-VDI”グループに仮想マシンが所属していることを確認する



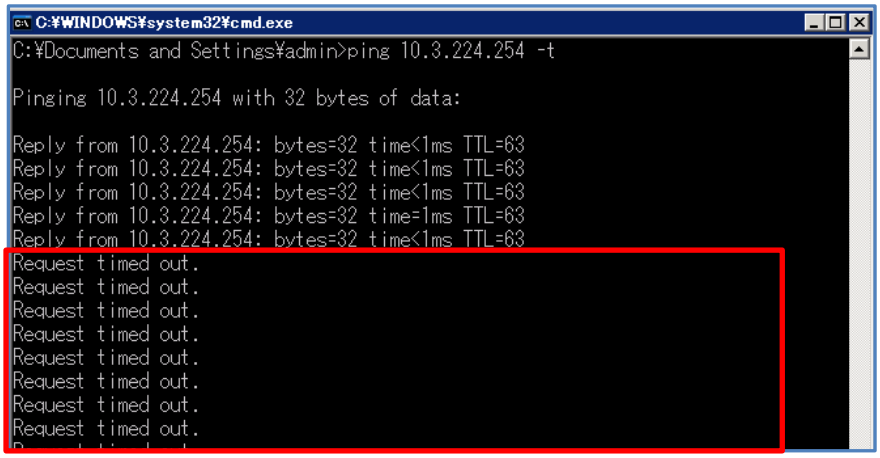
2) 隔離を実施する仮想マシンから外部ネットワークに対してコマンドプロンプトにて Ping を実行する



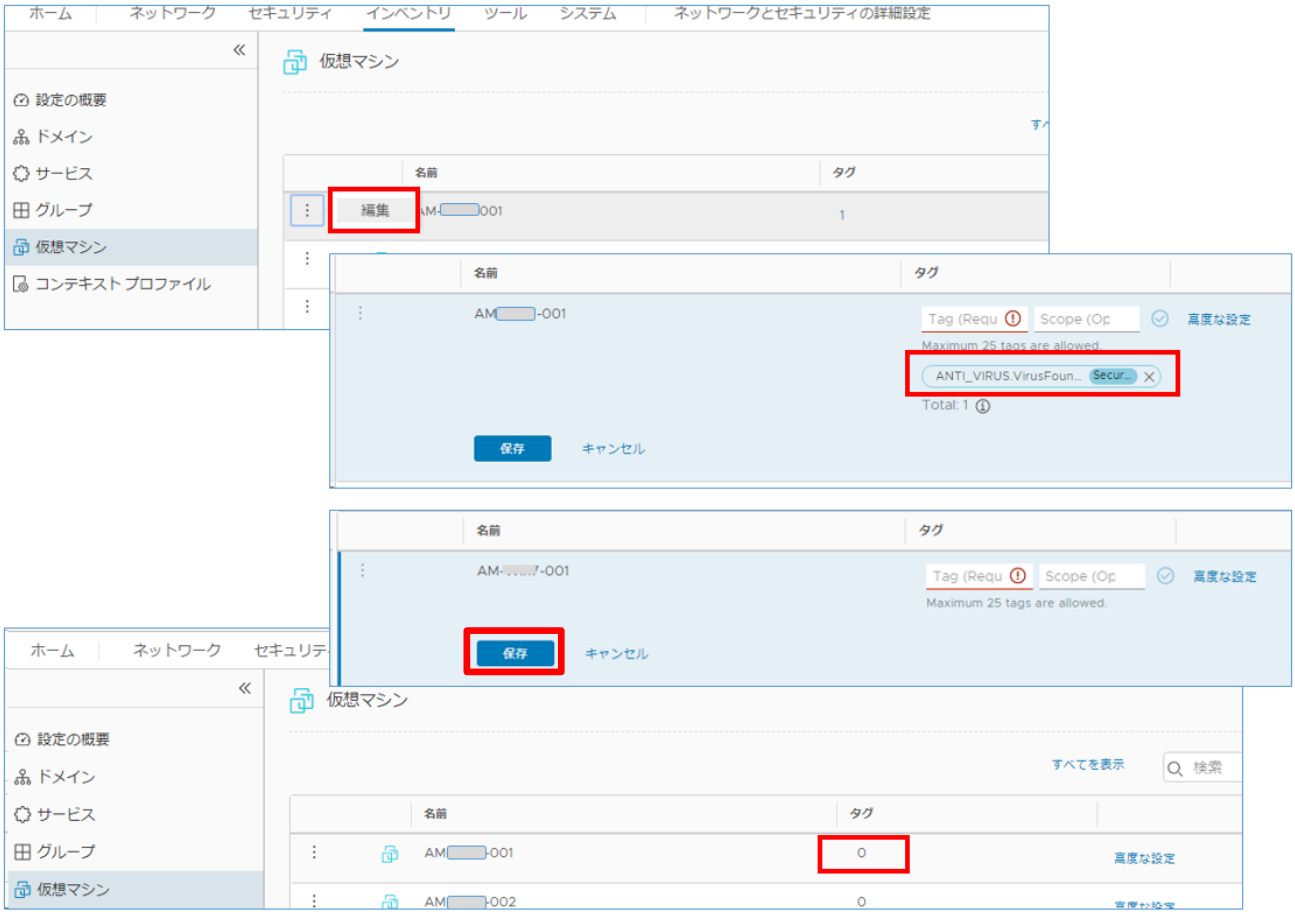
3) 仮想マシンからテスト用ウイルスファイル(EICAR)をダウンロードする
（リモートデスクトップでアクセスしている場合にはアクセスが切断されます）
詳細及びテスト用ウイルスファイルの取得については、以下の FAQ を参照してください。
http://esupport.trendmicro.com/solution/ja-JP/1114066.aspx

4) EICAR を検出した仮想マシンが“TRENDNSX-VDI-Quarantine”に移動していることを確認する

また、 2)で実行していた Ping が、仮想マシンが分散ファイアウォールにより隔離されたことにより、疎通 NG となっていることを確認してください。(Web コンソールなどで確認ができる場合)

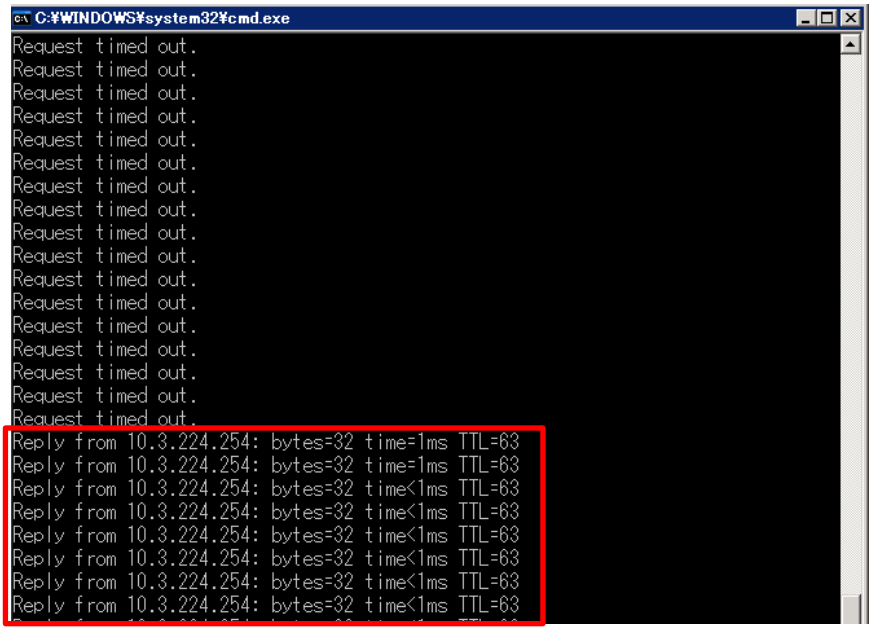


5) NSX Manager から該当仮想マシンのセキュリティタグを手動で削除することによって、隔離の解除（**“TRENDNSX-VDI”**への復帰）を行う
（セキュリティタグの横についている[×]マークで削除）



