



構築ガイド

## Windows Server 2008 R2 Failover Cluster 構築ガイド

ウイルスバスター コーポレートエディション

11.0

[分類]

2015/09/28

トレンドマイクロ株式会社

Copyright (c) 2015 Trend Micro Incorporated. All Rights Reserved.

- 本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。
- 本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。
- 本ドキュメントおよびその記述内容は予告なしに変更されることがあります。
- TRENDMICRO、ウイルスバスターは、トレンドマイクロ株式会社の登録商標です。
- 本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

## ドキュメントコントロール

### 改訂記録

版	改訂内容	改訂日時	改訂者
Ver1.0	初版作成	2015/09/28	トレンドマイクロ

## 目 次 一 覧

### 【本文目次】

構築ガイド .....	1
<b>Windows Server 2008 R2 Failover Cluster 構築ガイド.....</b>	<b>1</b>
<b>1. はじめに .....</b>	<b>4</b>
1.1. ドキュメントの目的.....	4
<b>2. 事前準備 .....</b>	<b>5</b>
2.1. Windows Server 2008R2 Failover Cluster 環境の構築.....	5
2.2. 想定環境.....	5
2.3. 事前に確認するポイント .....	6
<b>3. ウイルスバスターCorp.11.0 のインストール.....</b>	<b>7</b>
3.1. Node A でウイルスバスターCorp.11.0 のインストーラを開始.....	7
3.2. Node A でウイルスバスターCorp.のサービスを停止.....	22
3.3. 共有ディスクの所有者ノードの変更と PCCSRV フォルダの削除.....	22
3.4. Node B でウイルスバスターCorp.11.0 のインストーラを開始 .....	24
3.5. IIS の認証設定 .....	39
3.6. ウイルスバスターCorp.のフォルダ権限設定.....	42
3.7. ウイルスバスターCorp. サービススタートアップ設定 .....	48
3.8. Cluster Generic Script の作成.....	50
3.9. High availability Cluster Generic Script の作成.....	52
3.10. ウイルスバスターCorp. サービスの役割設定.....	59
3.11. サービスの依存性設定 .....	65
3.12. レジストリのレプリケーション設定 .....	72
3.13. サービスの役割を起動 .....	73
3.14. 共有フォルダの設定.....	75
3.15. ウイルスバスターCorp.クライアントの設定.....	86

## 1. はじめに

### 1.1. ドキュメントの目的

このドキュメントはウイルスバスター コーポレートエディション (以下、ウイルスバスターCorp.) 11.0 サーバを Windows Server 2008 R2 Failover Cluster 上で稼働させるための設定ガイドになります。

#### ご注意

本ドキュメントでは Windows Cluster 上でウイルスバスターCorp.11.0 サーバを稼働させるための最低限の内容のみを記載しています。

Windows Cluster に関する詳細な情報はマイクロソフト社様へご確認下さい。

## 2. 事前準備

### 2.1. Windows Server 2008R2 Failover Cluster 環境の構築

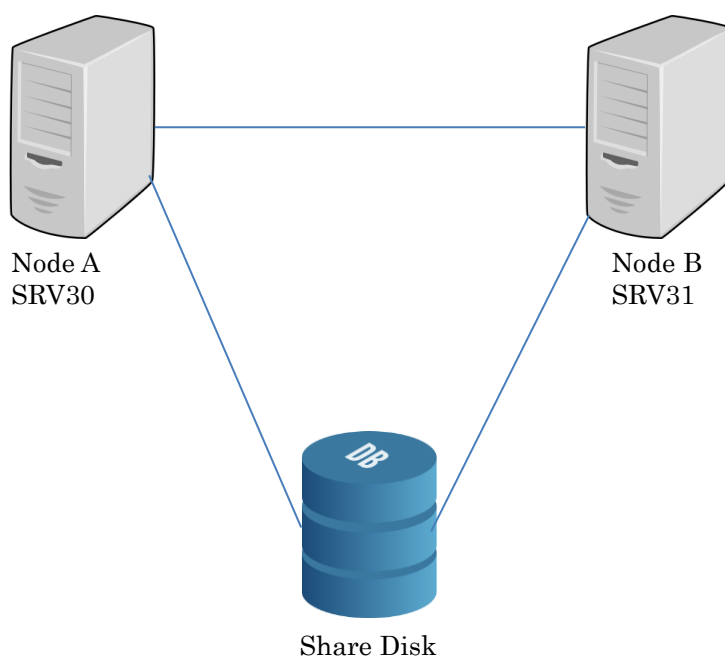
事前に Windows Server 2008 R2 上で、Failover Cluster の環境を構築します。

Failover Cluster の構築手順についてはマイクロソフト社のドキュメントなどをご参照下さい。

また、ウイルスバスター Corp.サーバは Active/Passive 構成のみサポートしています。

### 2.2. 想定環境

本ドキュメントでは以下の Cluster 環境を構築済みとして解説しています。



サーバ名	O.S	ソフトウェア	補足
SRV30.odin.local	Windows Server 2008 R2	ウイルスバスター Corp. 11.0	Node A プライマリノード
SRV31.odin.local	Windows Server 2012 R2	ウイルスバスター Corp. 11.0	Node B セカンダリノード
Storage.odin.local (Share Disk)	Windows Server 2012R2	-	Share Disk

## 2.3. 事前に確認するポイント

### 2.3.1. IIS のセットアップ

ウイルスバスターCorp. 11.0 のインストール時には Web サーバとして、IIS か Apache を選択することができますが、Windows Failover Cluster 環境へインストールする場合は必ず IIS を選択する必要があります。

IIS は事前にセットアップを完了させておく必要があります。

ウイルスバスターCorp.11.0 のインストール前に IIS のセットアップを完了させて下さい。

<http://esupport.trendmicro.com/solution/ja-JP/1306142.aspx>

### 2.3.2. Windows Failover Cluster の FQDN と IP アドレス

ウイルスバスターCorp.11.0 のインストール時に、ウイルスバスターCorp.クライアントがサーバを識別する値を設定する必要があります。

Windows Failover Cluster 環境では Cluster の FQDN か IP アドレスを指定する必要があります。

Cluster の FQDN、IP アドレスは Failover Cluster Manager で確認することができます。

### 2.3.3. ご参考

*Windows Server 2008*、*Windows Server 2008 R2*、または *Windows Server 2012* フェールオーバークラスターで *IIS 7.0* 以降の *World Wide Web* 発行サービスを構成する

<https://support.microsoft.com/en-us/kb/970759/ja>

### 3. ウイルスバスターCorp.11.0 のインストール

本手順は Node A、Node B それぞれで実施する必要があります。

#### 3.1. Node A でウイルスバスターCorp.11.0 のインストーラを開始

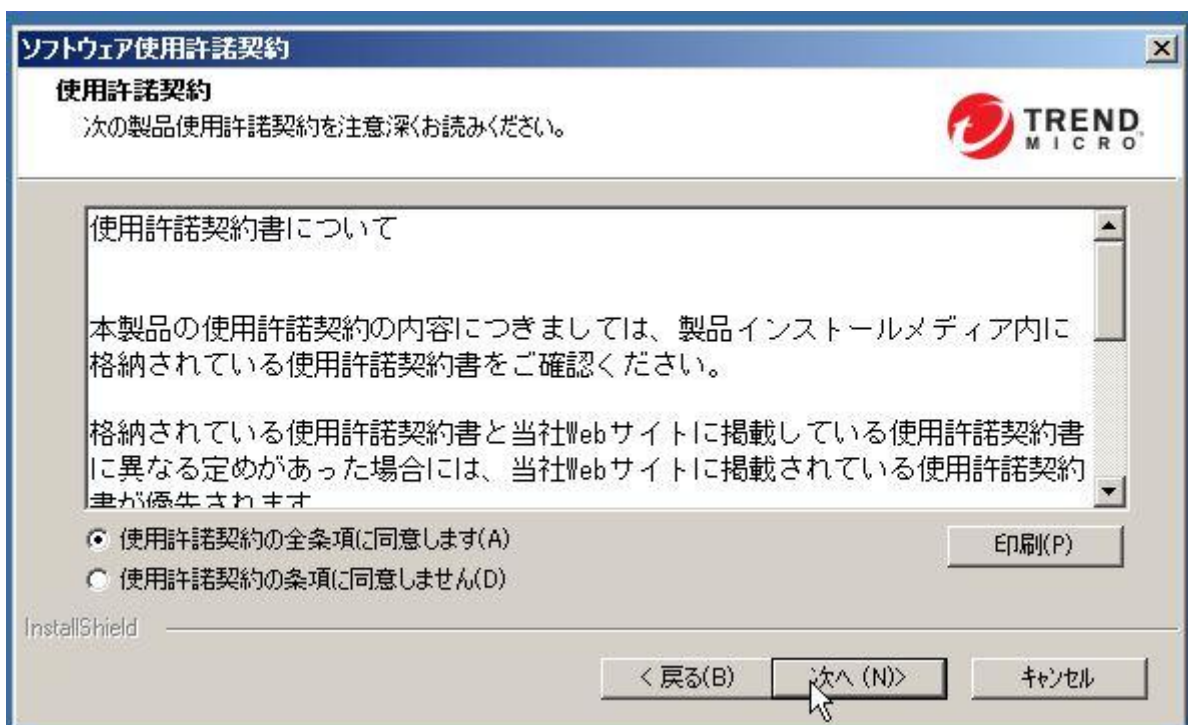
##### 3.1.1. インストーラを起動し、「開始」を選択します。



### 3.1.2. 「次へ」を選択します。

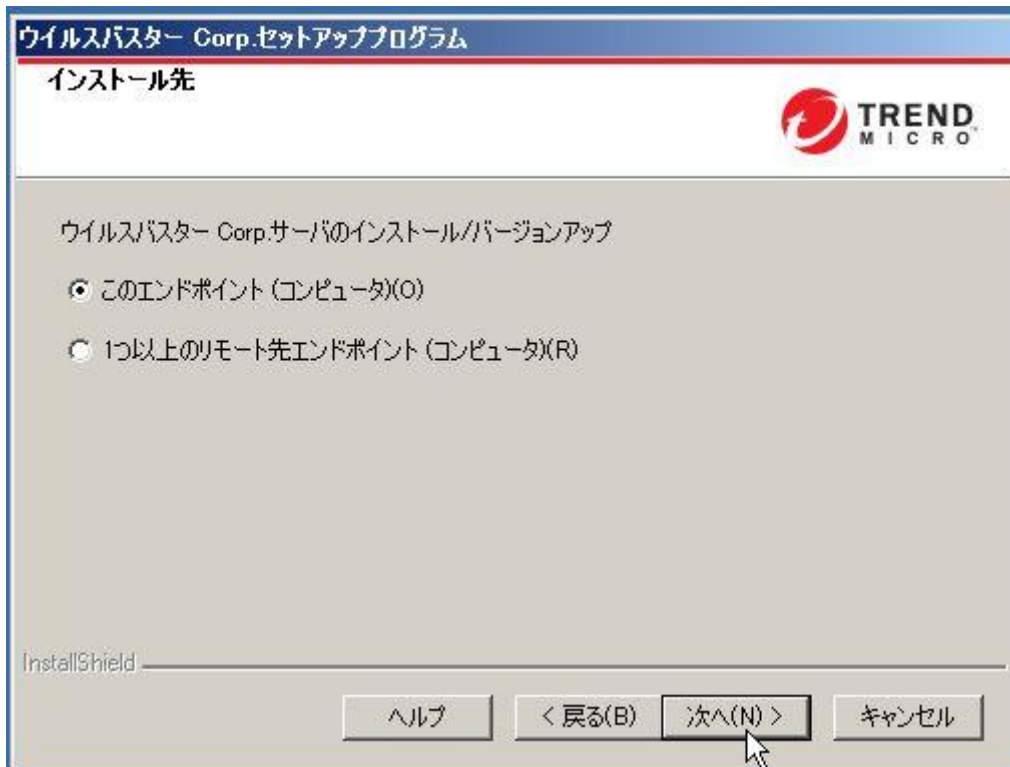


### 3.1.3. 使用許諾を読み、「同意します」にチェックを入れ「次へ」を選択します。

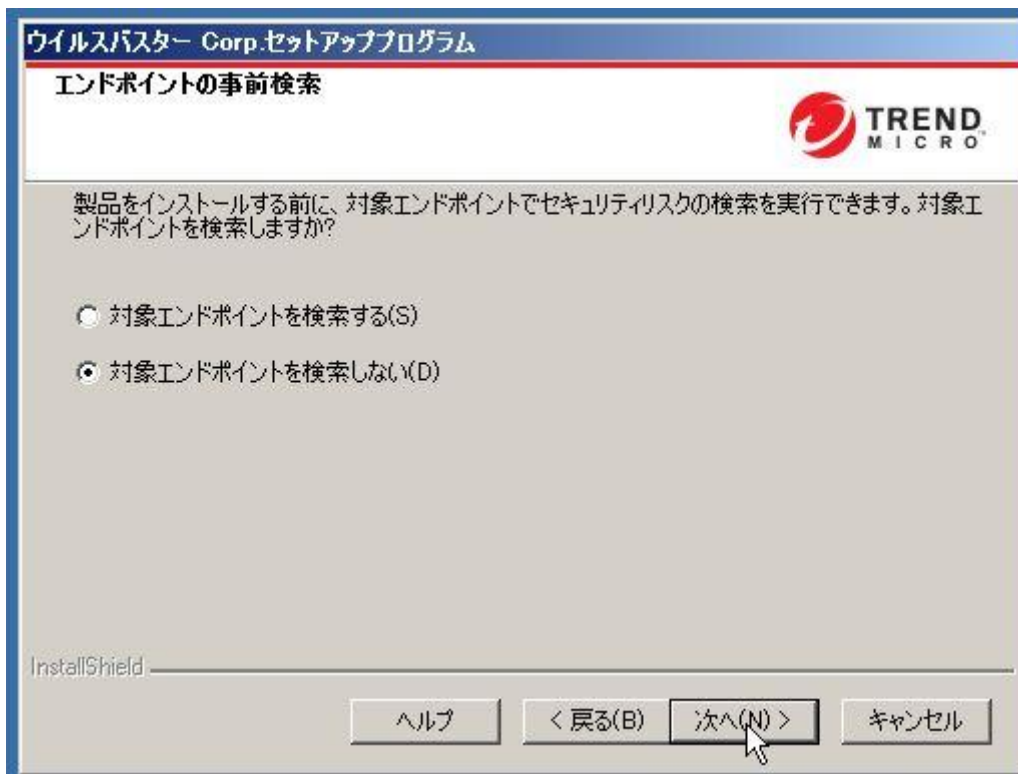




3.1.4. インストール先を選択し、「次へ」を選択します。

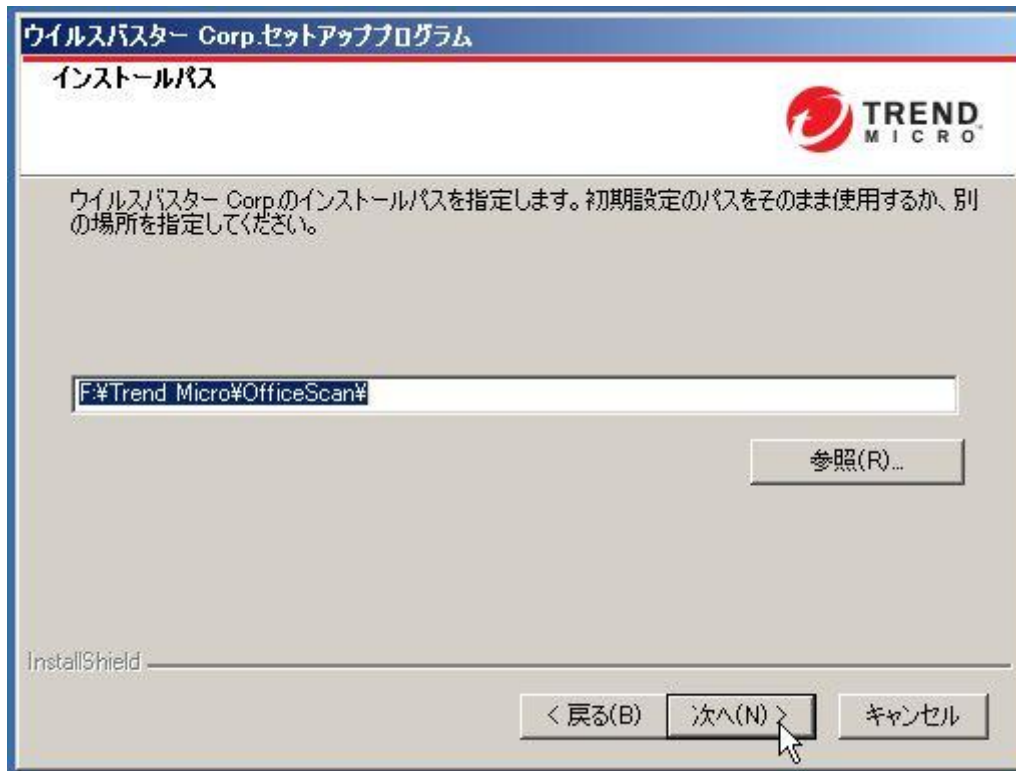


3.1.5. インストール先を事前に検索するか選択し、「次へ」を選択します。



### 3.1.6. 製品のインストールパスを指定します。

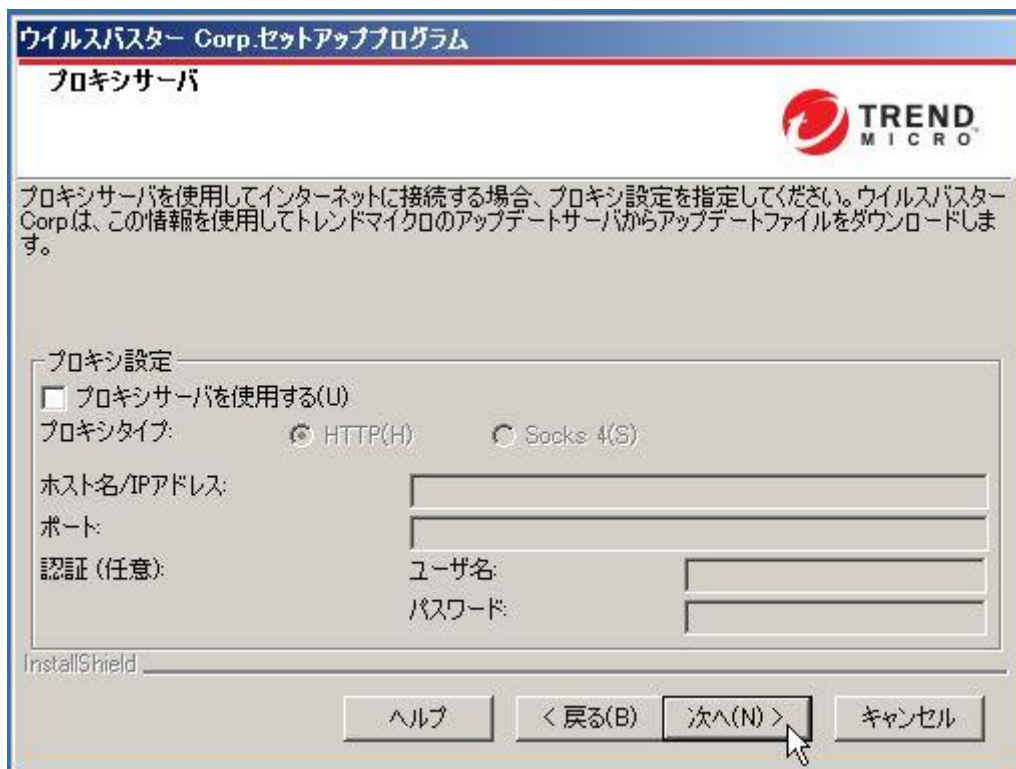
インストール先として、Cluster の共有ディスクを指定するため、「参照」を選択します。