または、DSM から該当仮想マシンに対して不正プログラムのフル検索を行い、完了後に隔離が解除されることを確認する
（**[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用された NSX セキュリティタグは削除されます。]**のチェックボックスをオンにしていた場合のみ）

6) セキュリティタグが外れたことを確認し、実行していた Ping 疎通が復旧していることを確認する



3. 設計・導入時に留意するべきポイント

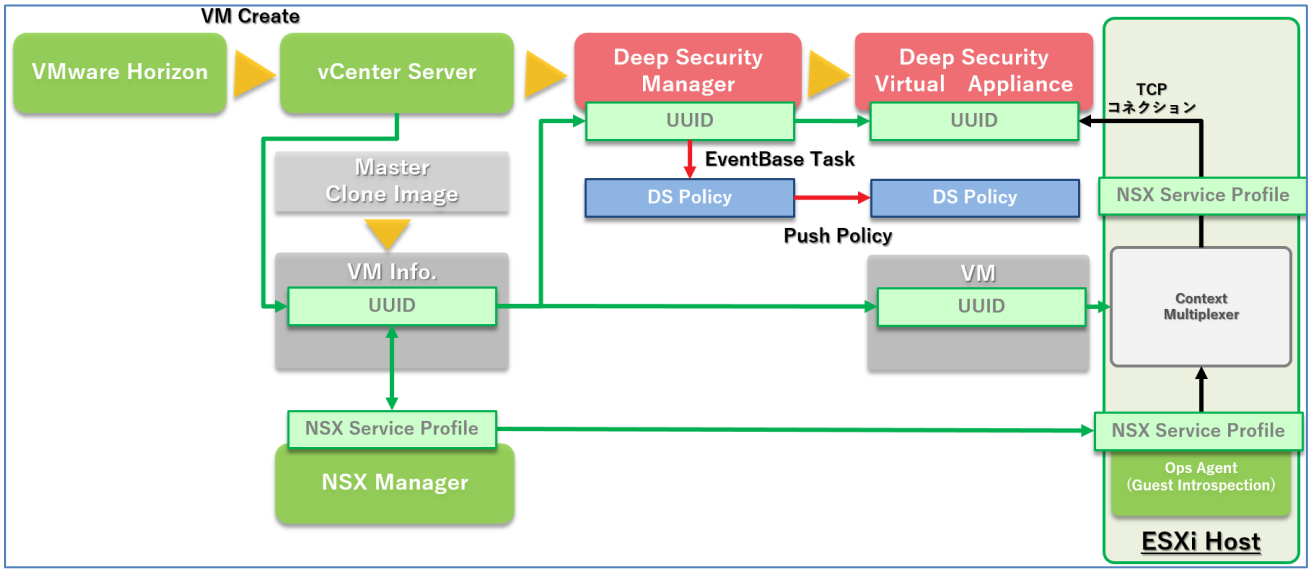
3-1. 設計上留意しておくべきポイント

3-1-1. システム全般

- DSM を稼動させるノードは DSR 以外のアプリケーションを同居させないでください。
  （小規模環境において、DSM 用 SQL サーバが同居することは可能）
- DSM 用 SQL サーバには、スケーラビリティの観点から Express 版の利用は避けるようにしてください。
- DSM 用 SQL サーバと DSM ノードは同一サイトに設置してください。DSM 用 SQL サーバと DSM サーバ間の通信遅延が大きい場合、DSM が正常に動作しない可能性があります。
- DSVA は各 ESXi ホストに 1 台ずつ配置される必要があります。特に共有ディスク上に配置しなくてはならない場合には、DRS/vMotion、Storage vMotion が発生しないように設計をしてください。
  また、他の保護対象マシンとのリソースを共有しないようにしてください。オーバーコミット状態の場合、正常に動作しない場合があります。
  詳細は以下の FAQ も参照してください。
  http://esupport.trendmicro.com/solution/ja-jp/1115886.aspx
- 仮想デスクトップ環境においては、仮想マシンが常に生成される状態が継続することから、クラスタ上で DRS を有効にしている環境では、仮想マシンの ESXi ホスト間の移動が発生しやすくなります。可能な限り、DRS の移行のしきい値を優先順位 2 または優先順位 3（デフォルト）に設定してください。

3-1-2. セキュリティ VM の特性

NSX Manager と連携をして vCenter Server から ESXi ホストへ配信される Guest Introspection、DSVA は、セキュリティ VM として ESX Agent Manager(EAM)によって管理されています。



DSM は vCenter Server と同期をすることにより、ESXi ホスト、仮想マシンのインベントリ情報を取得しています。また、NSX Manager は ESXi ホスト上の Guest Introspection Service のステータスを監視するとともに、Guest Introspection サービスを提供する仮想マシン毎に 3rd Party 連携を提供するためのサービスプロファイルを

Context Multiplexer へ提供します。そして、Context Multiplexer は仮想マシン毎に TCP コネクションを DSVA に張ることにより保護対象仮想マシンの情報を提供します。

一方 Deep Security では、NSX セキュリティポリシー連携またはイベントベースタスク(EBT)により仮想マシンに対して有効化、セキュリティポリシーの配信が行われ、Deep Security のポリシーが適用されます。このタイミングで Context Multiplexer からの TCP コネクションが何らかの理由で張られていない場合、正常にセキュリティ機能を提供することができません。
また、DRS/vMotion により仮想マシンが他の ESXi ホストに移動した場合でも DSM は vCenter Server とリアルタイムに同期しているため、新たな ESXi ホスト上で有効化、セキュリティポリシーの配信を自動的に行うことができます。

上記仕様から、NSX Manager、DSVA は常に稼働している必要があります。
そして DSVA は EAM により以下のような制御もされています。

- ホスト起動時の起動順序
- vMotion/DRS による仮想マシン移動の制限
- ステータスチェックと異常検出時の再配信などの解決策の提供

3-1-3. Deep Security が付与する NSX セキュリティタグの特性

Deep Security は、不正プログラム対策イベントが発生した場合に NSX セキュリティタグを付与することができます。(その他のイベントをトリガーにしてセキュリティタグを付与することはできません。)
それぞれのセキュリティタグには異なる属性がありますので、実装時には留意をして設計を行ってください。

➢ 不正プログラム対策 セキュリティタグ

3 つのタグには差異はなく、仮想マシングループ毎にセキュリティタグが付与された際に適用される分散ファイアウォールルール(所属するセキュリティグループ)を変えたい場合に利用します。

AV セキュリティタグ	NSX セキュリティタグ	セキュリティタグ 付与条件
ANTI_VIRUS.VirusFound.threat=high	ANTI_VIRUS.VirusFound.threat=high	Deep Security ポリシーにて任意に設定可能
ANTI_VIRUS.VirusFound.threat=medium	ANTI_VIRUS.VirusFound.threat=medium	
ANTI_VIRUS.VirusFound.threat=low	ANTI_VIRUS.VirusFound.threat=low	

3-2. 導入時に留意しておくべきポイント

3-2-1. DSVA リソースチューニング後の OVF ファイルの更新

仮想マシンの集約率が高い環境や DSVA の機能を複数利用する場合、DSVA のリソースがデフォルト値以上に必要になることがあります。その場合には DSVA の OVF ファイル内の下記のパラメータを DSVA のデプロイ前に変更しておく必要があります。

NSX-T2.4 までは、DSM へ DSVA OVF をアップロード後、DSM インストールフォルダ配下の以下のフォルダに格納される dsva.ovf ファイルの中の以下のパラメータを修正することで変更が可能です。

<DSM_Install>¥temp¥Appliance-ESX-<appliance_version>

```
<Item>
  <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
  <rasd:Description>Number of virtual CPUs</rasd:Description>
  <rasd:ElementName xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">4 virtual CPU</rasd:ElementN
  <rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">1</rasd:InstanceID>
  <rasd:ResourceType>3</rasd:ResourceType>
  <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
</Item>
<Item>
  <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
  <rasd:Description>Memory Size</rasd:Description>
  <rasd:ElementName xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">6144 MB of memory</rasd:Elem
  <rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">2</rasd:InstanceID>
  <rasd:Reservation>6144</rasd:Reservation>
  <rasd:ResourceType>4</rasd:ResourceType>
  <rasd:VirtualQuantity>6144</rasd:VirtualQuantity>
</Item>
```

NSX-T2.5 以降の環境では、セクション 1.4.6 で記載の通り、NSX の仕様の変更に伴い、DSVA など 3rd Party Security VM を各ホストへデプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチェックを実行するプロセスが追加されています（ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署名が付与されます）。

※Deep Security11.0/NSX-T2.4 までのバージョンで可能であった上記方法（DSVA Zip アップロード後に DSM インストールフォルダの OVF ファイルの変更する方法）を NSX-T2.5 以降の環境行う場合、DSVA デプロイ時に NSX Manager によるデジタル証明書のチェックが行われるためデプロイに失敗します。

NSX-T2.5 以降では、VMware 社によるデジタル署名が付与されている Deep Security 12.0 Update 3 以降の OVF パッケージを必ず使用する必要があり、DSVA に割り振るリソースに応じて以下の 4 種類の OVF ファイルから選択をする必要があります。

OVF Files	vCPU	Memory
dsva.ovf	2	4096MB
dsva-small.ovf	2	8192MB
dsva-medium.ovf	4	16384MB
dsva-large.ovf	6	24576MB

デプロイの方法を含めて詳細、**セクション 1.4.6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更** を参照してください。

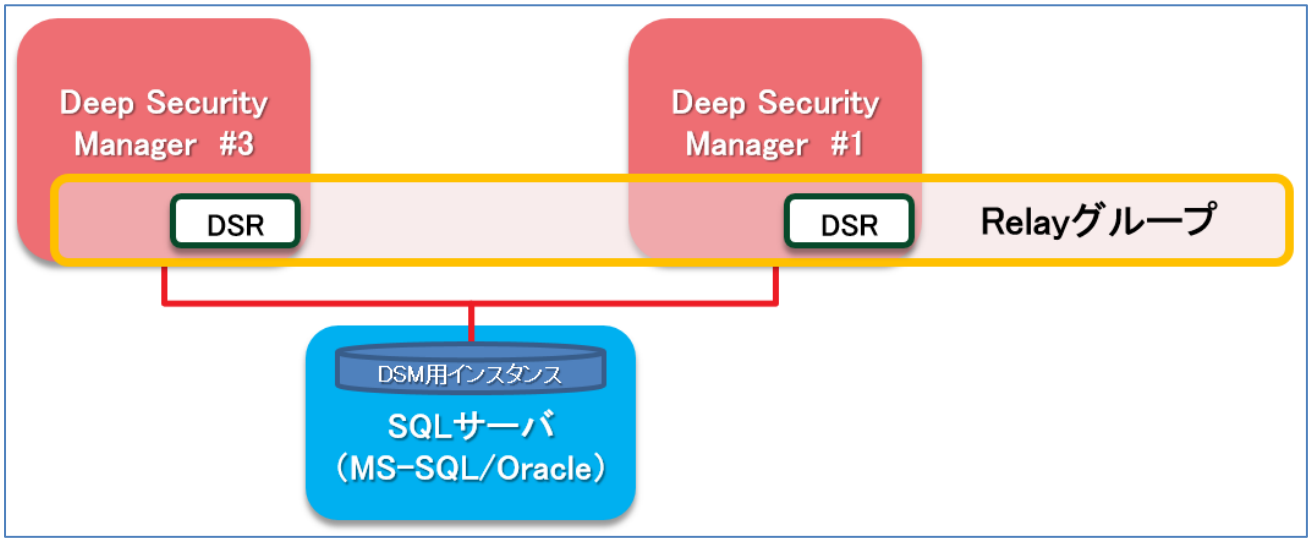
※ DSVA デプロイ後に vCenter Server から DSVA に対するリソースを変更することも可能ですが、DSVA の再

配信が発生した場合、パラメータ変更前の状態で再配信されてしまいますので留意が必要です。
本番環境では OVF ファイルの変更を行って運用することを推奨しています。