Cluster の共有ディスクを指定します。

Cluster の共有ディスクが指定された事を確認し、「次へ」を選択します。

### 3.1.7. プロキシサーバの利用の有無を選択し、「次へ」を選択します。



3.1.8. Web サーバとして IIS が選択されている事を確認し、「次へ」を選択します。



IIS が選択されていない場合、IIS のセットアップが正しく行われていません。  
ウイルスバスターCorp.11.0 のインストール前に IIS のセットアップを完了させて下さい。

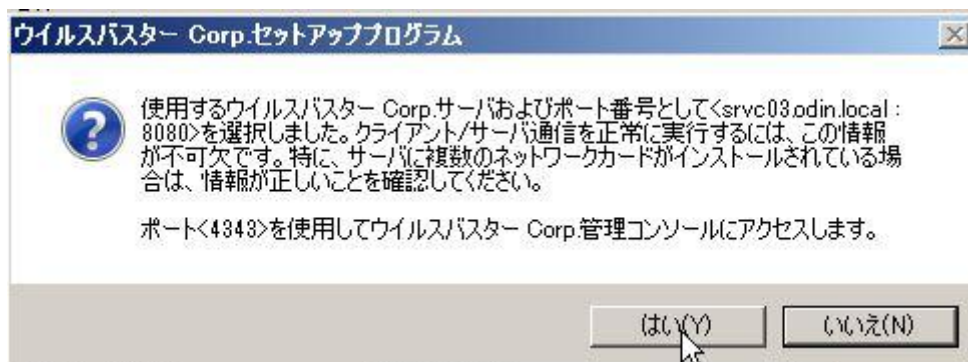
<http://esupport.trendmicro.com/solution/ja-JP/1306142.aspx>

### 3.1.9. サーバの識別名として、Cluster の FQDN または IP アドレスを指定し、「次へ」を選択します。



※Cluster の FQDN、IP アドレスは Failover Cluster Manager で確認することができます。


Cluster の FQDN、IP アドレスを選択すると以下の警告が表示されますが、「はい」を選択し、インストールを進めます。



### 3.1.10. 製品のアクティベーションコードを入力します。「次へ」を選択します。

**ウイルスバスター Corp.セットアッププログラム**

**製品のアクティベーション**  
 ステップ1: アクティベーションコードの入手



製品のアクティベーションは2つのステップで実施します。

1. アクティベーションコードを入手します。
2. アクティベーションコードを入力します。

アクティベーションコードはライセンス証書等に記載されています。レジストレーションキーが記載されている場合は、下の「オンライン登録」ボタンからユーザ登録を行い、アクティベーションコードを入手します（メールで送信されます）。

オンライン登録(R)


InstallShield

ヘルプ

事前に準備済みのアクティベーションコードを入力し、「次へ」を選択します。

**ウイルスバスター Corp.セットアッププログラム**

**製品のアクティベーション**  
 ステップ2: アクティベーションコードの入力



次の形式を使用して、ウイルスバスター Corp.サービスのアクティベーションコードを入力します。(コード形式: XX-XXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX)

ウイルス対策:

☐ ダメージクリーンナップサービス、Webレピュテーション、およびスパイウェア対策に同じアクティベーションコードを使用します

ダメージクリーンナップサービス:

Webレピュテーションおよびスパイウェア対策:

InstallShield

ヘルプ

### 3.1.11. クライアントの方式を選択し、「次へ」を選択します。





### 3.1.12. 統合 Smart Protection Server のインストールの有無を選択し、「次へ」を選択します。



**ウィルスバスター Corp. セットアッププログラム**

**統合 Smart Protection Server のインストール**

ウィルスバスター Corp. サーバに統合 Smart Protection Server をインストールすることができます。Smart Protection Server はファイルレピュテーションおよび Web レピュテーションを提供し、Deep Discovery Advisor と連携します。

スタンドアロンの Smart Protection Server をインストールすることをお勧めします。スタンドアロンは統合版と同等の機能を提供する一方で、より多くのクライアントをサポートします。

統合サーバをインストールしますか?

☐ いいえ、スタンドアロンの Smart Protection Server をすでにインストールしているか、後でインストールする予定です。

☒ はい、統合 Smart Protection Server をインストールします (ファイルレピュテーションサービスに SSL を使用)。

SSL 設定

証明書の有効期間:	3 年
SSL ポート:	4343

ヘルプ    < 戻る(B)    次へ(N) >    キャンセル

### 3.1.13. 対象のエンドポイントにウイルスバスター Corp. クライアントをインストールするかを選択し、「次へ」を選択します。



**ウィルスバスター Corp. セットアッププログラム**

**ウィルスバスター Corp. クライアントのインストール**

対象エンドポイントにウイルスバスター Corp. クライアントをインストールする場合に選択します。

☐ ウィルスバスター Corp. クライアントをインストールする(O) (ServerProtect for NT がインストールされているエンドポイントにはインストールできません)

ヘルプ    < 戻る(B)    次へ(N) >    キャンセル

### 3.1.14. スマートフィードバックを有効にするかを選択し、「次へ」を選択します。



ウイルスバスター Corp.セットアッププログラム

Smart Protection Network

TREND MICRO

TREND MICRO™ SMART PROTECTION NETWORK

Trend Micro Smart Protection Networkは、最新の脅威に対してプロアクティブな保護を提供するように設計された、次世代のクラウド-クライアント型のコンテンツセキュリティ基盤です。

☒ Trend Micro スマートフィードバックを有効にする (推奨)

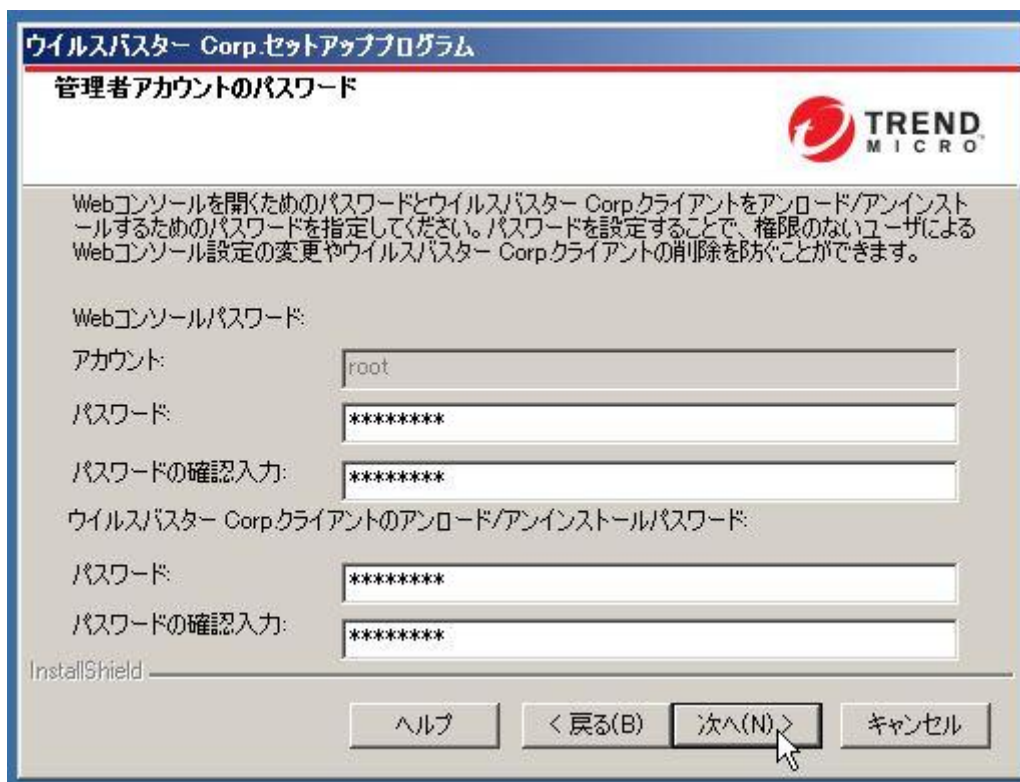
本機能を有効にすると、コンピュータで検出された脅威情報（アクセスされたWebアドレス、ファイルに関する情報等）がトレンドマイクロに送信され、新たな脅威の迅速な識別や対処に役立てられます。本機能は製品コンソールを介しても無効にできます。スマートフィードバックは製品コンソールからいつでも無効にできます。

業種 (オプション): 指定なし

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

### 3.1.15. 管理者用のアカウントを設定し、「次へ」を選択します。



ウイルスバスター Corp.セットアッププログラム

管理者アカウントのパスワード

TREND MICRO

Webコンソールを開くためのパスワードとウイルスバスター Corp.クライアントをアンロード/アンインストールするためのパスワードを指定してください。パスワードを設定することで、権限のないユーザによるWebコンソール設定の変更やウイルスバスター Corp.クライアントの削除を防ぐことができます。

Webコンソールパスワード:

アカウント: root

パスワード: \*\*\*\*\*

パスワードの確認入力: \*\*\*\*\*

ウイルスバスター Corp.クライアントのアンロード/アンインストールパスワード:

パスワード: \*\*\*\*\*

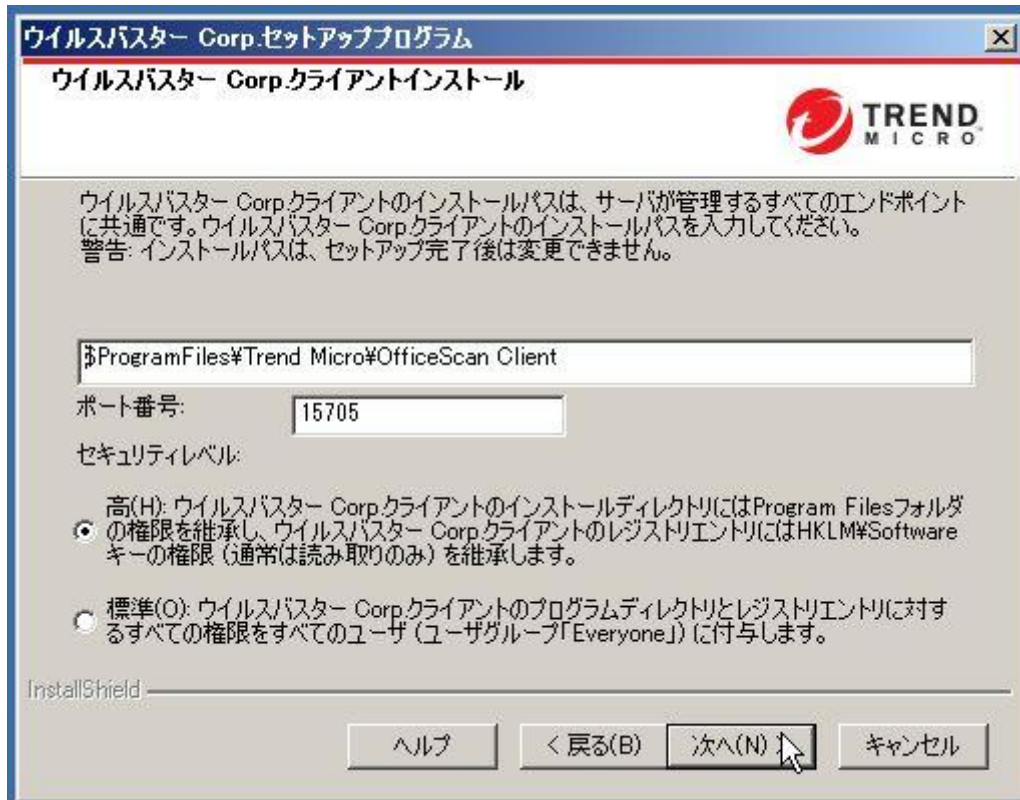
パスワードの確認入力: \*\*\*\*\*

InstallShield

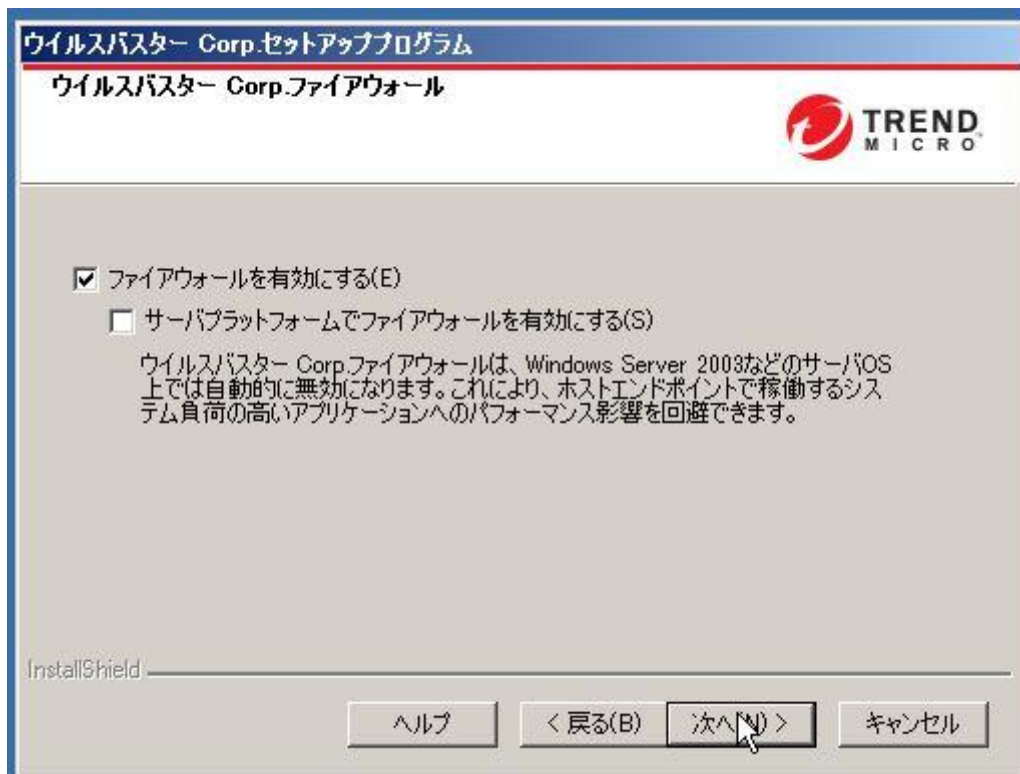
ヘルプ < 戻る(B) 次へ(N) > キャンセル



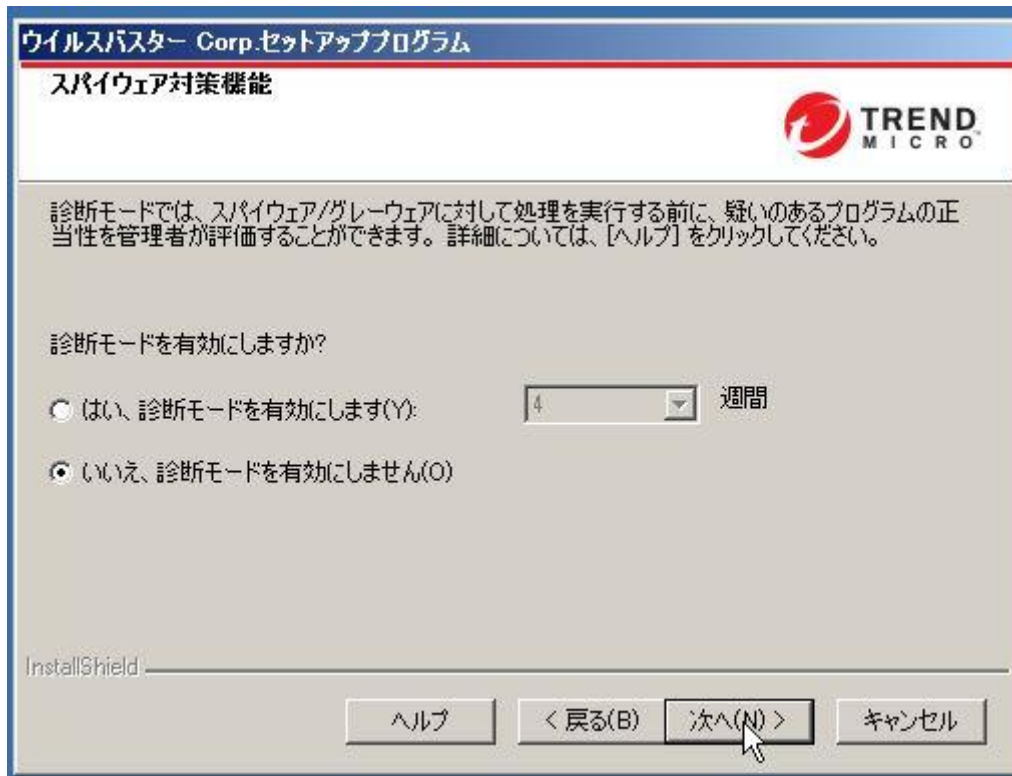
3.1.16. ウイルスバスターCorp.クライアントのインストールパス、接続ポートを設定し、「次へ」を選択します。



3.1.17. ファイアウォールを有効にするかを選択し、「次へ」を選択します。



### 3.1.18. スパイウェアの診断モードを有効にするかを選択し、「次へ」を選択します。



ウイルスバスター Corp. セットアッププログラム

スパイウェア対策機能

診断モードでは、スパイウェア/グレーウェアに対して処理を実行する前に、疑いのあるプログラムの正当性を管理者が評価することができます。詳細については、[ヘルプ] をクリックしてください。

診断モードを有効にしますか?

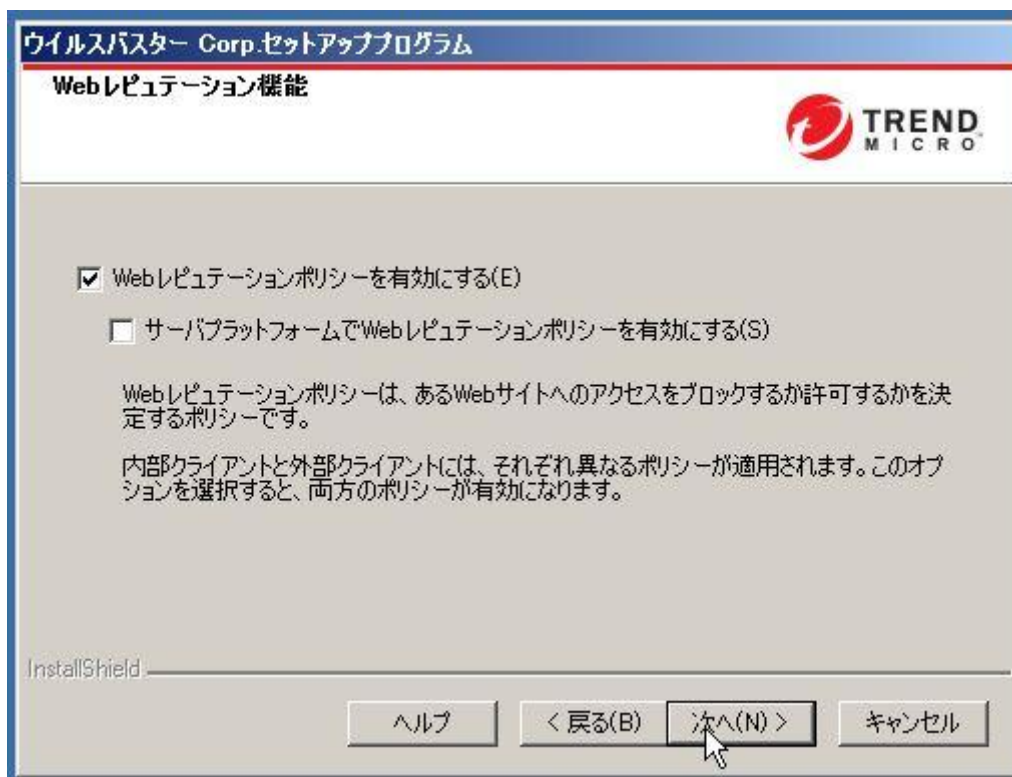
☐ はい、診断モードを有効にします(Y): 4 週間

☒ いいえ、診断モードを有効にしません(O)

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

### 3.1.19. Web レピュテーションを有効にするかを選択し、「次へ」を選択します。



ウイルスバスター Corp. セットアッププログラム

Webレピュテーション機能

☒ Webレピュテーションポリシーを有効にする(E)

☐ サーバプラットフォームでWebレピュテーションポリシーを有効にする(S)

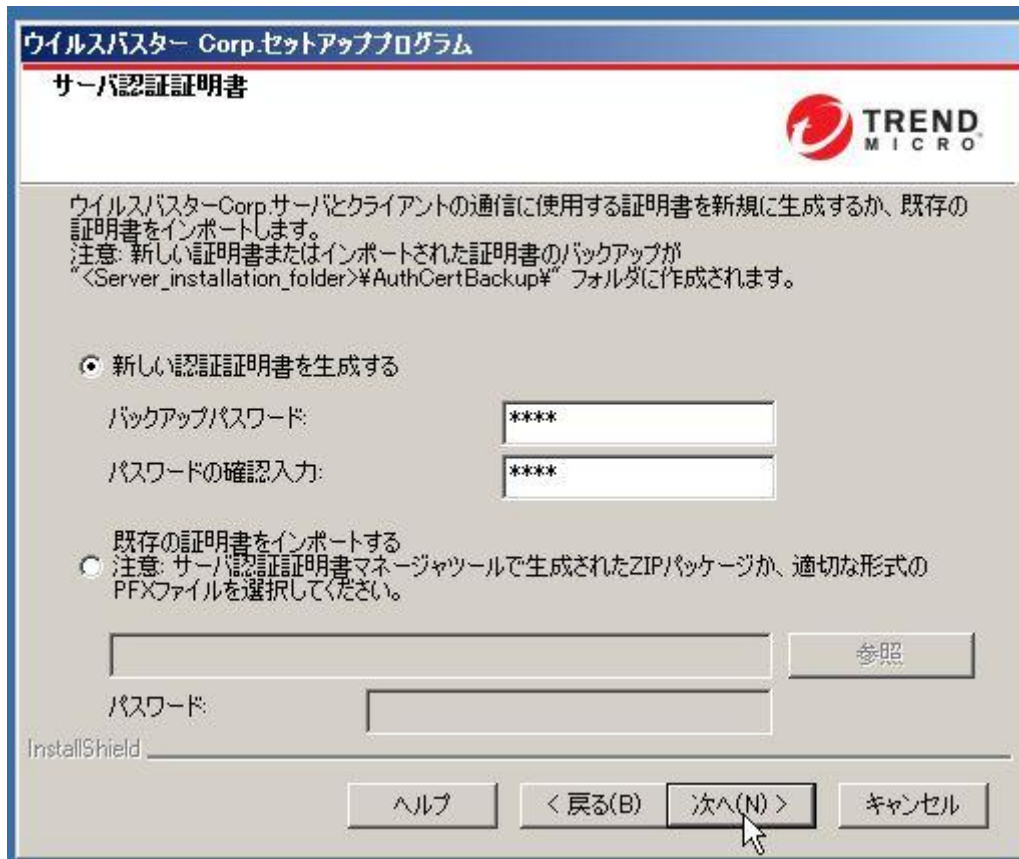
Webレピュテーションポリシーは、あるWebサイトへのアクセスをブロックするか許可するかを決定するポリシーです。

内部クライアントと外部クライアントには、それぞれ異なるポリシーが適用されます。このオプションを選択すると、両方のポリシーが有効になります。

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

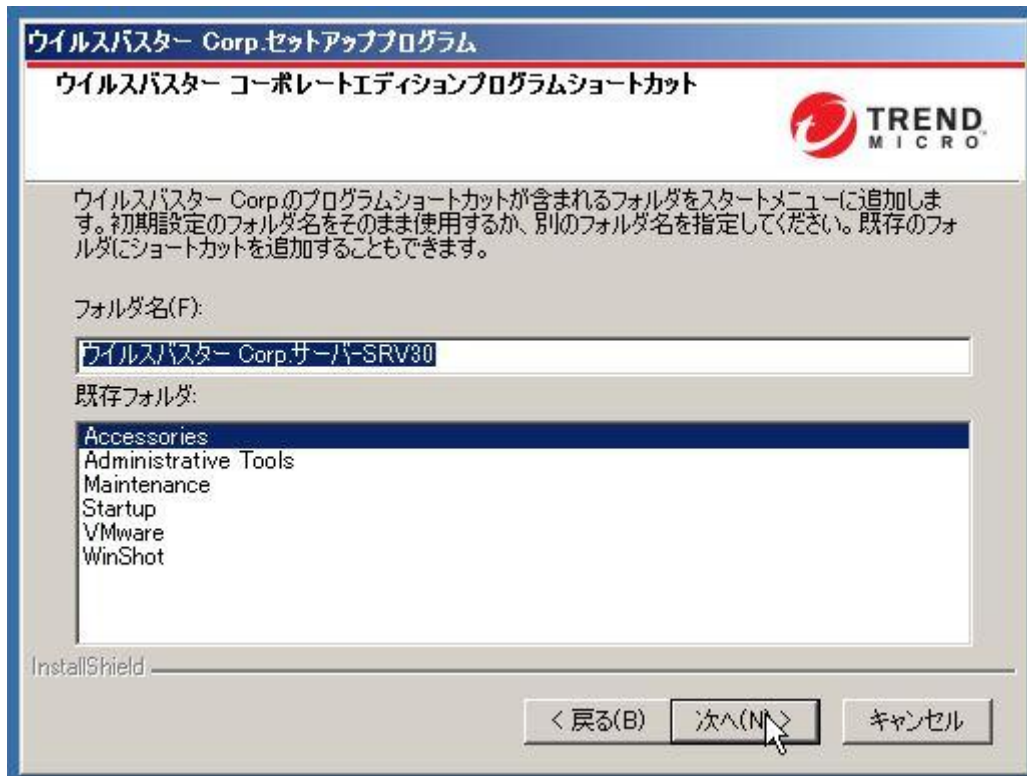
### 3.1.20. サーバ証明書を設定し、「次へ」を選択します。



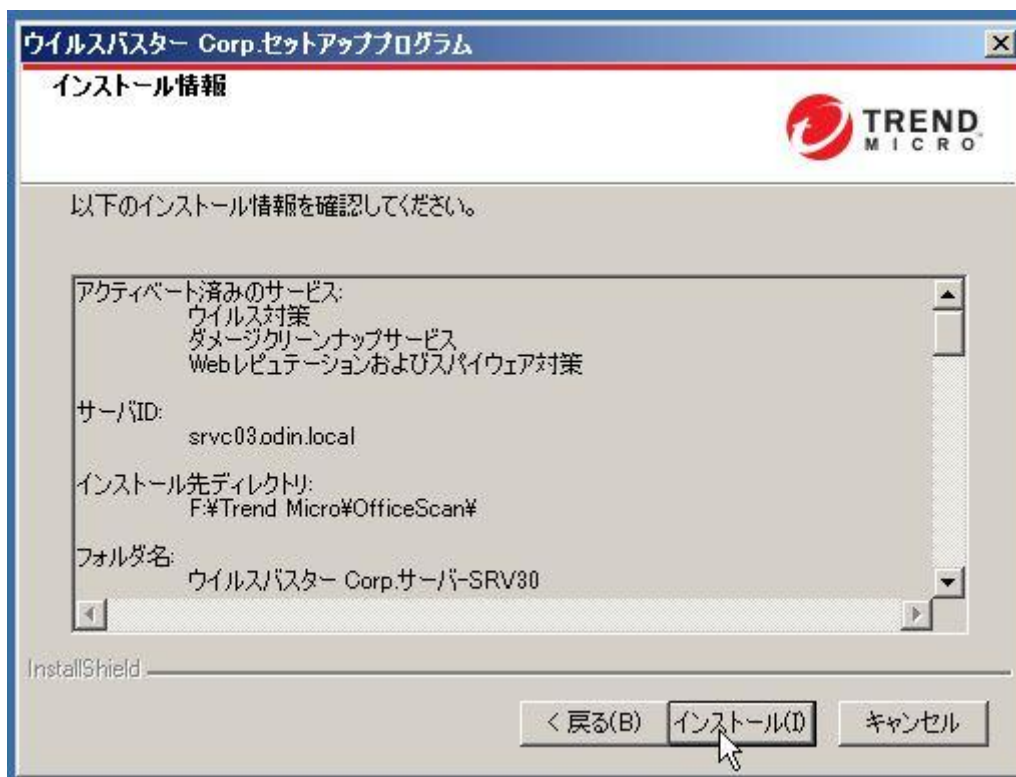
NodeA と NodeB は同じサーバ証明書を使用する必要があります。

NodeA で作成したサーバ証明書は NodeB へのウイルスバスターCorp.11.0 のインストール時にも指定する必要があります。

### 3.1.21. ショートカット名を設定し、「次へ」を選択します。



### 3.1.22. インストール情報を確認し、「インストール」を選択します。



### 3.1.23. インストールが終了することを確認します。



### 3.2. Node A でウイルスバスターCorp.のサービスを停止

Node A でウイルスバスターCorp.のインストールが終了した後、以下のサービスを停止します。

- OfficeScan Master Service
- OfficeScan Active Directory Intergration Service
- OfficeScan Log Receiver Service
- OfficeScan Plug-in Manager
- Trend Micro Local Web Classification Service
- Trend Micro Smart Scan Server

### 3.3. 共有ディスクの所有者ノードの変更と PCCSRV フォルダの削除

共有ディスクの所有者を Node A から Node B へ変更します。

※共有ディスクの所有者を変更する方法はマイクロソフト社のドキュメントなどをご参照下さい。

ここでは Node A を一時停止し、Node B に役割を移動します。

#### 3.3.1. Cluster Manager で Node A が停止したことを確認します。

ノード	
名前	状態
srv30	停止
srv31	稼働中

#### 3.3.2. 現在のホストサーバが Node B となっていることを確認します。

osce\_failover

 **osce\_failover の概要**

状態: オンライン

警告: <なし>

優先する所有者: <なし>

現在の所有者: srv31



### 3.3.3. Node B で共有ディスク内の PCCSRV フォルダを削除します。

共有ディスクを選択し、PCCSRV フォルダを削除します。

本手順を実施することで、Node B への Plug-in Manager Service のインストールに失敗する問題を回避することができます。

尚、本手順を実施せずに作業を進め、Plug-in Manager Service のインストールに失敗した場合、NodeA、NodeB ともに再インストールが必要になりますのでご注意ください。



AuthCertBackup フォルダは NodeA インストール時に作成したサーバ証明書のバックアップが保存されているので、そのまま残しておきます。

### 3.4. Node B でウイルスバスターCorp.11.0 のインストーラを開始

#### 3.4.1. インストーラを起動し、「開始」を選択します。

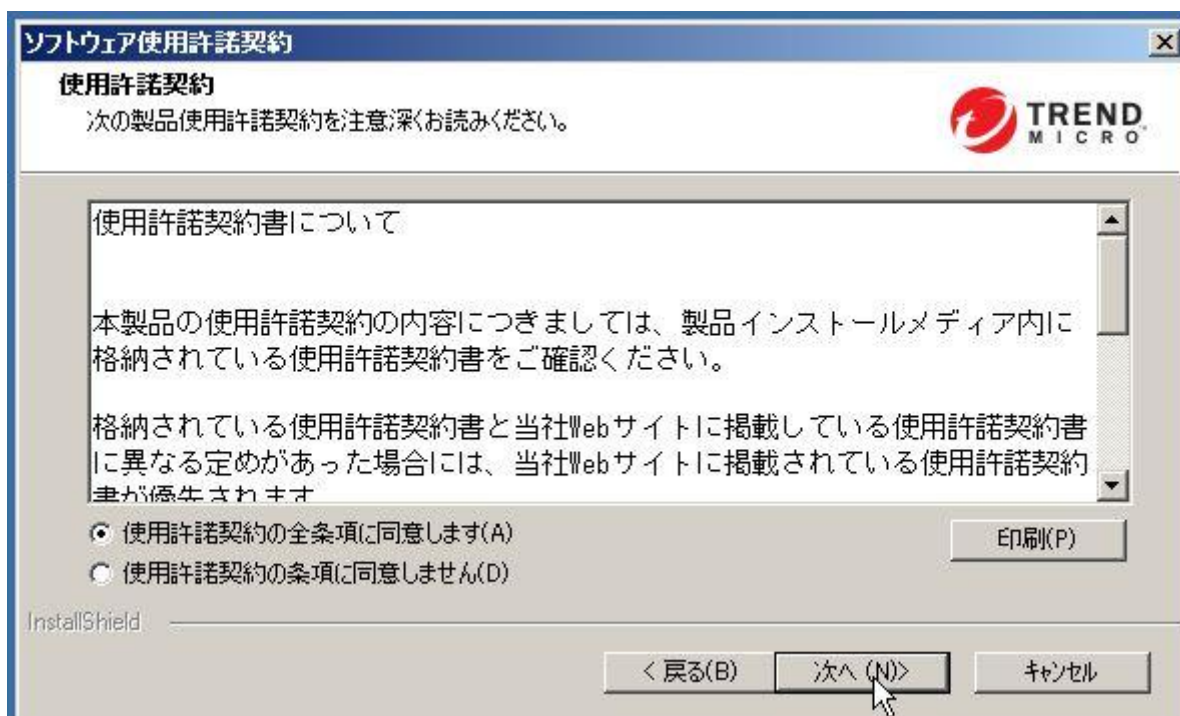




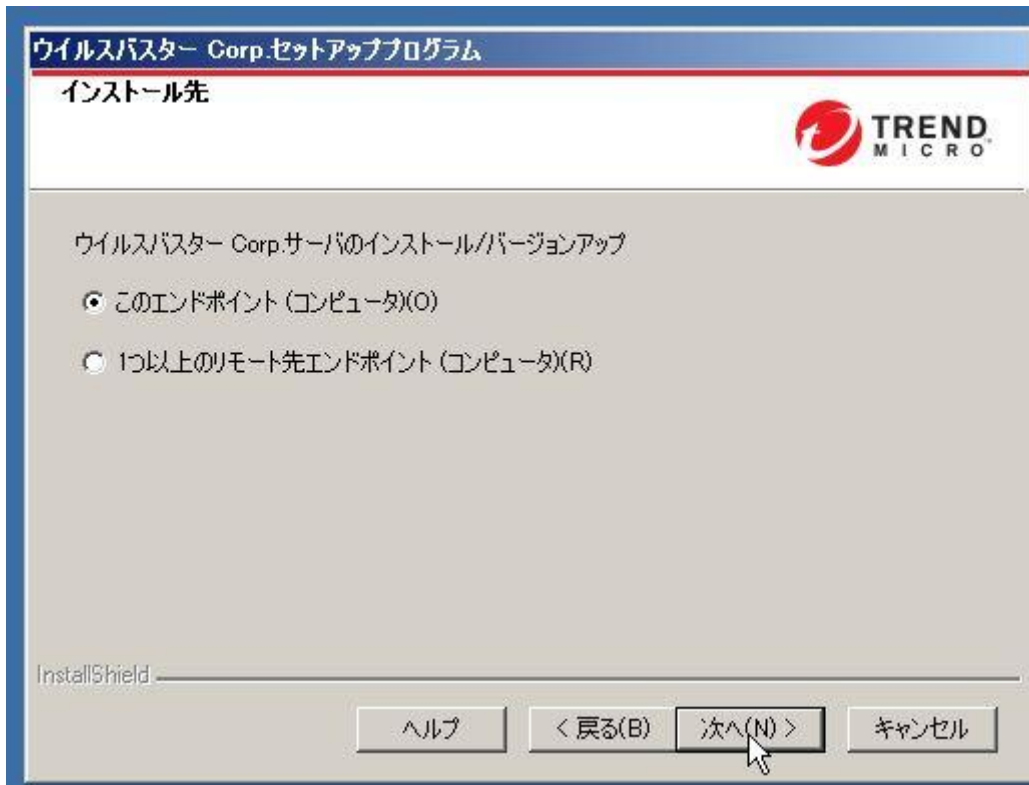
### 3.4.2. 「次へ」を選択します。



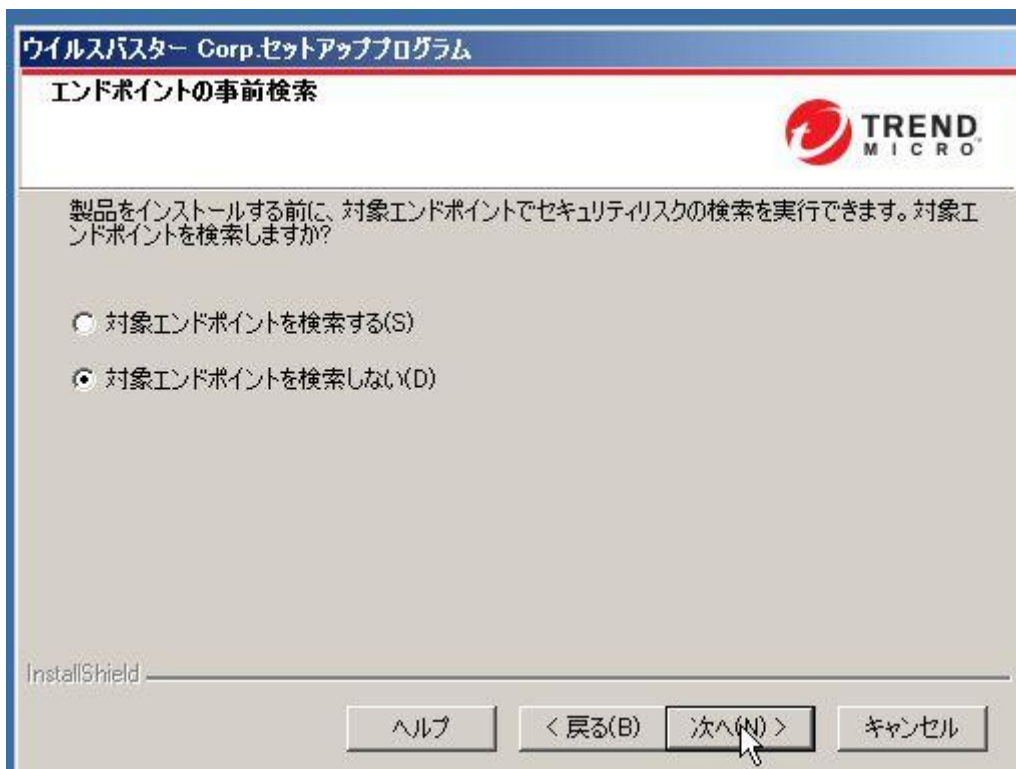
### 3.4.3. 使用許諾を読み、「同意します」にチェックを入れ「次へ」を選択します。