3-2-2. マルチノード DSM の導入手順

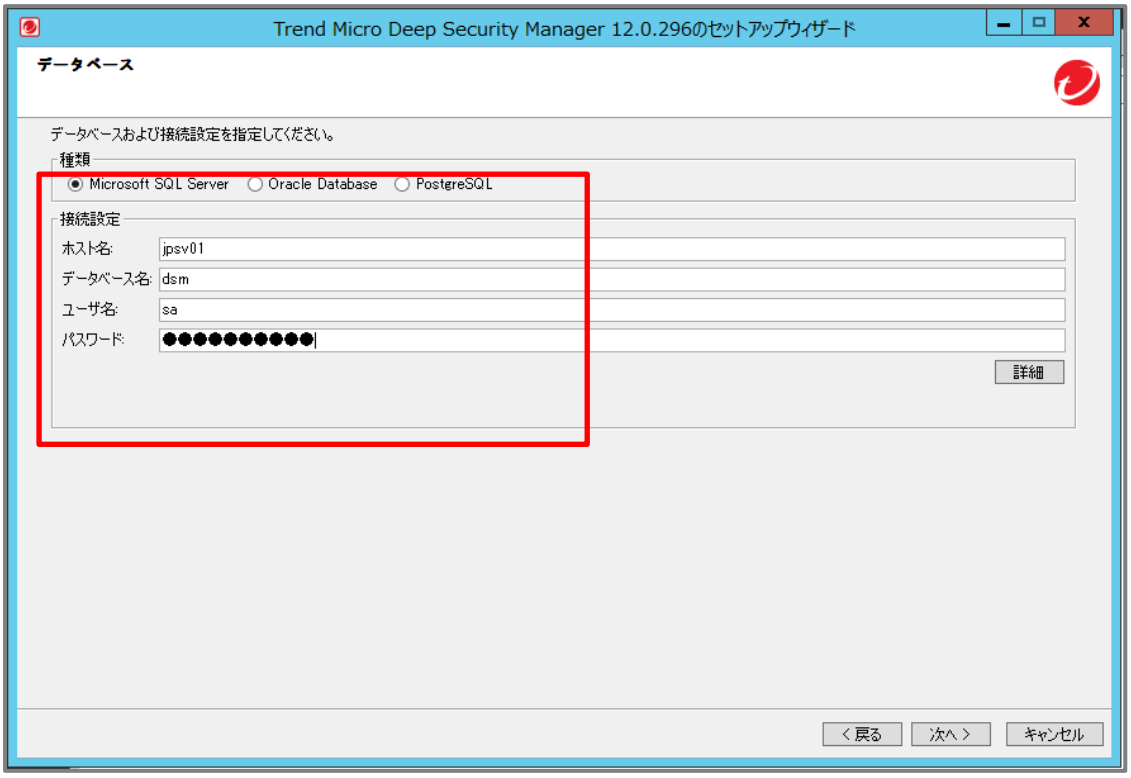
仮想デスクトップ(VDI)環境などにおいて、1000 台の仮想マシンを越える環境で運用する場合、2 台以上の DSM を配置することを推奨しています。DSM を増設することにより各仮想マシンに対する有効化処理や管理などの負荷分散を図ることが可能です。(複数のセキュリティ機能を利用する場合や有効化処理、ポリシー再配信などが頻繁に発生することでジョブの処理が多い場合には、1000 台以下であっても DSM の増設が必要な場合があります。)

- 1 台の DSM 用 SQL サーバに接続する DSM は最大 2 台までとすることを推奨しています。
- 各 DSM サーバのビルドは統一してください。

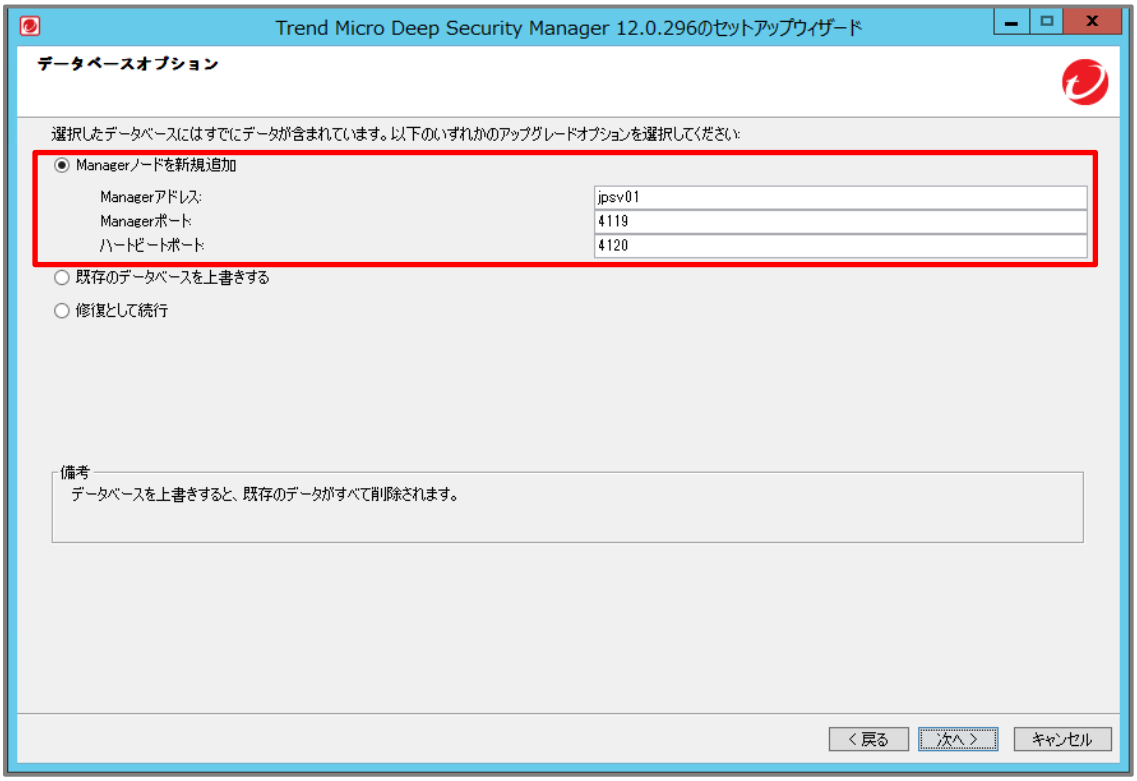


以下に DSM を増設するための手順を記載します。

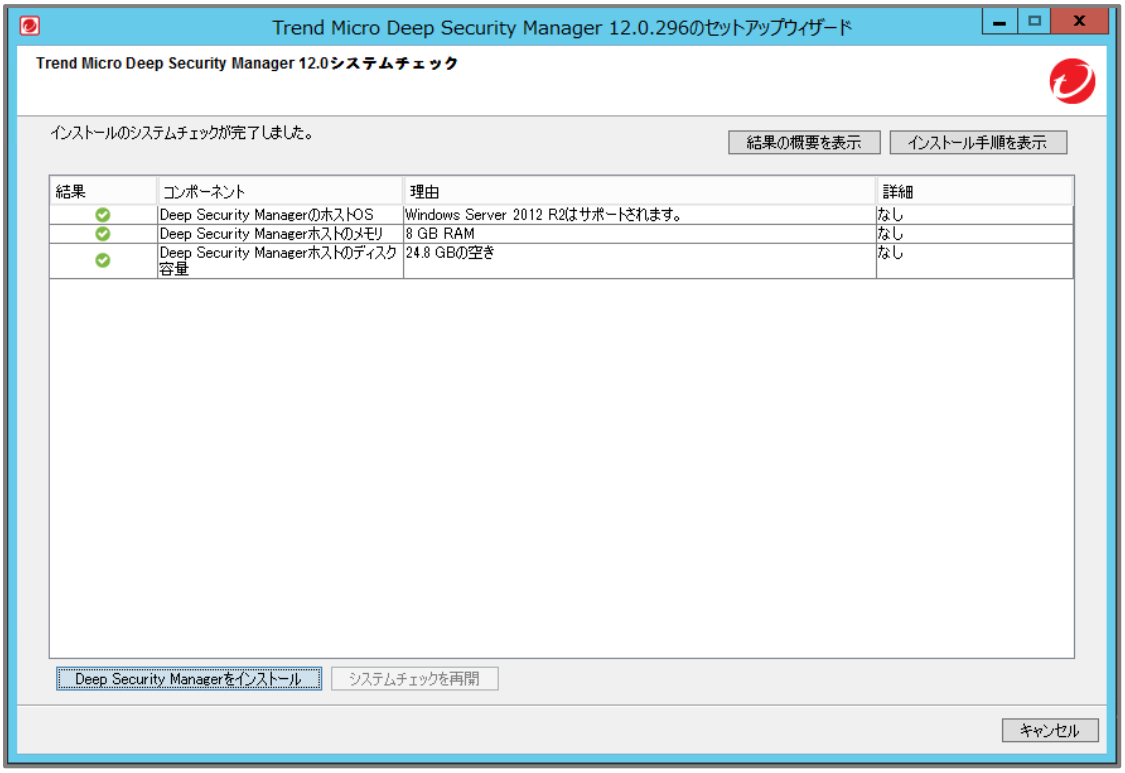
1) 新規に追加する DSM サーバ上で DSM インストーラを実行し、セットアップウィザードにてデータベースの接続設定まで進み、現在動作している SQL インスタンスを指定する（それまでの手順はセクション 2-3-2 を参照）



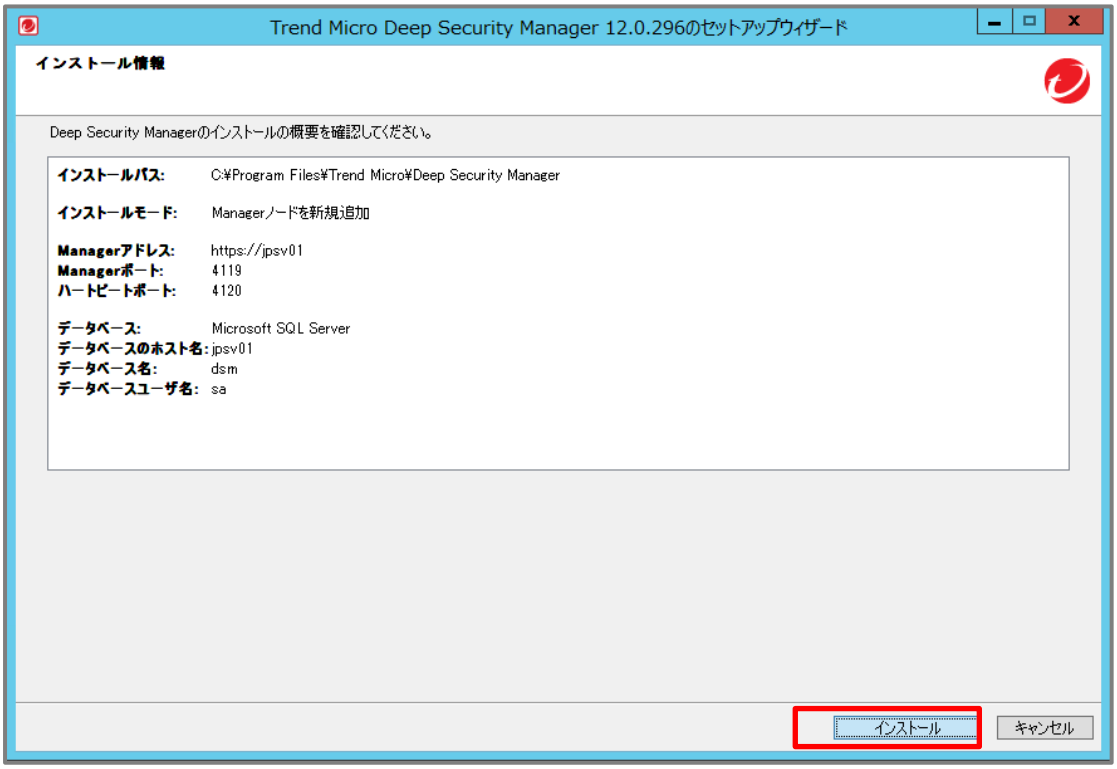
2) データベースオプションで**[Manager ノードを新規追加]**をクリックし、追加する DSM サーバの情報を設定する（Manager ポート、ハートビートポートは 1 台目の DSM と同様にする）