3.4.4. インストール先を選択し、「次へ」を選択します。

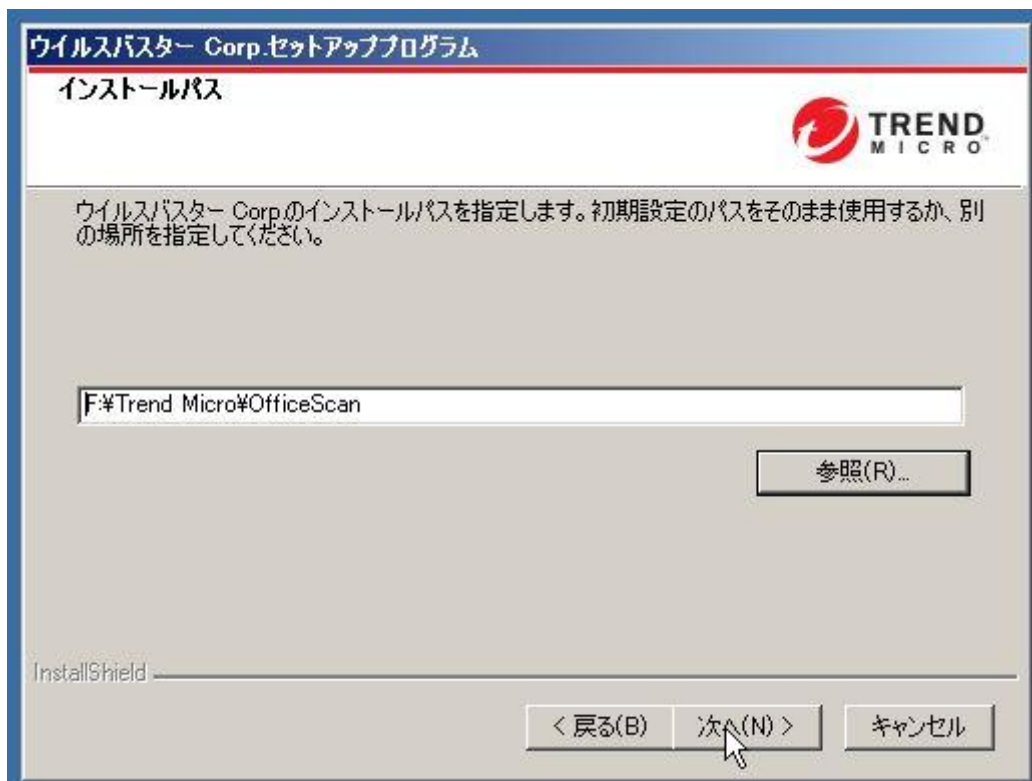


3.4.5. インストール先を事前に検索するか選択し、「次へ」を選択します。



### 3.4.6. 製品のインストールパスを指定します。

ここではインストール先として、Cluster の共有ディスクを指定するため、「参照」を選択します。

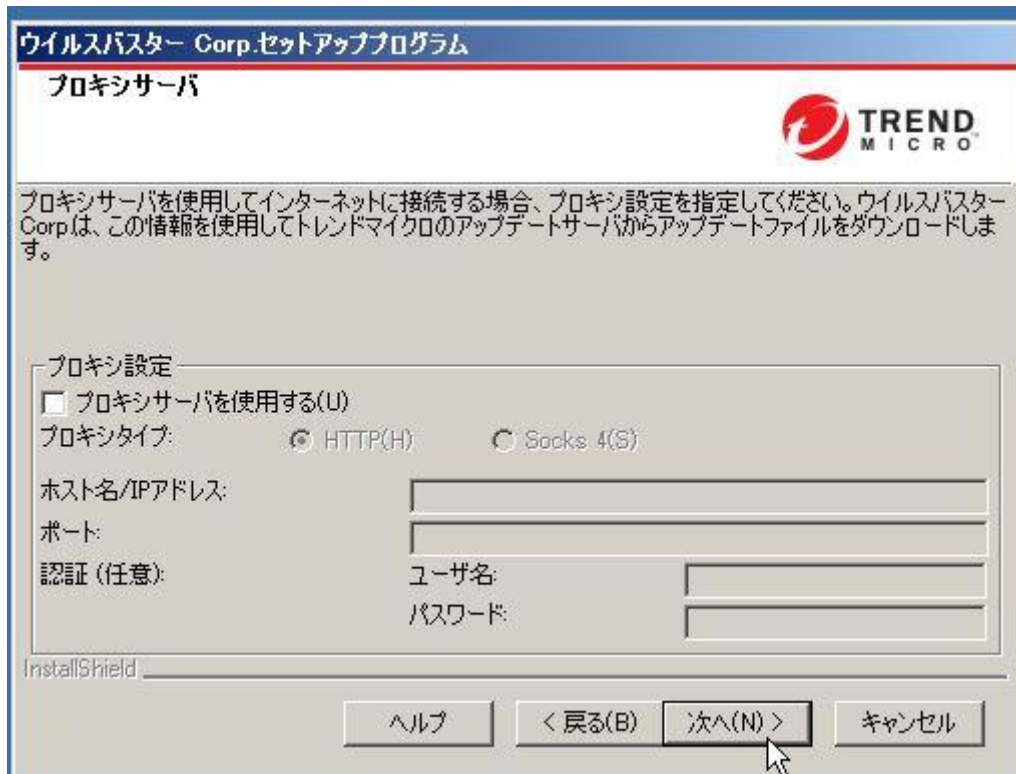


Cluster の共有ディスクを指定します。

Cluster の共有ディスクが指定された事を確認し、「次へ」を選択します。

Cluster の共有ディスクが見えない場合、共有ディスクの所有者が Node B に移っていることを確認してください。

3.4.7. プロキシサーバの利用の有無を選択し、「次へ」を選択します。



ウイルスバスター Corp.セットアッププログラム

プロキシサーバ

プロキシサーバを使用してインターネットに接続する場合、プロキシ設定を指定してください。ウイルスバスター Corp.は、この情報を使用してトレンドマイクロのアップデートサーバからアップデートファイルをダウンロードします。

プロキシ設定

☐ プロキシサーバを使用する(U)

プロキシタイプ: ☒ HTTP(H) ☐ Socks 4(S)

ホスト名/IPアドレス:

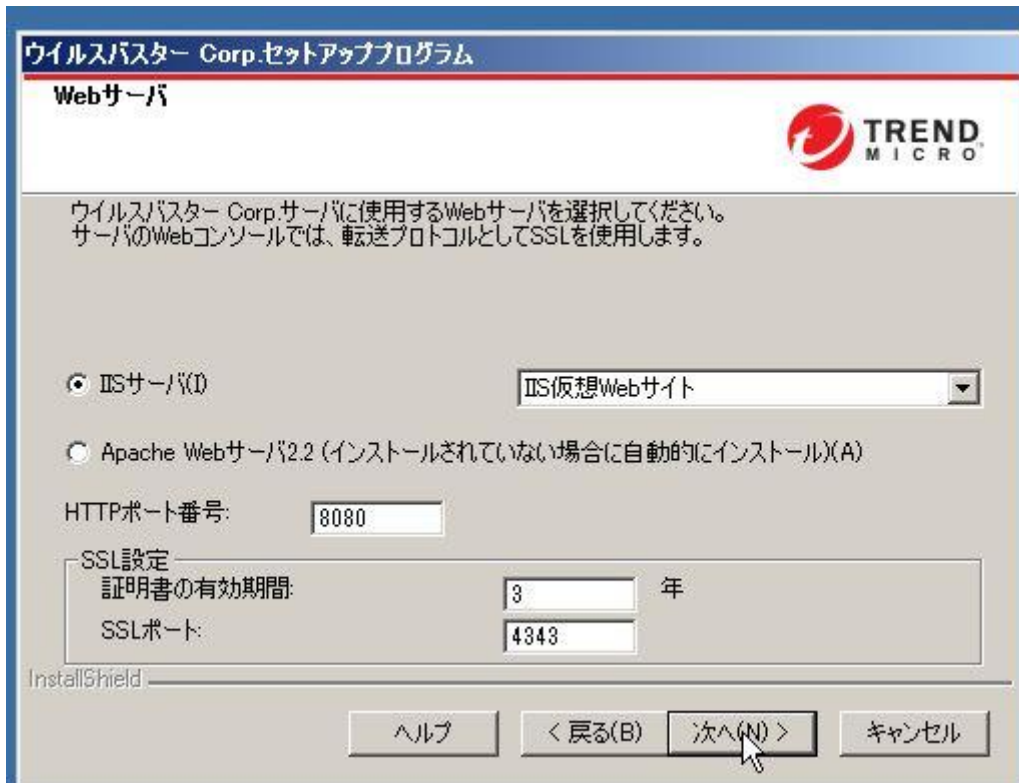
ポート:

認証 (任意): ユーザ名:   
パスワード:

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

3.4.8. Web サーバとして IIS が選択されている事を確認し、「次へ」を選択します。



**ウイルスバスター Corp. セットアッププログラム**

**Webサーバ**

ウイルスバスター Corp. サーバに使用するWebサーバを選択してください。  
サーバのWebコンソールでは、転送プロトコルとしてSSLを使用します。

☒ IISサーバ(I) IIS仮想Webサイト

☐ Apache Webサーバ2.2 (インストールされていない場合に自動的にインストール)(A)

HTTPポート番号:

SSL設定

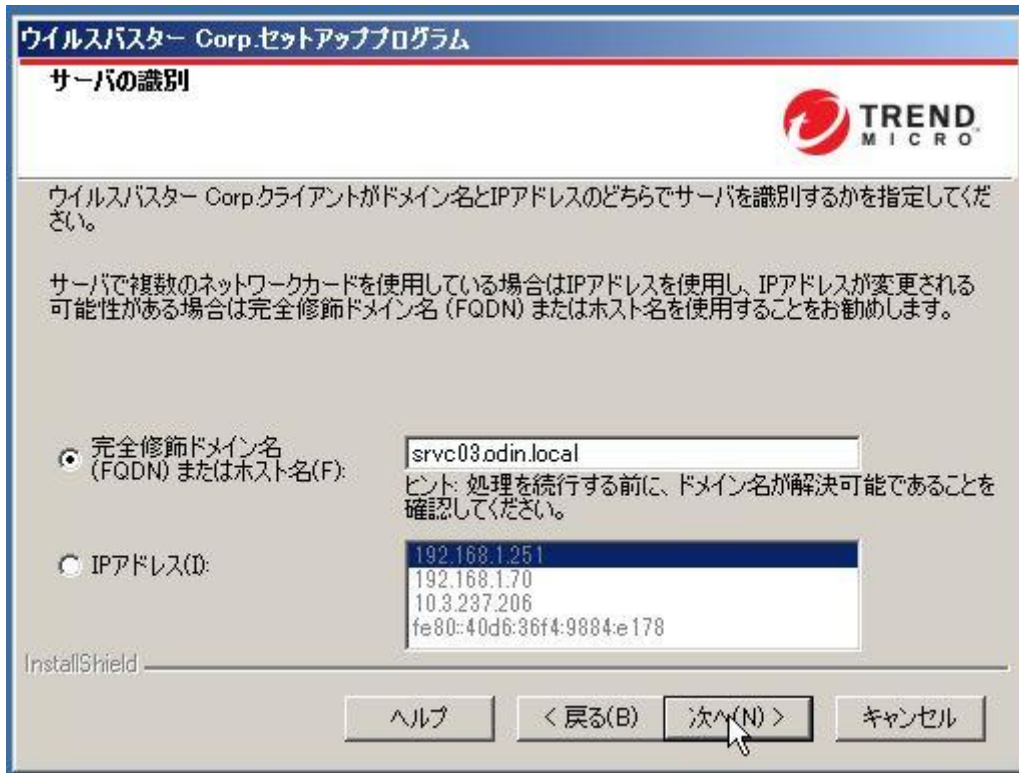
証明書の有効期間:  年

SSLポート:

InstallShield

ヘルプ < 戻る(B) **次へ(N) >** キャンセル

3.4.9. サーバの識別名として、Cluster の FQDN または IP アドレスを指定し、「次へ」を選択します。



**ウイルスバスター Corp. セットアッププログラム**

**サーバの識別**

ウイルスバスター Corp. クライアントがドメイン名とIPアドレスのどちらでサーバを識別するかを指定してください。

サーバで複数のネットワークカードを使用している場合はIPアドレスを使用し、IPアドレスが変更される可能性がある場合は完全修飾ドメイン名 (FQDN) またはホスト名を使用することをお勧めします。

☒ 完全修飾ドメイン名 (FQDN) またはホスト名(F):

ヒント: 処理を続行する前に、ドメイン名が解決可能であることを確認してください。

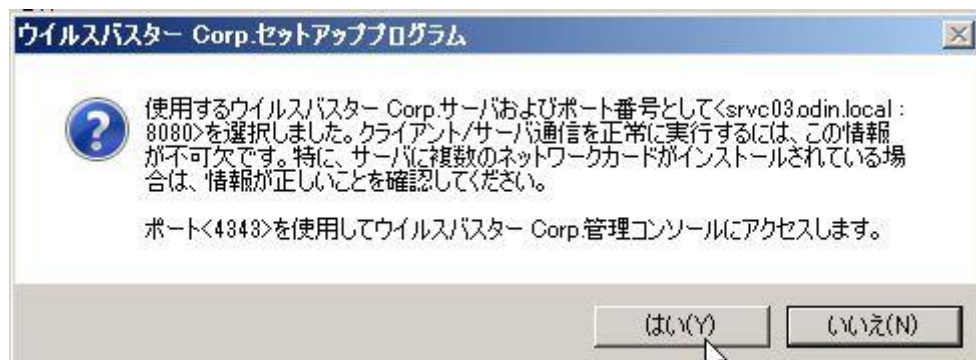
☐ IPアドレス(I):

192.168.1.70  
10.3.237.206  
fe80::40d6:36f4:9884:e178

InstallShield

ヘルプ < 戻る(B) **次へ(N) >** キャンセル

Cluster の FQDN、IP アドレスを選択すると以下の警告が表示されますが、「はい」を選択し、インストールを進めます。



#### 3.4.10. 製品のアクティベーションコードを入力します。「次へ」を選択します。




事前に準備済みのアクティベーションコードを入力し、「次へ」を選択します。



**ウイルスバスター Corp.セットアッププログラム**

**製品のアクティベーション**  
 ステップ2. アクティベーションコードの入力



次の形式を使用して、ウイルスバスター Corp.サービスのアクティベーションコードを入力します。(コード形式: XX-XXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX)

ウイルス対策:

☐ ダメージクリーンナップサービス、Webレпутーション、およびスパイウェア対策に同じアクティベーションコードを使用します

ダメージクリーンナップサービス:

Webレпутーションおよびスパイウェア対策:

InstallShield \_\_\_\_\_

ヘルプ

< 戻る(B)


次へ(N) >

キャンセル

3.4.11. クライアントの方式を選択し、「次へ」を選択します。

**ウイルスバスター Corp.セットアッププログラム**

**ウイルスバスター Corp.クライアント配信**



この画面の情報をを使用して、ウイルスバスター Corp.クライアントの配信を計画してください。

ウイルスバスター Corp.クライアントパッケージのサイズは、使用する配信方法、および配信時のサーバ上のコンポーネントのサイズによって異なります。

次のパッケージサイズは本製品出荷時のコンポーネントのサイズを示しています。このパッケージサイズは、ウイルスバスター Corp.サーバがコンポーネントをアップデートするたびに変わります。

**従来型スキャン方式**

Webインストール: 83MB  
 リモートインストール: 144MB  
 ログオンスクリプト (AutoPcc.exe): 181MB

**スマートスキャン方式**

Webインストール: 72MB  
 リモートインストール: 144MB  
 ログオンスクリプト (AutoPcc.exe): 171MB

InstallShield \_\_\_\_\_

ヘルプ

< 戻る(B)

次へ(N) >

キャンセル

3.4.12. 統合 Smart Protection Server のインストールの有無を選択し、「次へ」を選択します。



3.4.13. 対象のエンドポイントにウイルスバスター Corp. クライアントをインストールするかを選択し、「次へ」を選択します。





#### 3.4.14. スマートフィードバックを有効にするかを選択し、「次へ」を選択します。

**ウイルスバスター Corp.セットアッププログラム**

**Smart Protection Network**



Trend Micro Smart Protection Networkは、最新の脅威に対してプロアクティブな保護を提供するように設計された、次世代のクラウドクライアント型のコンテンツセキュリティ基盤です。

☒ Trend Micro スマートフィードバックを有効にする (推奨)

本機能を有効にすると、コンピュータで検出された脅威情報 (アクセスされたWebアドレス、ファイルに関する情報等) がトレンドマイクロに送信され、新たな脅威の迅速な識別や対処に役立てられます。本機能は製品コンソールを介しても無効にできます。スマートフィードバックは製品コンソールからいつでも無効にできます。

業種 (オプション):


InstallShield

ヘルプ < 戻る(B) **次へ(N) >** キャンセル

#### 3.4.15. 管理者用のアカウントを設定し、「次へ」を選択します。

**ウイルスバスター Corp.セットアッププログラム**

**管理者アカウントのパスワード**



Webコンソールを開くためのパスワードとウイルスバスター Corp.クライアントをアンロード/アンインストールするためのパスワードを指定してください。パスワードを設定することで、権限のないユーザによるWebコンソール設定の変更やウイルスバスター Corp.クライアントの削除を防ぐことができます。

Webコンソールパスワード:

アカウント:

パスワード:

パスワードの確認入力:

ウイルスバスター Corp.クライアントのアンロード/アンインストールパスワード:

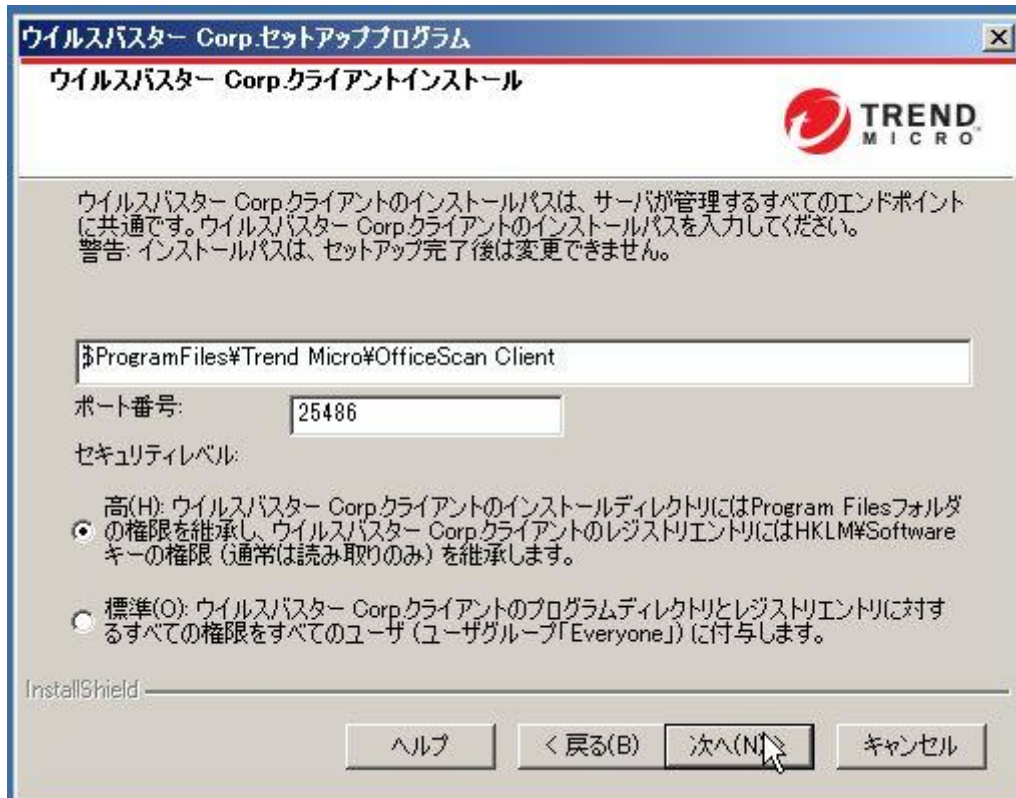
パスワード:

パスワードの確認入力:

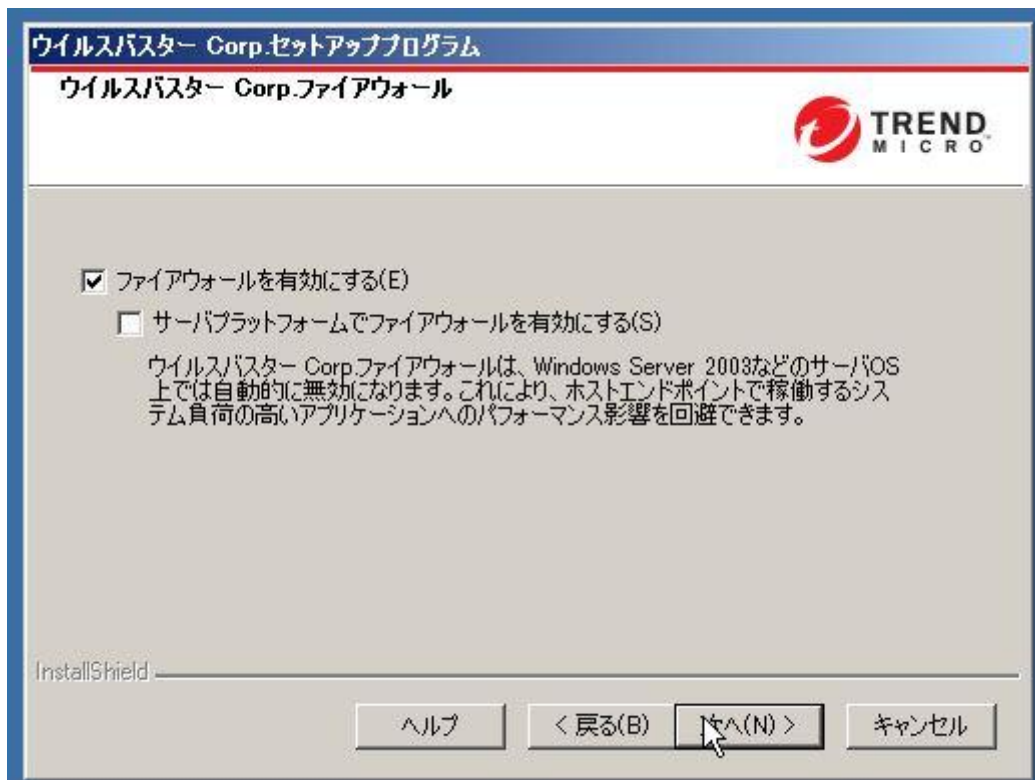
InstallShield

ヘルプ < 戻る(B) **次へ(N) >** キャンセル

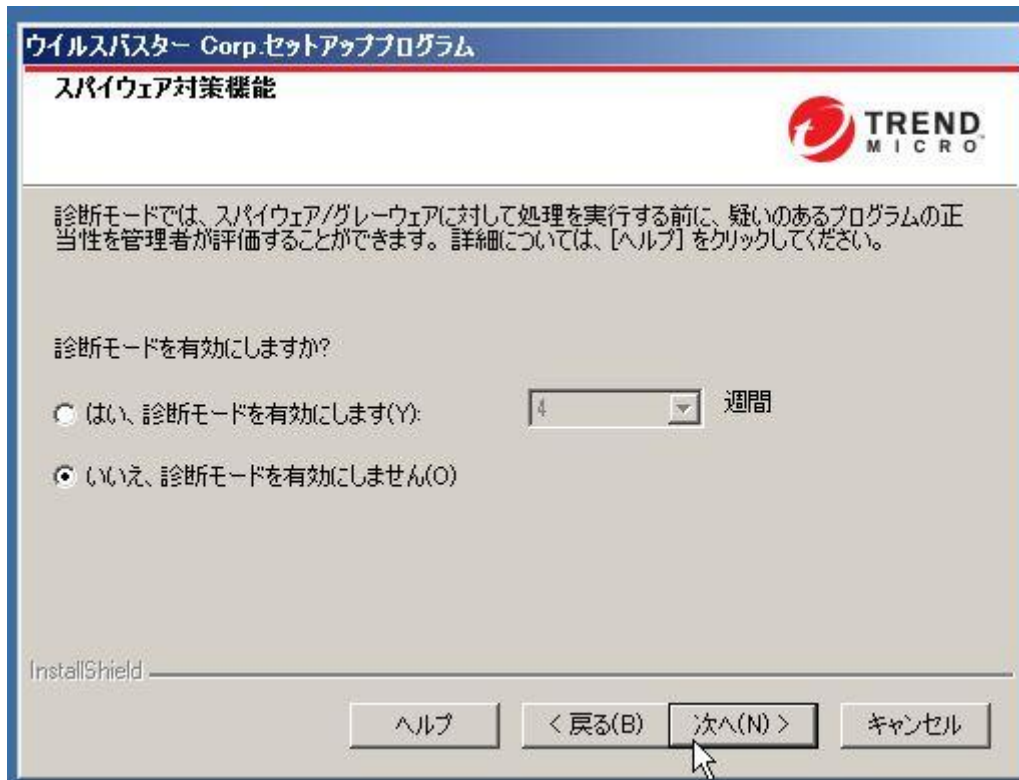
3.4.16. ウイルスバスターCorp.クライアントのインストールパス、接続ポートを設定し、「次へ」を選択します。



3.4.17. ファイアウォールを有効にするかを選択し、「次へ」を選択します。



### 3.4.18. スパイウェアの診断モードを有効にするかを選択し、「次へ」を選択します。



ウイルスバスター Corp.セットアッププログラム

スパイウェア対策機能

診断モードでは、スパイウェア/グレーウェアに対して処理を実行する前に、疑いのあるプログラムの正当性を管理者が評価することができます。詳細については、[ヘルプ]をクリックしてください。

診断モードを有効にしますか?

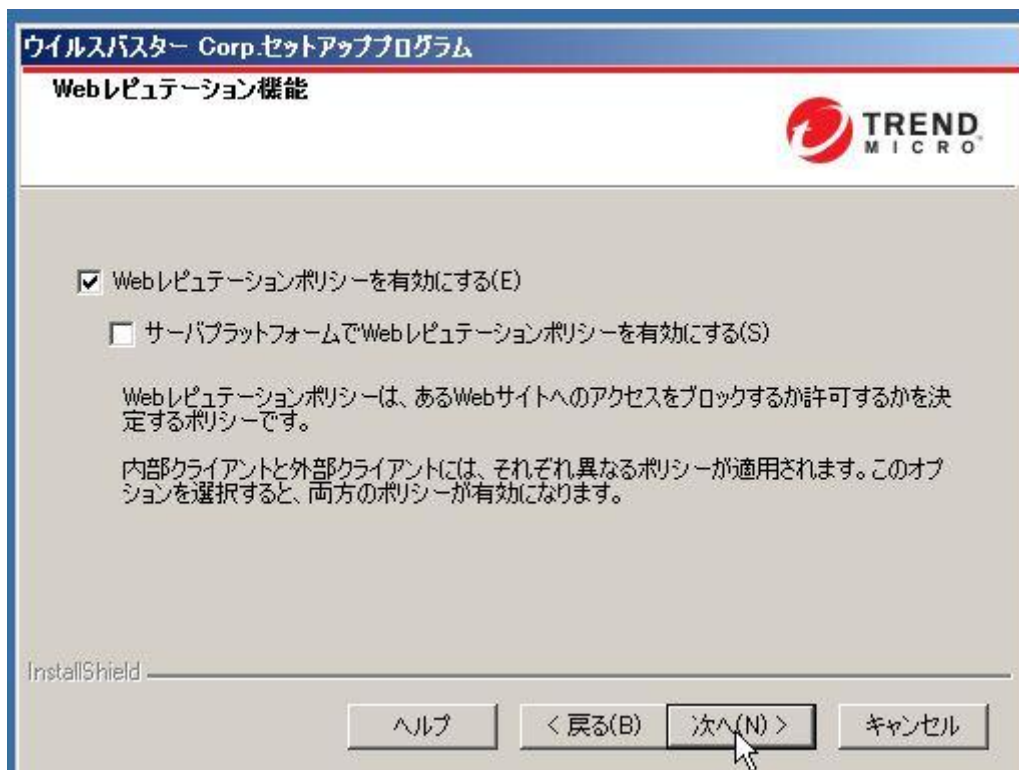
☐ はい、診断モードを有効にします(Y): 4 週間

☒ いいえ、診断モードを有効にしません(O)

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

### 3.4.19. Web レピュテーションを有効にするかを選択し、「次へ」を選択します。



ウイルスバスター Corp.セットアッププログラム

Webレピュテーション機能

☒ Webレピュテーションポリシーを有効にする(E)

☐ サーバプラットフォームでWebレピュテーションポリシーを有効にする(S)

Webレピュテーションポリシーは、あるWebサイトへのアクセスをブロックするか許可するかを決定するポリシーです。

内部クライアントと外部クライアントには、それぞれ異なるポリシーが適用されます。このオプションを選択すると、両方のポリシーが有効になります。

InstallShield

ヘルプ < 戻る(B) 次へ(N) > キャンセル

### 3.4.20. サーバ証明書を設定し、「次へ」を選択します。

NodeB では「既存の証明書をインポートする」にチェックが入っていることを確認します。



**ウイルスバスター Corp.セットアッププログラム**

**サーバ認証証明書**

対象エンドポイントの次の場所に既存のウイルスバスター Corp 認証証明書が見つかりました:  
<Server installation folder>%AuthCertBackup%. ウイルスバスター Corp クライアントがこの証明書  
を現在使用している場合は、インストール時にこの証明書をインポートすることをお勧めします。

☐ 新しい認証証明書を生成する

バックアップパスワード:

パスワードの確認入力:

☒ 既存の証明書をインポートする

注意: サーバ認証証明書マネージャツールで生成されたZIPパッケージか、適切な形式の  
PFXファイルを選択してください。

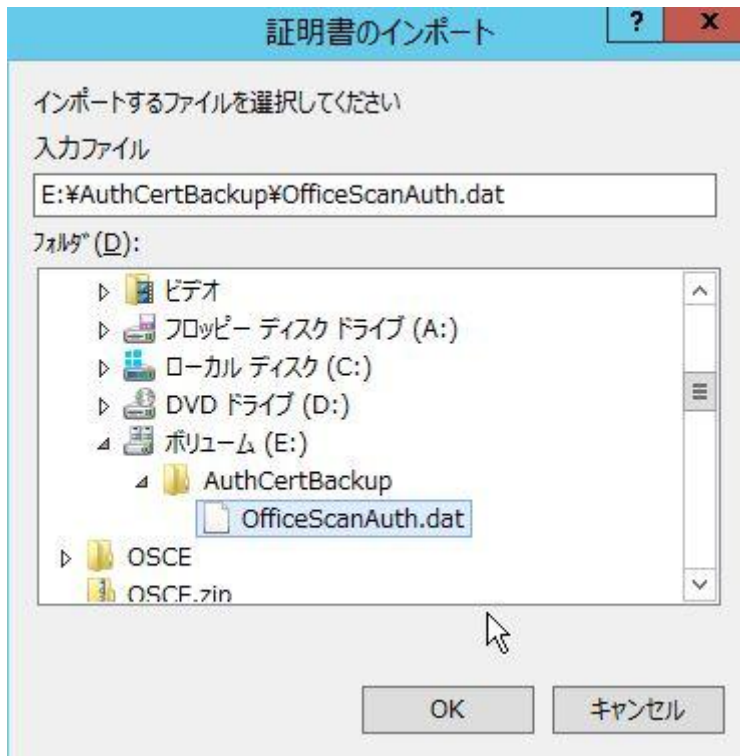
F:\Trend Micro\OfficeScan\AuthCertBackup\OfficeScanAuth.d:

パスワード:

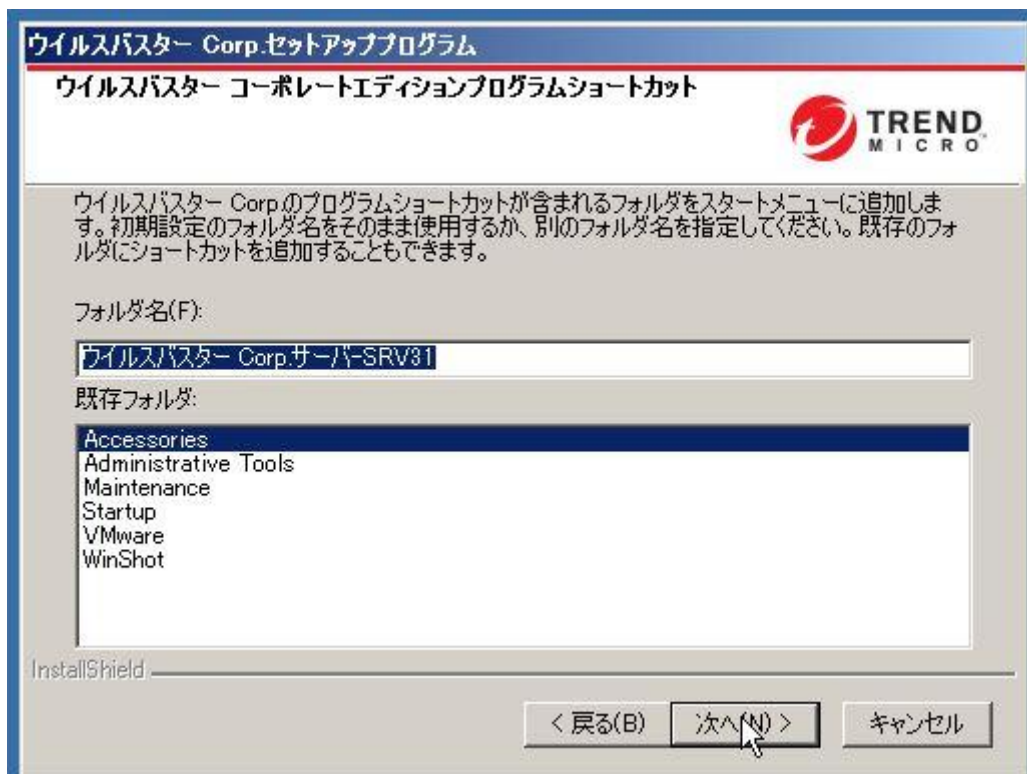
InstallShield



「既存の証明書をインポートする」にチェックが入っておらず、正しく参照されていない場合は「参照」を選択し、共有ディスクにあるサーバ証明書のバックアップファイルを指定します。



3.4.21. ショートカット名を設定し、「次へ」を選択します。



3.4.22. インストール情報を確認し、「インストール」を選択します。



3.4.23. インストールが終了することを確認します。



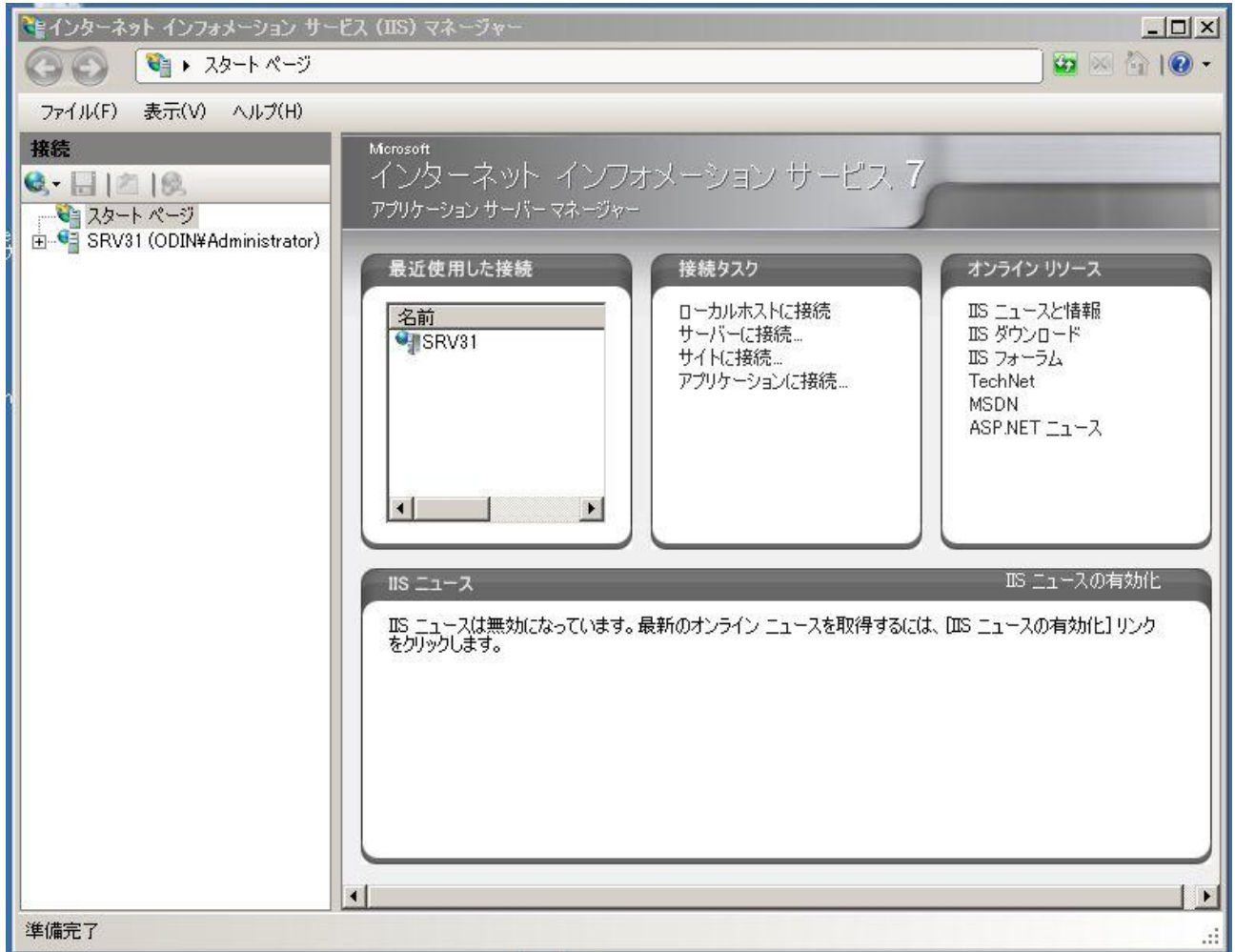
### 3.5. IIS の認証設定

IIS の管理コンソールを起動し、認証設定を変更します。

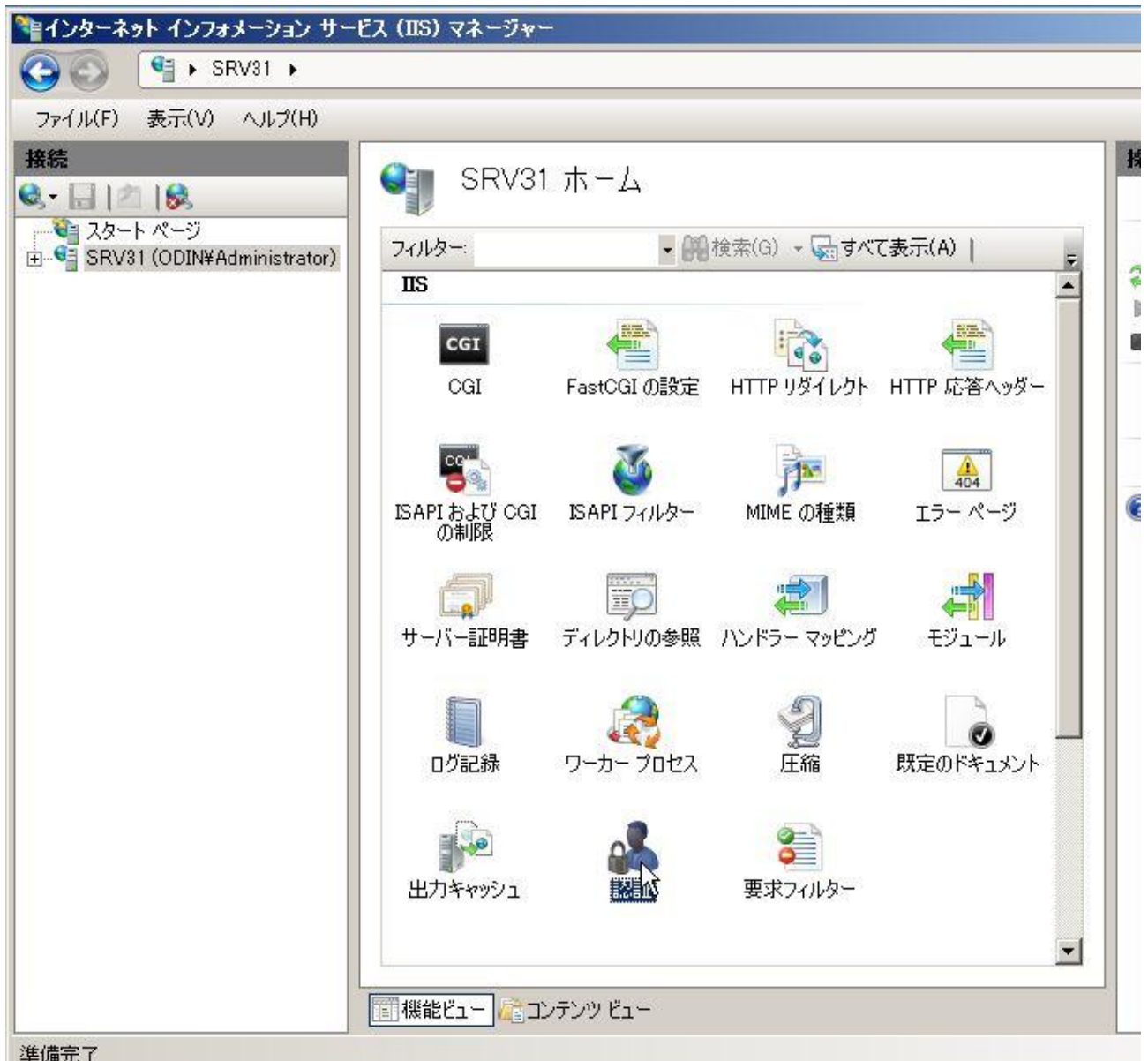
この操作は Node A、Node B でそれぞれ実施します。

#### 3.5.1. サーバマネージャを起動し、IIS マネージャを起動します。

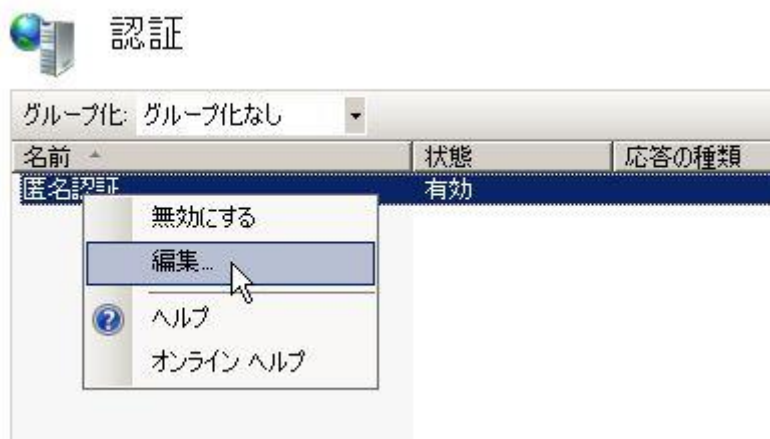
IIS マネージャが起動します。



### 3.5.2. サーバ名を選択し、「認証」をダブルクリックします。



### 3.5.3. 匿名認証を選択し、「編集」を選択します。





3.5.4. 資格情報の編集画面で、特定のユーザ>「設定」を選択します。

3.5.5. 資格情報の設定にドメインのユーザ名、パスワードを設定します。



3.5.6. ドメインユーザ情報が設定されたことを確認し、「OK」を選択します。

### 3.6. ウイルスバスターCorp.のフォルダ権限設定

以下フォルダのアクセス権を確認します。

#### 3.6.1. PCCSRV¥Download（読み取り）



### 3.6.2. PCCSRV¥TEMP（変更、読み取りと実行、フォルダの内容の一覧表示、読み取り、書き込み）



### 3.6.3. PCCSRV¥Web（読み取り）



### 3.6.4. PCCSRV¥Web\_OSCE¥Web\_console¥CGI（読み取りと実行、フォルダ内容の一覧表示、読み取り）



### 3.6.5. PCCSRV¥Web\_OSCE¥Web\_console¥HTML¥ClientInstall (変更、読み取りと実行、フォルダの内容の一覧表示、読み取り、書き込み)





### 3.6.6. PCCSRV¥Web\_OSCE¥Web\_console¥RemoteInstallCGI（変更、読み取りと実行、フォルダの内容の一覧表示、読み取り、書き込み）

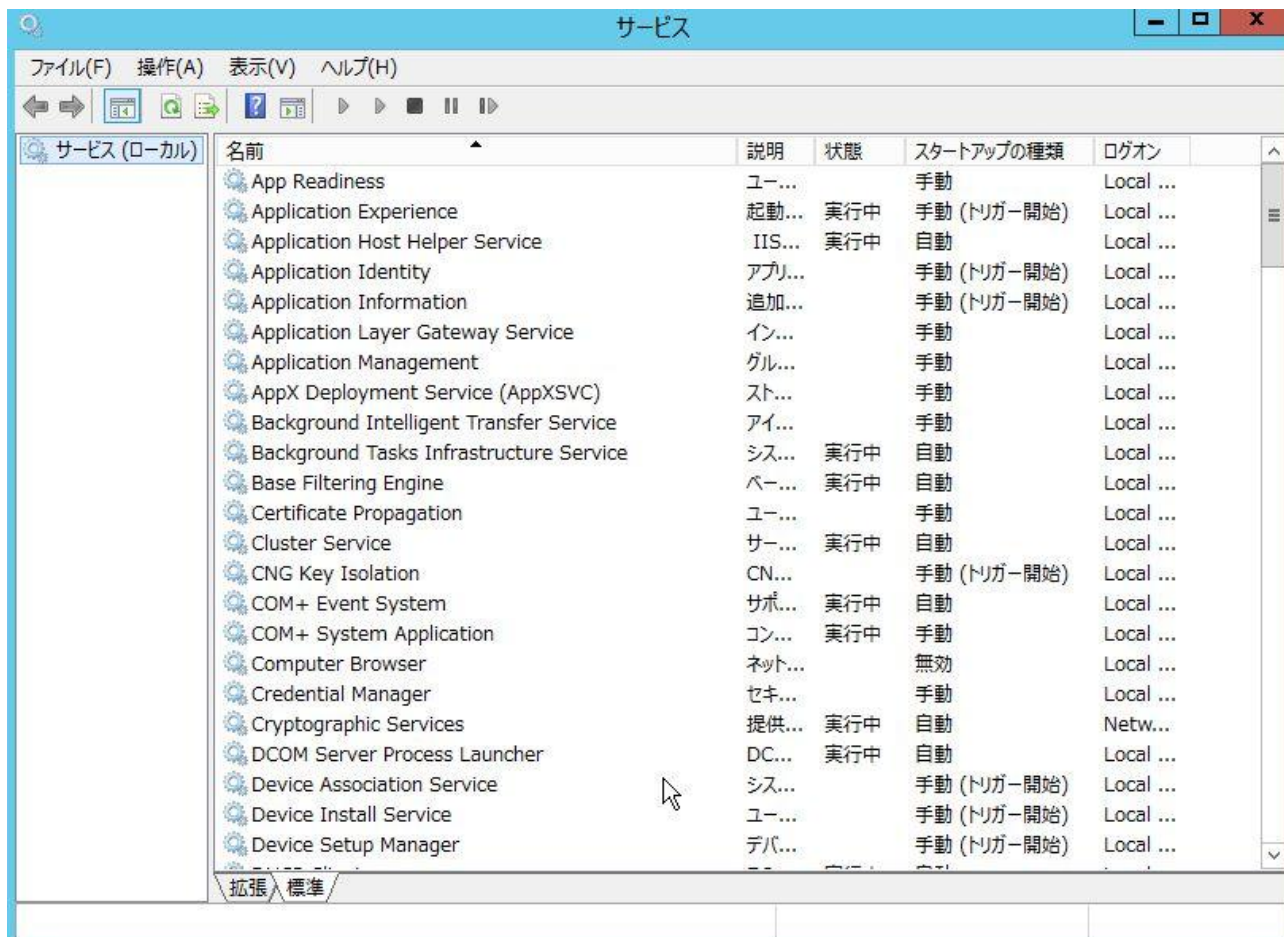


### 3.7. ウイルスバスターCorp. サービススタートアップ設定

ウイルスバスターCorp.のサービスのスタートアップ設定を変更します。

この操作は Node A、Node B でそれぞれ実施します。

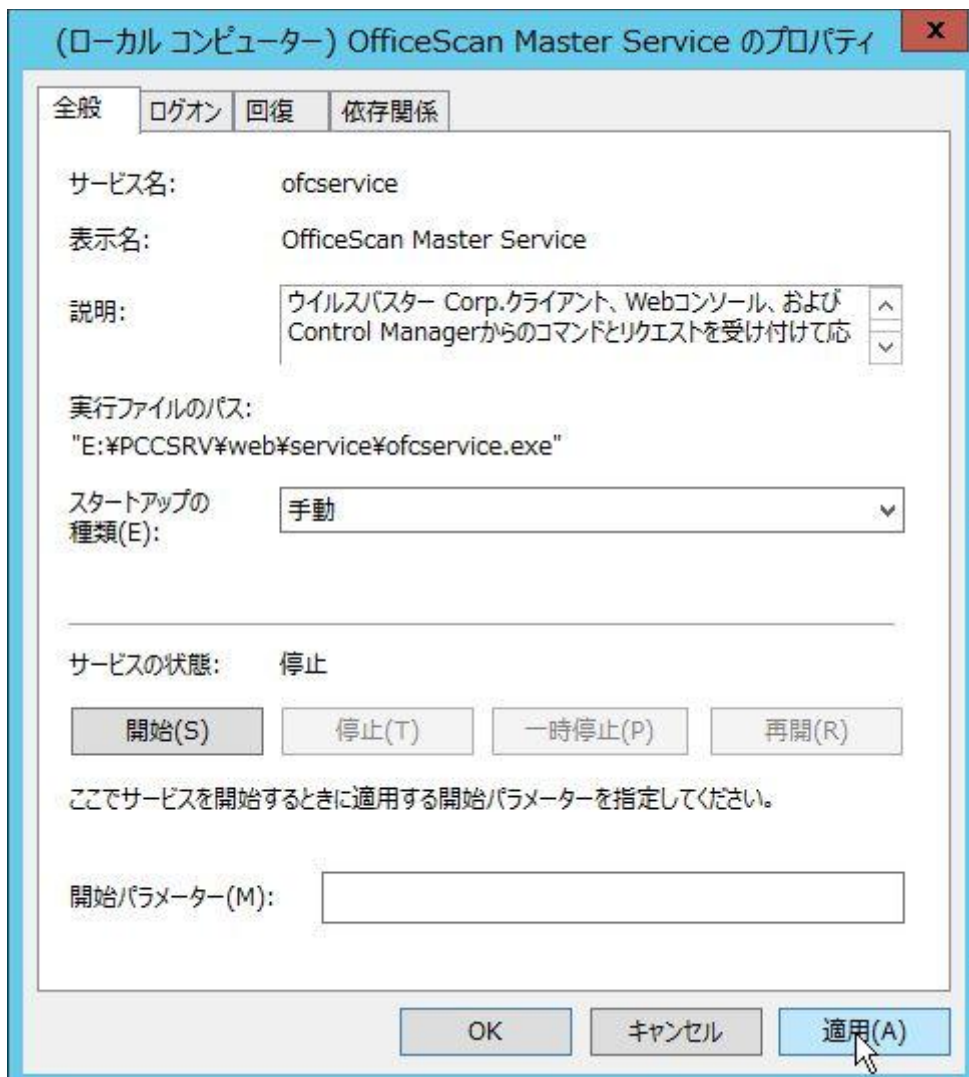
#### 3.7.1. サービスを起動します。



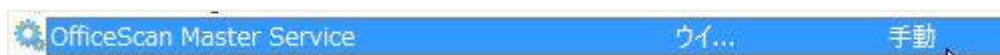
### 3.7.2. OfficeScan Master Service を選択します



スタートアップの種類を手動に変更します。



手動に変更されたことを確認します。



### 3.8. Cluster Generic Script の作成

Cluster で使用するスクリプトファイルを作成します。

本操作は Node A、Node B のそれぞれで実施します。

#### 3.8.1. Generic Script の準備

以下のサンプルスクリプトをコピーし、編集します。



Clusweb7.vbs

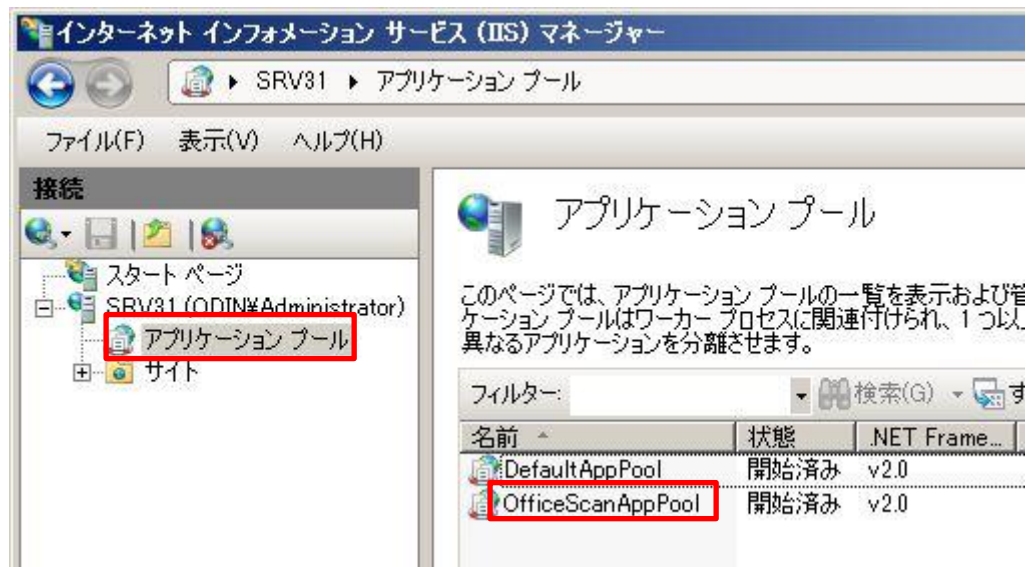
#### 3.8.2. SITE\_NAME、APP\_POOL\_NAME の確認

スクリプトファイルの中の以下記述を確認し、環境と一致していることを確認します。

```
'Note:
'Replace this with the site and application pool
'Make sure that the same web site and applicati
SITE_NAME = "OfficeScan"
APP_POOL_NAME = "OfficeScanAppPool" I
```

#### 3.8.3. 確認方法

IIS マネージャを起動し、サイト名と SITE\_NAME、アプリケーションプール名と APP\_POOL\_NAME が一致していることを確認します。



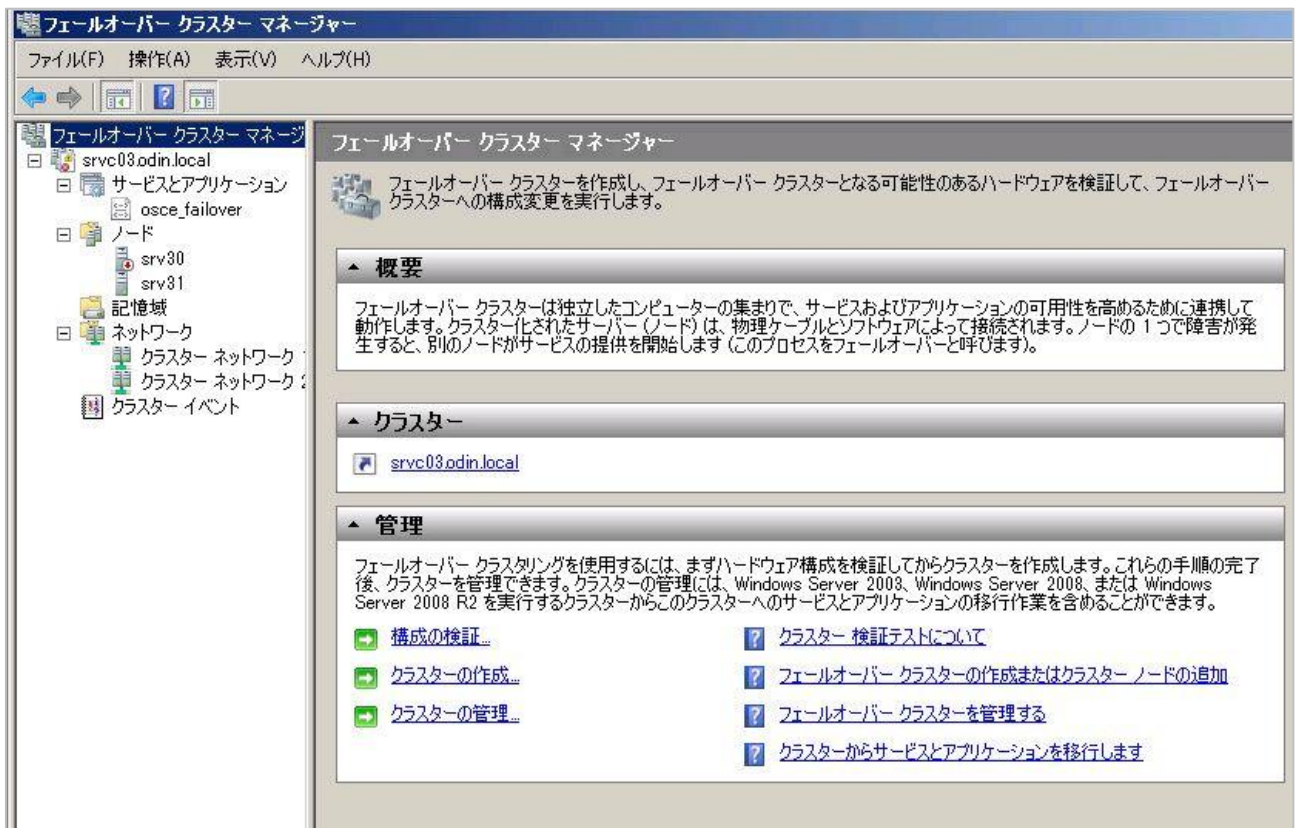
### 3.8.4. Generic Script を System32\inetsrv に保存します。