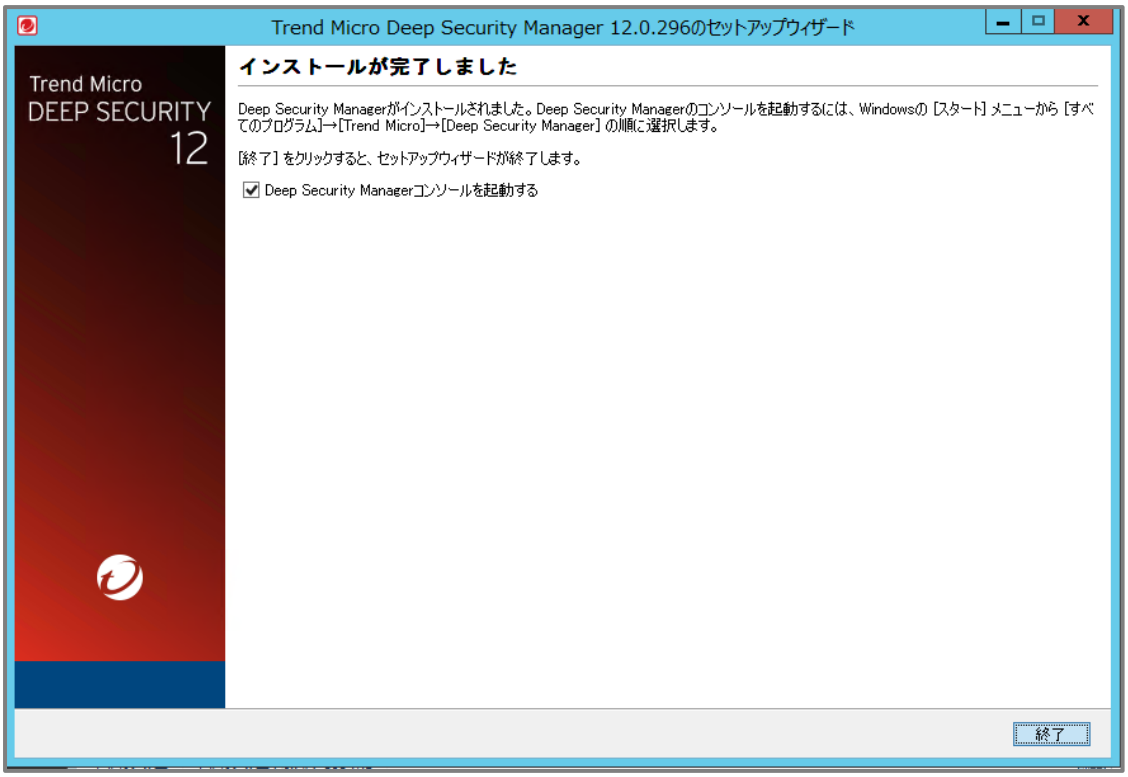
3）インストールチェックを行う



4）インストール情報を確認し、**[インストール]**ボタンをクリックする

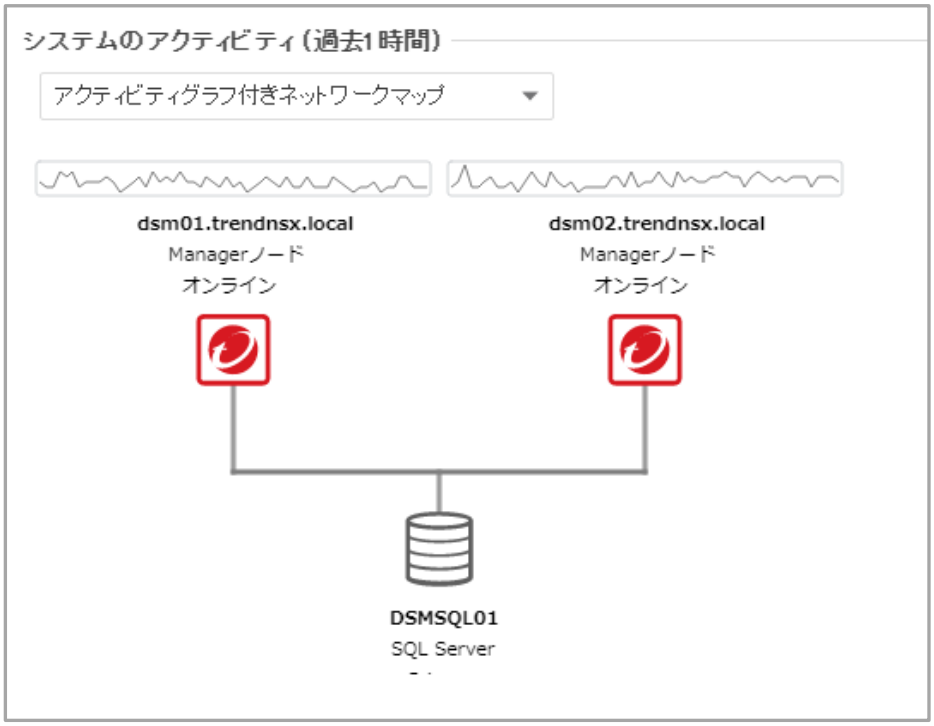


5) インストール完了を確認する



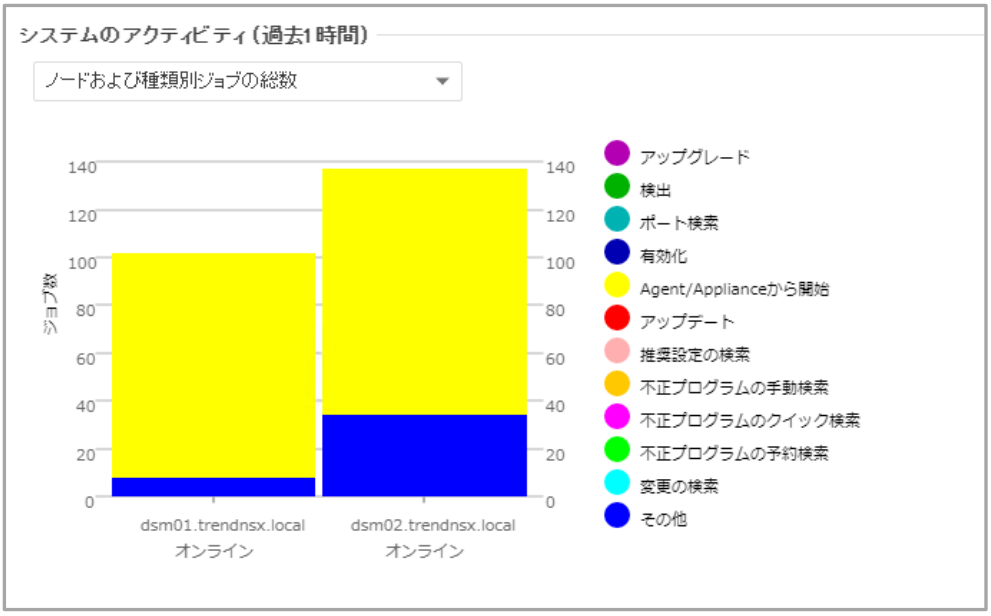
DSM へアクセスし、DSM が複数ノード SQL サーバに接続していることを確認することができます。

[管理]>[システム情報]>[システムノアクティビティ]>[アクティビティグラフ付きネットワークマップ]



- DSM が複数ノードで構成されると有効化処理やイベントの取得などは DSM 間で負荷分散することが可能となります。

- vCenter Server との同期処理については、最後に SQL サーバに接続された DSM サーバが行います。
  [管理]>[システム情報]>[システムノアクティビティ]>[ノードおよび種類別ジョブの総数]
  青い“その他”の部分の処理の中に vCenter との同期処理などが含まれています。



- NSX Manager とのコミュニケーションについては、デフォルトでは最初に SQL サーバに接続された DSM が行います。また、NSX Manager はその DSM サーバの URL 情報を保持し、ステータスを監視しています。

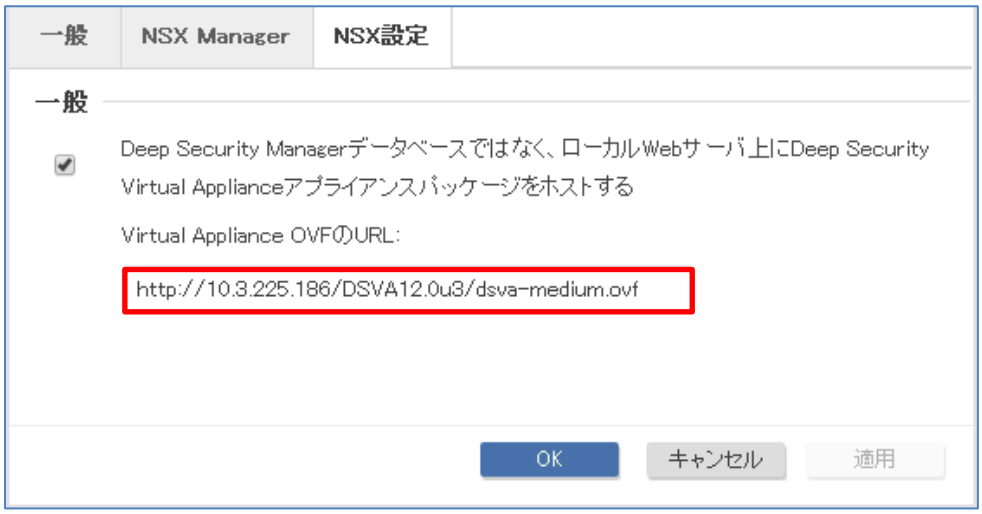
NSX Manager と通信をする DSM サーバは以下の設定により変更が可能です。
[管理]>[システム設定]>[詳細]>[NSX 通信の Manager ノード]