### 3.9. High availability Cluster Generic Script の作成

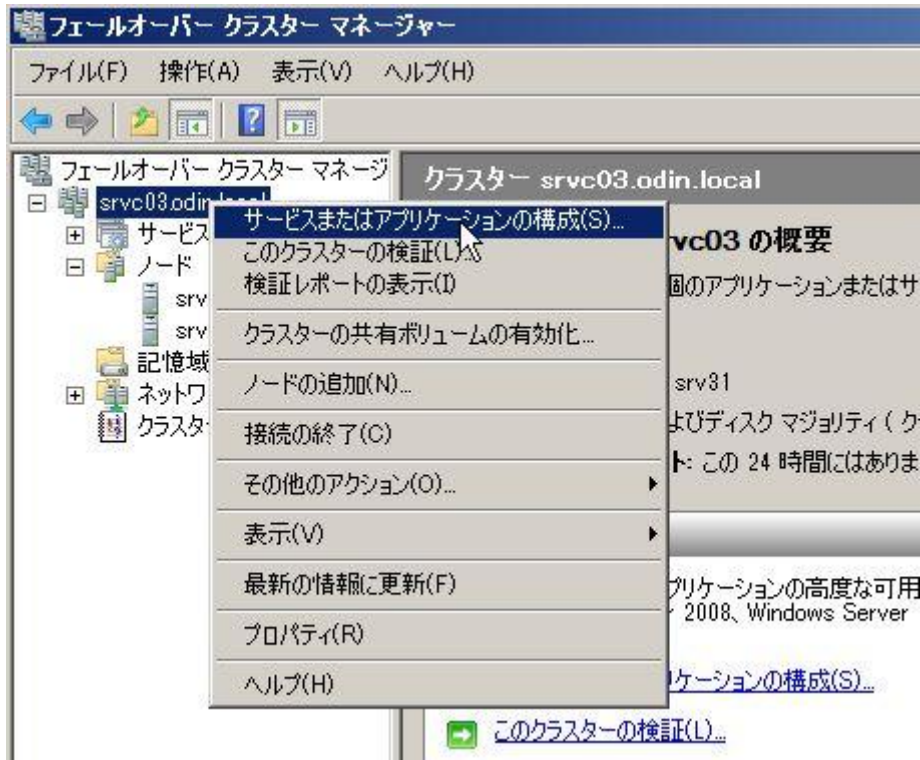
Failover Cluster Manager を起動し、上記で作成したスクリプトを設定します。

#### 3.9.1. Failover Cluster Manager を起動します。





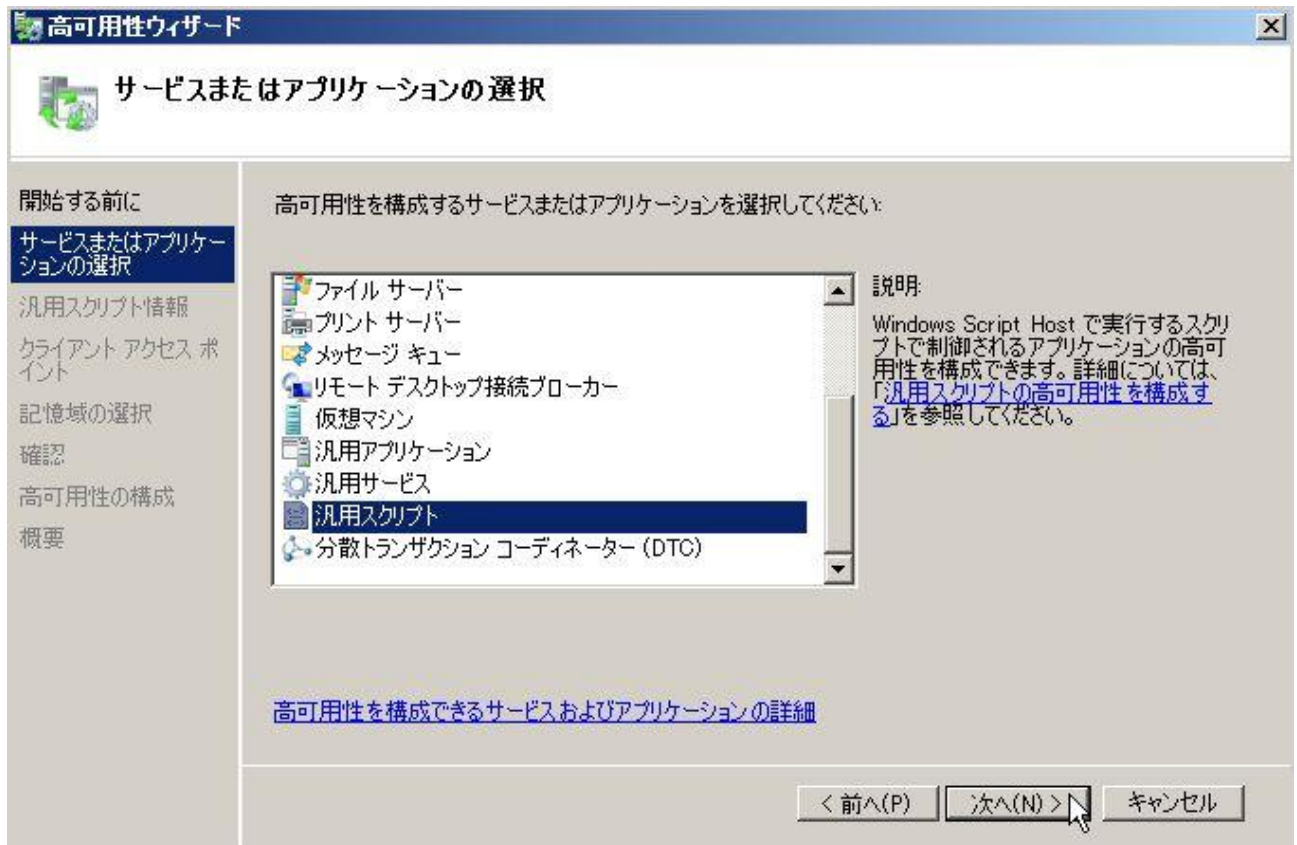
3.9.2. Cluster を選択し、右クリック>サービスまたはアプリケーションの構成を選択します。



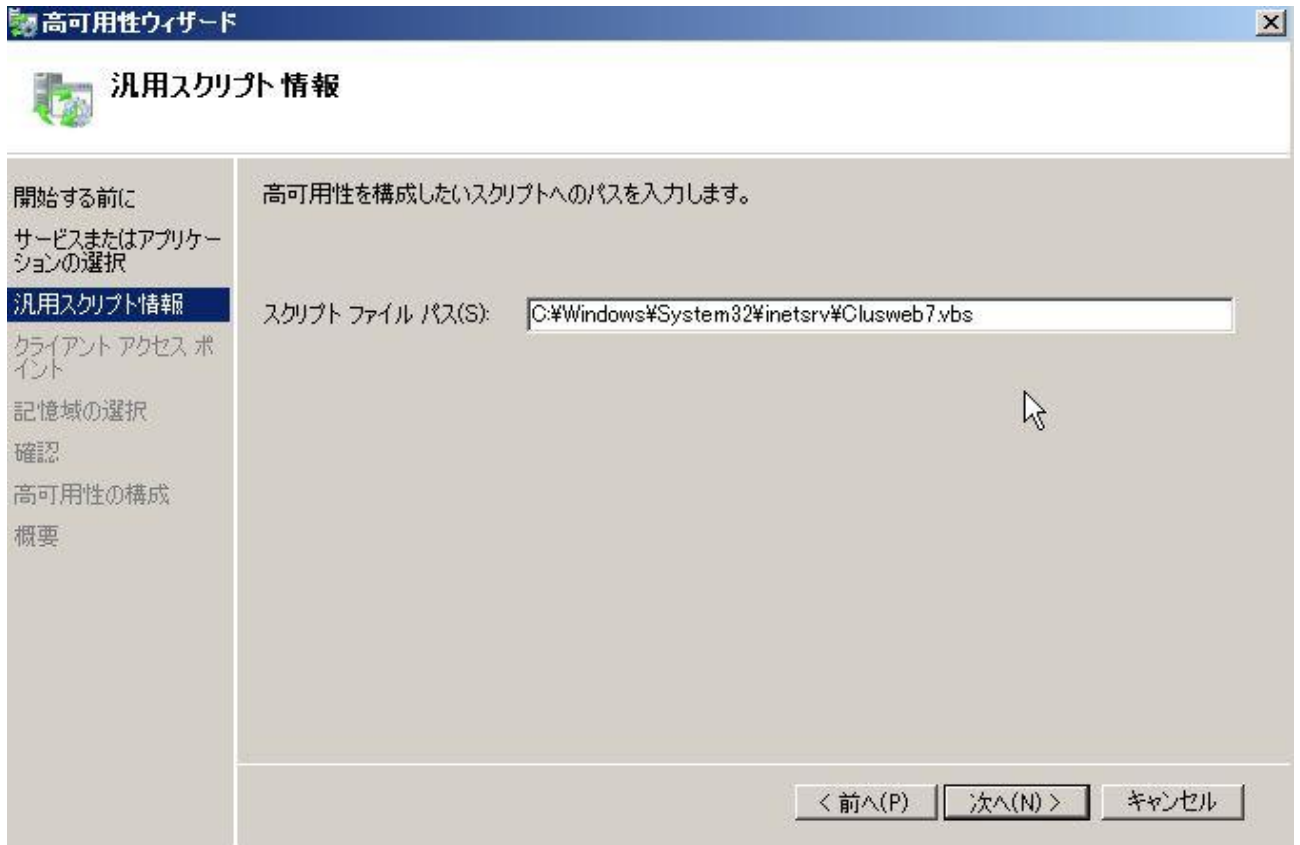
3.9.3. 高可用性ウィザードに従って設定を進めます。 「次へ」を選択します



### 3.9.4. 役割から「汎用スクリプト」を選択し、「次へ」を選択します。

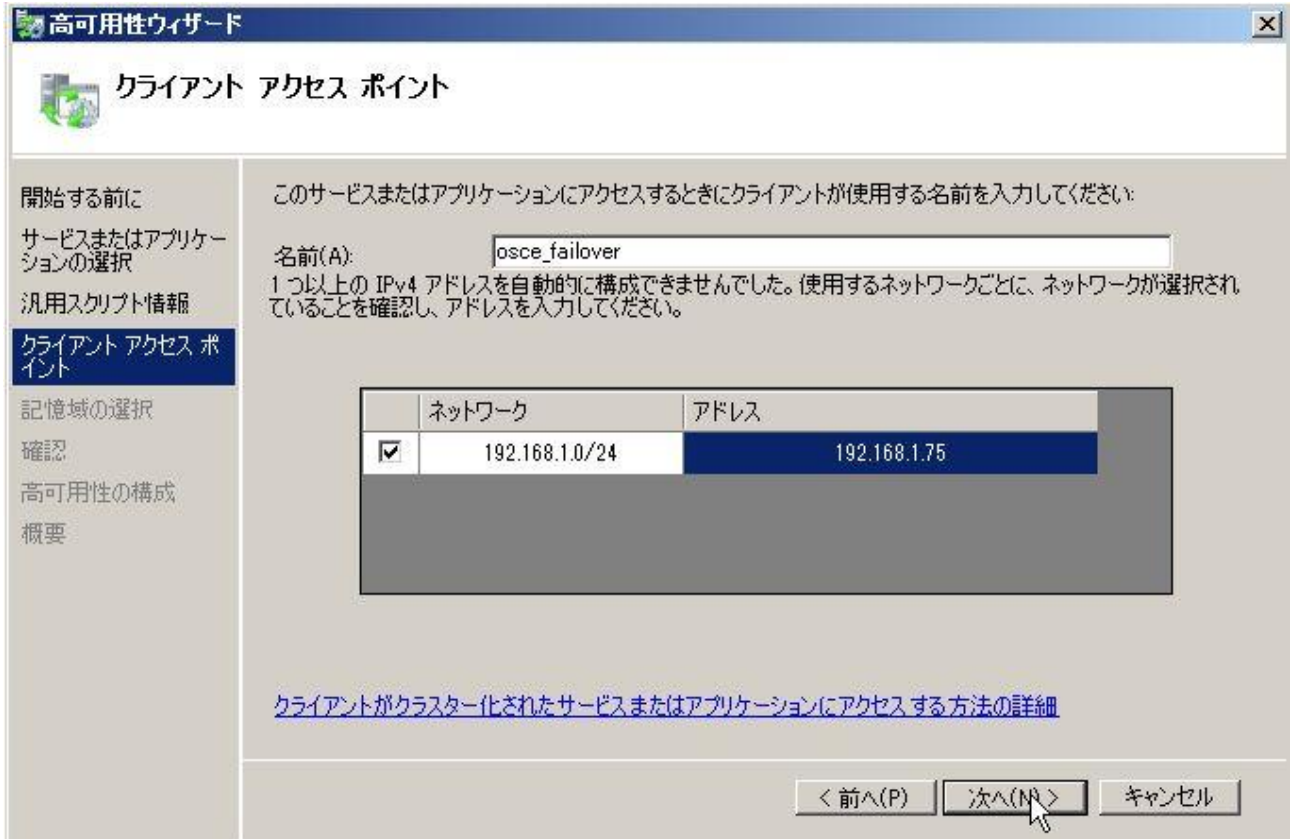


### 3.9.5. 汎用スクリプトの場所を指定します。



スクリプトファイルパスは [3.8 Cluster Generic Script の準備](#) で保存したファイルパスを指定します。

### 3.9.6. この役割にアクセスする際の名前と IP アドレスを設定します。



高可用性ウィザード

クライアント アクセス ポイント

開始する前に  
サービスまたはアプリケーションの選択  
汎用スクリプト情報  
**クライアント アクセス ポイント**  
記憶域の選択  
確認  
高可用性の構成  
概要

このサービスまたはアプリケーションにアクセスするときにクライアントが使用する名前を入力してください。

名前(A):

1 つ以上の IPv4 アドレスを自動的に構成できませんでした。使用するネットワークごとに、ネットワークが選択されていることを確認し、アドレスを入力してください。

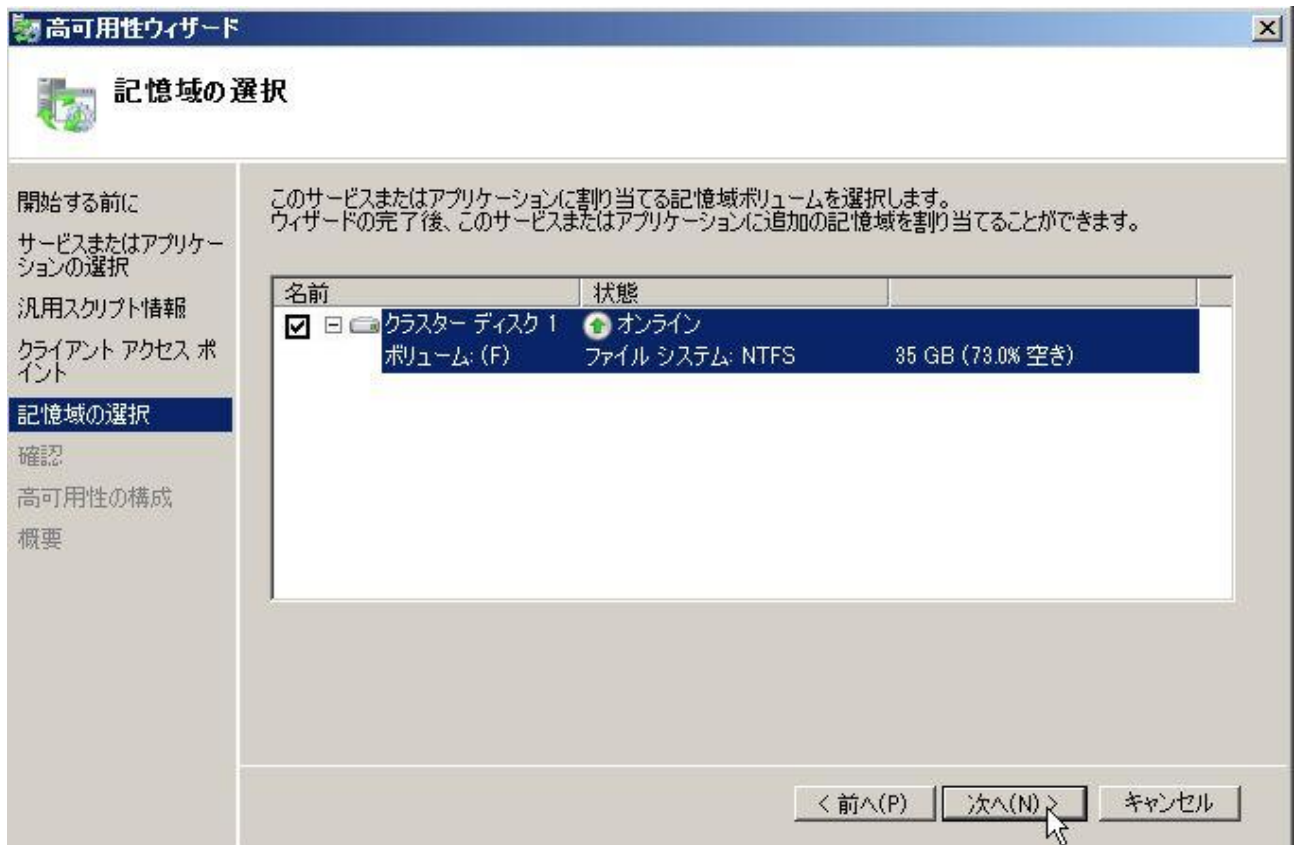
	ネットワーク	アドレス
<input checked="" type="checkbox"/>	192.168.1.0/24	192.168.1.75

[クライアントがクラスター化されたサービスまたはアプリケーションにアクセスする方法の詳細](#)