ここで指定された DSM サーバは DSVA を配信する際に NSX Manager が OVF ファイルをダウンロードするノードでもあります。
マルチノード DSM 環境では、コミュニケーションしている DSM サーバがメンテナンスなどでシャットダウンした場合、他の通信可能な DSM サーバの情報が NSX Manager 側に自動的に通知されます。
NSX Manager は DSVA の OVF ファイルのダウンロード先 DSM サーバの URL が更新されると、DSVA の再デプロイが必要と判断する仕様となっており、意図せず DSVA の再配信が発生します。

上記のような意図しない再配信を回避するためには、DSM にて DSVA OVF ファイルのダウンロード先 URL を明示的に設定してください。（一意の DSM サーバの DSVA パッケージアップロード URL または外部 Web サーバに格納したソフトウェアパッケージの URL を指定）

DSM の**[コンピュータ]**画面から連携している vCenter Server の[プロパティ]を選択して、[NSX Manager]で以下の設定を実施

- **[Deep Security Manager データベースではなく、ローカル Web サーバ上に Deep Security Virtual Appliance アプライアンスパッケージをホストする]** ： チェックボックスを入れる
- **[Virtual Appliance OVF の URL]** ： 特定の DSM サーバまたは OVF ファイルを格納した外部 Web サーバ



指定した NSX Manager からも以下の画面で OVF ファイルの URL が確認できます。

[ネットワークとセキュリティの詳細設定]＞[パートナーサービス]＞[カタログ]＞[登録されたサービス]

3-3. 管理サーバ群を DSVA で保護する場合の考慮事項

vCenter Server や DSM サーバを配置する ESXi ホストを DSVA で保護することも可能です。ただし、管理サーバである DSM を管理される DSVA で保護する場合、障害発生時の切り分けに時間を要することが懸念されます。そのような環境に DSM を配置する場合には、DSM と同居している DSR(リレー化した DSA)にてセキュリティ保護を行うことを推奨しています。

Deep Security では DSA と DSVA を同時に稼動させるコンバインモードの実装が可能です。
コンバインモードの特徴は以下のとおりです。

- DSVA が動作する ESXi ホスト上に DSA がインストールされた仮想マシンが配置されると自動的にコンバインモードとして動作します。
- コンバインモードでは機能ごとに DSA または DSVA を使い分けることができます。

- コンバインモードの動作仕様は以下の 4 つから選択可能です(DS9.6 ではデフォルトから変更不可)
  - **Appliance 優先** ： Appliance 障害時に Agent にてセキュリティ機能継続
  - **Agent 優先** ： Agent 障害時に Appliance にてセキュリティ機能継続
  - **Appliance のみ** ： Appliance 障害時に Agent へのセキュリティ保護移行を行わない
  - **Agent のみ** ： Agent 障害時に Appliance へのセキュリティ保護移行を行わない
- デフォルトでは以下のように動作します。
  - **不正プログラム対策** ： **Appliance 優先**
  - **Web レピュテーション/ファイアウォール/侵入防御** ： **Agent 優先**
  - **変更監視** ： **Appliance 優先**
  -

コンバインモードとなっている DSM サーバは、すべての機能を**“Agent のみ”**にて設定することをご検討ください。(Deep Security では DSM と同居する DSA のライセンスはかかりません)

3-4. 仮想デスクトップ環境における NSX、DSVA のサイジング

NSX 環境において、DSVA を利用したエージェントレスによる仮想デスクトップの保護を行う場合のサイジング、導入時に必要となるチューニングについて記載します。

サイジングについては、運用開始後のチューニング、ノード追加はシステム影響、作業工数に影響がありますので、できる限り余裕をもった設計を行うことを推奨します。

Deep Security に関する各種パフォーマンス情報は、DSM 上から確認することができます。

[管理]>[システム情報]>[システムの詳細]>[Manager ノード]

3-4-1. DSM サーバのサイジング指標

- **リソースの割り当て**
  - 不正プログラム対策を利用して 500～1000 台程度の仮想デスクトップを保護する場合には、DSM アプリケーション用として以下のリソースを割り当てることを推奨します。(DSM 用 SQL データベースを別サーバに構築することを前提)
    - **4vCPU**
    - **メモリ 8GB(サーバに対しては OS のオーバヘッドを考慮して 12GB 程度)**
    - **ディスク 10GB 以上**
      すべての構成・イベント情報をデータベースに保存するため、プログラム自体のディスク容量としては 5GB 程度確保いただければ問題ありませんが、障害発生時など、デバッグレベルのログを生成する場合は一時的に大量のログを保存する場合があるため
  - IOPS については OS およびデータベースの使用を満たしていれば問題ありません。
  - 1000 台を超える仮想デスクトップ環境を保護する場合、または DSM の冗長化が必要な場合には、DSM の増設(同一データベースインスタンスへの接続)を推奨します。
  - 仮想デスクトップ環境において、DSVA による不正プログラム対策のみを利用する場合、VDI1000 台から 1200 台毎に DSM を増設することを推奨します。
    - 「不正プログラム対策エンジンがオフライン」エラーの発生がないこと、Deep Security システム全体として稼働に問題がないと判断される場合には、リソース使用状況に応じてそれ以上の台数を収容しても問題ありませんが、導入初期段階から本指標以上を前提とした構成は推奨しておりません。)
    - フルクローンの固定割り当て型の場合には、DSM での仮想マシンへの有効化処理などのジョブが多くなく、比較的多くの仮想デスクトップ端末を DSM で管理することができる傾向にあります。一方リンククローンやインスタントクローンなどフローティング割り当てが採用されている場合には、常に仮想デスクトップ端末の有効化処理やポリシー配信などのジョブ処理が DSM 上で行われることになるため、DSM での管理台数をベースとして上記指標をベースに構成いただくことを推奨しています。
  - 同一データベースインスタンスに対する DSM の接続は 2 台までとして DSM セットを構成することを推奨しています。
  - 仮想デスクトップ環境の場合、vCenter 1Block あたりに1DSM セットで構成してください。
  - DS が利用するコンポーネント間の通信に関しては最低 1Gbps の帯域を推奨しています。

- **【TIPS】DSM アプリケーションに対するメモリ割り当て**

DSM は標準インストール状態では OS に割り振っているメモリ容量に関わらず、4GB までしかメモリを使用しないように制御されています。物理リソースの割り当て以外に必ず以下の手順に添って、DSM アプリケーションの最大メモリ使用量の変更を行ってください。

1) Deep Security Manager のインストールディレクトリに移動する（Deep Security Manager の実行可能ファイルと同じディレクトリ）

2) 新しいファイルを作成し、プラットフォームに応じて、次のようにファイル名を設定する。

- **Windows ： Deep Security Manager.vmoptions**
- **Linux ： dsm_s.vmoptions**

3) ファイルに「-Xmx10g 」という行を追加する
（この例では「10g」を指定することにより、Deep Security Manager で 10GB のメモリを使用可能となる）

4) ファイルを保存し、Deep Security Manager を再起動します。

5) **[管理]＞[システム情報]** に進み、**[システムの詳細]＞[Manager ノード]＞[メモリ]** を展開して、**[最大メモリ]** に新しいパラメータが反映されていることを確認する

- **仮想デスクトップ環境におけるパフォーマンスプロファイルの変更による DSM のジョブ処理能力の向上**

DSM の各種処理はすべてジョブとして管理されており、ジョブの同時処理能力は CPU に依存しています。そのため、DSM における有効化処理、ポリシー配信が遅いなどの事象が発生する場合には、

- DSM に対する vCPU の追加割り当て
- DSM の増設

を検討する必要があります。
また、1000 台を超える仮想マシンの保護を行う場合、短期間にジョブ処理が集中することにより処理遅延、有効化の失敗などが発生する場合があります。その場合には、パフォーマンスプロファイルの変更を行うことで処理効率を向上することが可能となります。
必要に応じて、以下の FAQ よりパフォーマンスプロファイルをダウンロードして適用してください。
http://esupport.trendmicro.com/solution/ja-JP/1119051.aspx
※DSM サーバが複数ノード存在する場合には全ノードで適用してください。
※パフォーマンスプロファイルは、DSM アプリケーションが正常に動作できるように考慮したチューニングがされていますので、お客様独自でカスタマイズすることは避けてください。必要な場合には弊社までご相談ください。

3-4-2. DSM 用 SQL サーバのサイジング指標

➢ **DSM アプリケーションとの同居について**

DSM と SQL データベースを同一サーバで稼動することは可能ですが、仮想デスクトップ環境を保護する場合、または一定以上の規模で展開する場合には、DSM サーバと DSM 用 SQL サーバを別仮想マシンとして構築してください。

SQL サーバについては必ずしも DSM サーバ専用に用意する必要はありません。

ただし、vCenter Block が複数ある場合に、同一 SQL サーバにインスタンスを複数作成して、2 つ以上の DSM セットを接続することはパフォーマンス面から推奨していません。

➢ リソースの割り当て

データベースのシステム要件に従い、サイジングを行っていただくことが前提となりますが、DSM からのデータベースアクセスのボトルネックにならないように設定することが重要です。

- **4～8vCPU**
- **メモリ 8～16GB**
- ディスクについては、イベント発生量やイベント保持期間設定により、必要なディスク容量は大きく異なります

  以下の FAQ を参考にデータベース容量のサイジングを行ってください。

  http://esupport.trendmicro.com/solution/ja-JP/1310096.aspx

※Microsoft SQL を想定

また、DSM のパフォーマンスに問題がないにもかかわらず、多くのジョブが滞留するような場合には、SQL サーバ側で「max worker threads」などの値をチューニングすることで改善できる場合があります。

3-4-3. DSVA のサイジング指標

DSVA に割り振るリソースについては、Deep Security で利用する機能により判断をする必要があります。

➢ **不正プログラム対策のみ使用する場合のリソースの割り当て**

- 仮想デスクトップ環境ではホストあたりの仮想デスクトップ集約率は 100～120 台程度を推奨します。
- 不正プログラム対策のフルスキャンを行う場合は、DSVA のリソース、対象ストレージに IOPS、同時実行数に考慮が必要です。
- VMware NSX では Guest Introspection Service を展開している場合のホストの最大集約率が定義されています。NSX-T 環境では 250 台が ESXi ホストあたりの最大仮想デスクトップとして定義されていますが、この値は仮想デスクトップの保護完了が即時に行われることを保証する値ではありません。水準の集約率で DSVA の保護を利用した場合、ユーザが仮想デスクトップのログインを完了するまでにセキュリティ保護が完了しない事象が発生する可能性が高まります。NSX の要件も含めて 100-120 台の集約率に抑えて設計することを強く推奨します。

  上記情報は VMware Configure Maximum で確認可能です。

  https://configmax.vmware.com/

  Deep Security において最大要件は明示していませんが、Deep Security のセキュリティ機能を安定して適応するために集約率は 100-120 台/1ESXi に収めるようにしてください。

- 集約率が高くない場合には、2vCPU/4-10GB メモリ）で対応可能なケースが多いと想定されます。環境に応じてサイジングを決定してください（なるべく 8-10GB の割り振りができることが理想です。）
- ESXi ホストあたりの仮想マシンの集約率が 100 台を超える場合、4vCPU/10～12GB メモリを割り当てることを推奨します。
- 集約率が 150 台近くなる場合には、上記に加えてさらに 2vCPU/4GB メモリの追加を検討してください。（あくまで弊社で確認をした実績ベースであり、指標として検討してください。環境によってそれ以上のリソースが必要になる場合があり、NSX 側のパフォーマンスとの兼ね合いも出てくるため、できる限り集約率はそれよりも余裕がある設計にすることを強く推奨します。）
- 予約検索を実行するは環境によって検索に要する時間が異なります。お客様環境に応じて同時検索台数を 5 台以上に設定する場合には、適宜 CPU、メモリの割り当てを増やすことが必要になる場合があります。（不正プログラム対策のフルスキャンを行う場合は、DSVA のリソース、対象ストレージに IOPS、同時実行数に考慮が必要となるため）

3-4-4. DSR のサイジング指標

DSR は通常 DSM と同居してインストールされます。DSVA によるエージェントレス型セキュリティを利用する場合、DSR はパターンファイルやコンポーネントのダウンロード機能に加えて、DRS/vMotion 時の DSVA 巻の設定以降に利用されるため、DSM ノードと同居させることで、同数以上の DSR を配置することを推奨します。

- **リソースの割り当て**
  - DSM と DSR が同居している場合には、DSR 用に CPU/メモリを追加する必要はありません。DSM サーバが直接インターネットに接続できない場合など、DSR を単体で配置する場合、DSA のシステム要件に従ってサイジングを行ってください。
  - DSR はエンジン、ルール、パターンファイルなどのコンポーネントに加え、DSA などのアップグレード用プログラムを配信するためにローカルディスクを使用します。配信用データを格納するために 10GB 程度のディスク容量を確保してください。

4. 参考資料

本ガイドのほかに、必要に応じて以下の情報を参照してください。

- **全般情報**
  - Trend Micro Deep Security サポートウェブ
    http://esupport.trendmicro.com/ja-jp/enterprise/ds/top.aspx
  - NSX と Trend Micro Deep Security DSVA 9.5/9.6/10.0 トラブルシューティングガイド
    https://campaign.vmware.com/imgs/apac/jp_dwn/PDF/techresources/DSVA_9.5-10TroubleshootingTips_NSX_r2.1.pdf
  - Deep Security＋VMware NSX 関連情報（ブログ、アーキテクチャなど）
    https://www.trendmicro.com/ja_jp/business/campaigns/vmware.html

- **バージョンアップ**
  - Deep Security12.0 アップグレードガイドブック(DSVA 編)
    http://files.trendmicro.com/jp/ucmodule/tmds/doc/ds12_upgradeguide_dsa.pdf