< 前へ(P)    次へ(N) >    キャンセル

ウイルスバスターCorp. クライアントを Autopcc.exe でインストールする際など、このアドレス宛の共有フォルダにアクセスします。

### 3.9.7. この役割に割り当てる共有ディスクを指定し、「次へ」を選択します。



### 3.9.8. 画面を確認し、「次へ」を選択します。



### 3.9.9. 役割が正しく構成されることを確認し、「完了」を選択します。

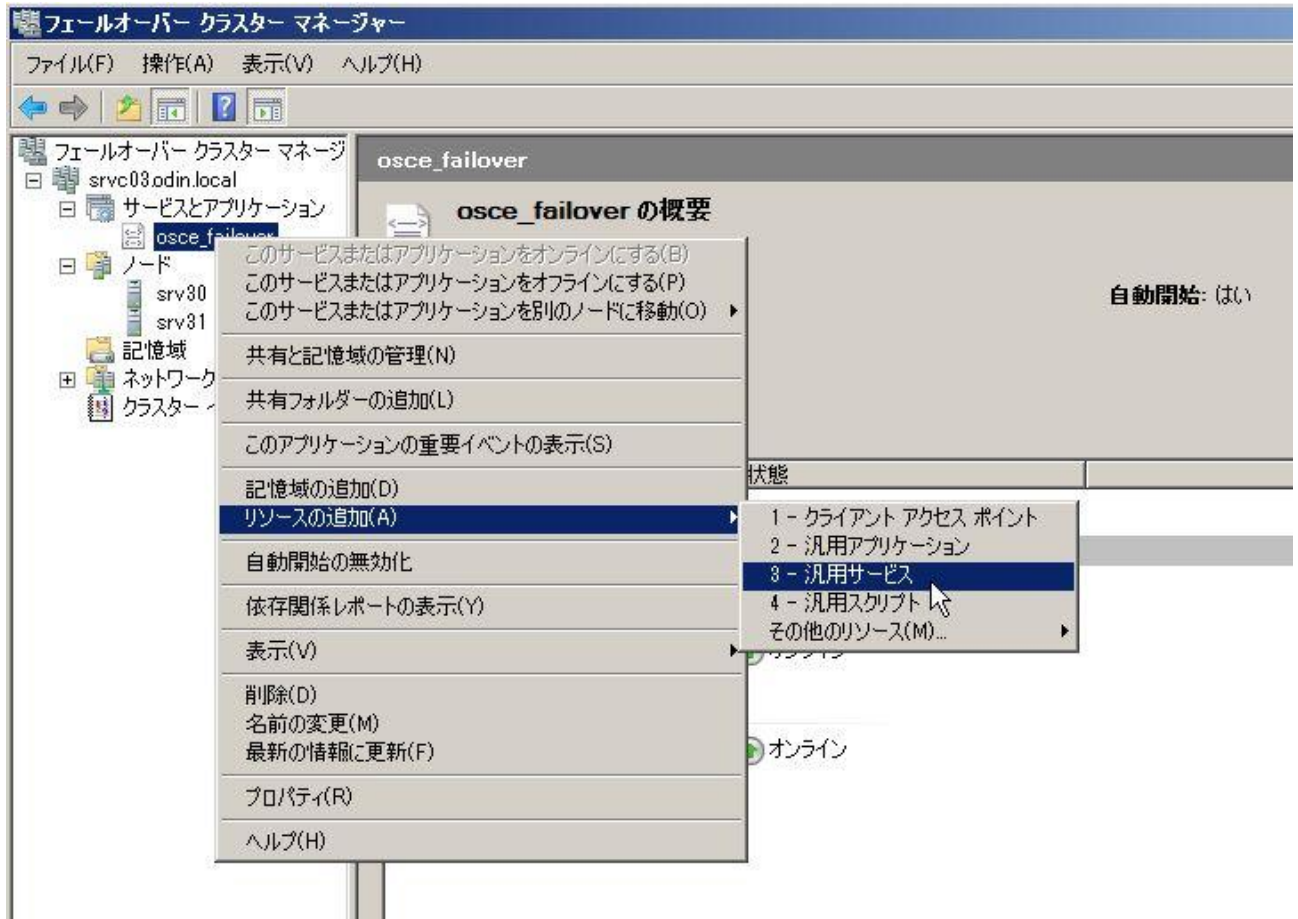




### 3.10. ウイルスバスターCorp. サービスの役割設定

この役割にリソースを追加します。

#### 3.10.1. Failover Cluster Manager を起動し、サービスを選択し、右クリック>リソースの追加>汎用サービスを選択します。



3.10.2. リソースウィザードに従って設定を進めます。 サービスの一覧から「OfficeScan Master Service」を選択し、「次へ」を選択します。



### 3.10.3. 「次へ」を選択します。



### 3.10.4. 「完了」を選択します。



### 3.10.5. 以下のサービスについても同じように追加します。

OfficeScan Active Directory Integration Service



OfficeScan Log Receiver Service



## OfficeScan Plug-in Manager





### 3.10.6. 以下 4 つのサービスを登録できたことを確認します。

名前	状態
<b>サーバー名</b>	
名前: osce_failover	オンライン
<b>ファイル サーバー</b>	
FileServer-(osce_failover)(クラスター ディ...	オンライン
<b>ディスク ドライブ</b>	
クラスター ディスク 1	オンライン
<b>その他のリソース</b>	
Clusweb7 スクリプト	オンライン
OfficeScan Active Directory Integration ...	オフライン
OfficeScan Master Service	オフライン
OfficeScan Plug-in Manager	オフライン
OfficeScan Log Receiver Service	オフライン

Trend Micro Local Web Classification Server サービスと Trend Micro Smart Scan Server サービスは登録の必要はありません。これらのサービスは OfficeScan Master Service の起動時に自動的に起動します。



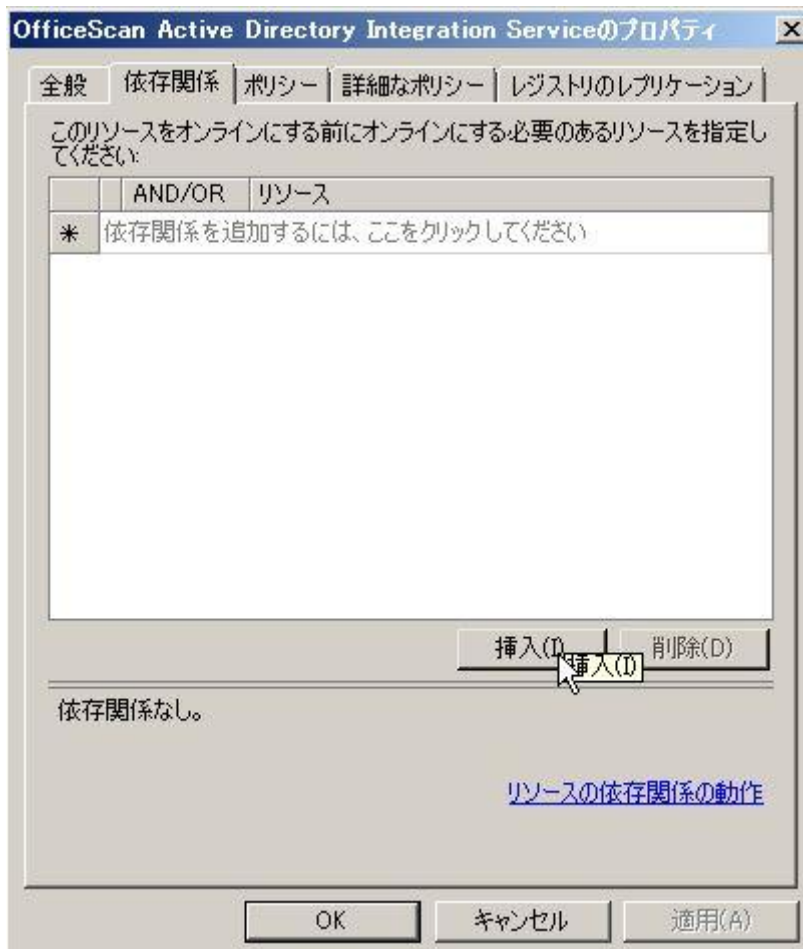
### 3.11. サービスの依存性設定

サービスに依存性の設定を行います。

#### 3.11.1. 「OfficeScan Active Directory Integration Service」を選択し、右クリック>プロパティを選択します。



### 3.11.2. 依存関係のタブを表示します。

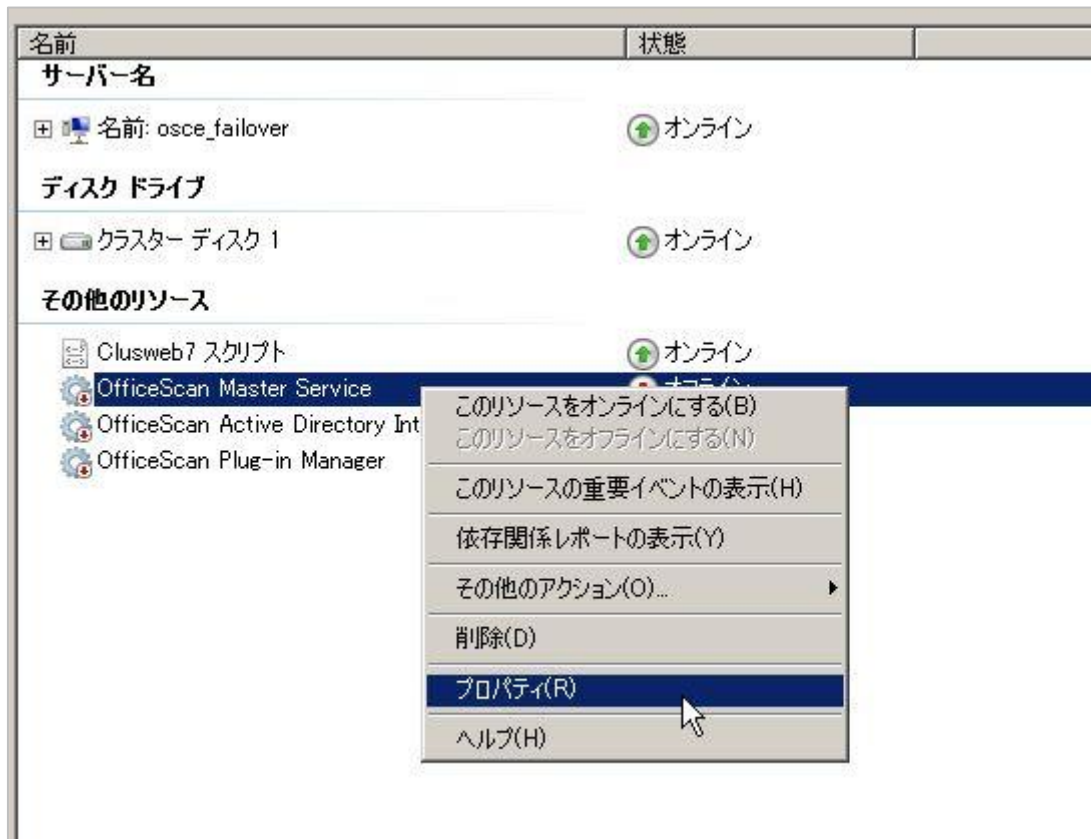


3.11.3. 依存性のあるサービスを登録します。 OfficeScan Master Service を選択し、「挿入」を選択します。



3.11.4. OfficeScan Log Received Service、OfficeScan Plug-in Manager にも同様に、依存性のあるサービスとして OfficeScan Master Service を登録します。

3.11.5. 役割の「OfficeScan Master Service」を選択し、右クリック>プロパティを選択します。



3.11.6. 依存関係タブを選択します。

### 3.11.7. Cluster Name を選択し、「挿入」を選択します。



### 3.11.8. 共有ディスクを選択し、「挿入」を選択します。





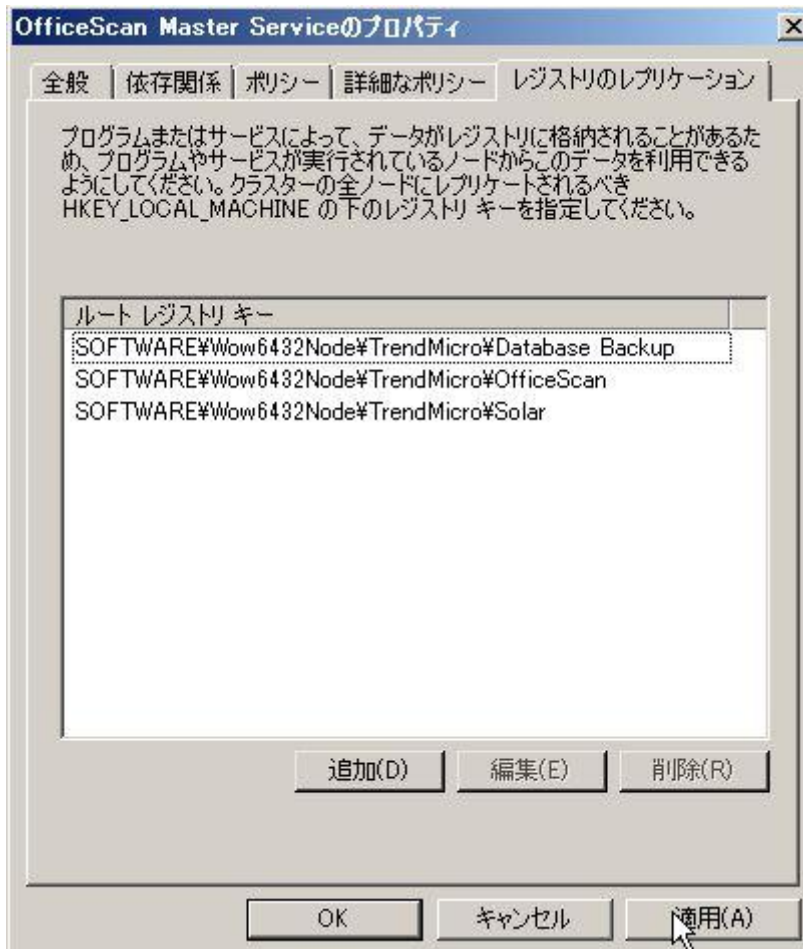
### 3.11.9. 以下のような状態になっていることを確認します。



### 3.12. レジストリのレプリケーション設定

ウイルスバスターCorp.のレジストリのレプリケーションを設定します。

#### 3.12.1. Master Service のプロパティ>レジストリのレプリケーションで以下の設定を入力します。



### 3.13. サービスの役割を起動

ウイルスバスターCorp. のサービスの役割をオンラインへ変更します。

3.13.1. Failover Cluster Manager を起動し、役割の「OfficeScan Master Service」を右クリック>オンラインを選択します。

3.13.2. 「OfficeScan Active Directory Integration Service」を右クリック>オンラインを選択します。

### 3.13.3. 全てのサービスがオンラインとなることを確認します。

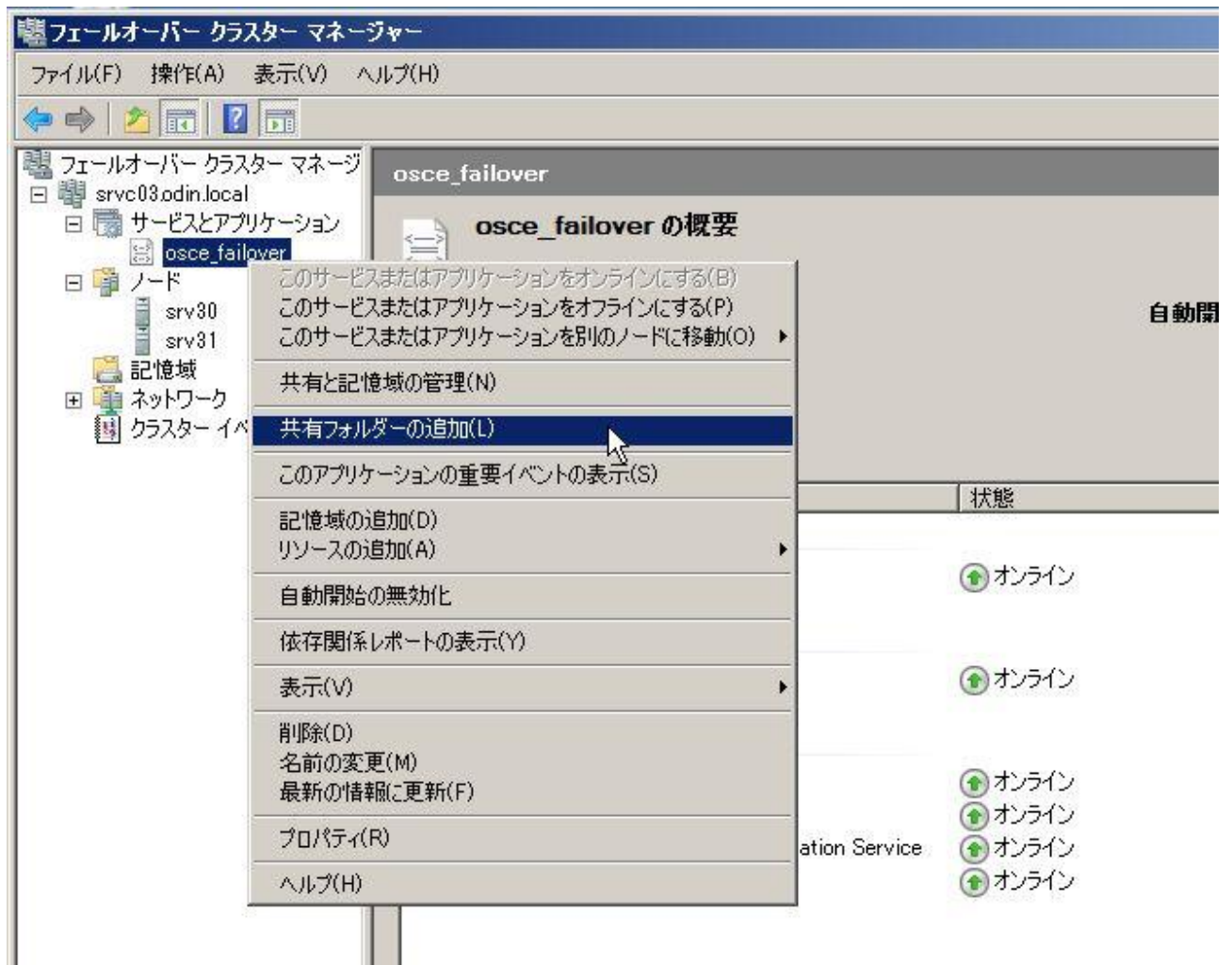
※オフラインのサービスがある場合には個別にオンラインに変更します。

名前	状態
<b>サーバー名</b>	
名前: osce_failover	オンライン
<b>ファイル サーバー</b>	
FileServer-(osce_failover)(クラスター ディ...	オンライン
<b>ディスク ドライブ</b>	
クラスター ディスク 1	オンライン
<b>その他のリソース</b>	
Clusweb7 スクリプト	オンライン
OfficeScan Active Directory Integration ...	オンライン
OfficeScan Master Service	オンライン
OfficeScan Plug-in Manager	オンライン
OfficeScan Log Receiver Service	オンライン

### 3.14. 共有フォルダの設定

ウイルスバスターCorp.の共有フォルダを設定します。

#### 3.14.1. Failover Cluster Manager を起動し、サービスを選択し、右クリック>共有フォルダーの追加を選択します。



### 3.14.2. 共有フォルダーの場所の参照を選択します。

共有フォルダーの準備ウィザード (osce\_failover)

共有フォルダーの場所

ステップ:

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- 設定の確認と共有の作成
- 確認

共有するフォルダーを指定します。適切な種類で十分な空き領域のあるボリューム上で、既存のフォルダーを選択するか、または新しいフォルダーを作成してください。適切なボリュームが存在しない場合は、[記憶域の準備] をクリックし、新しいボリュームを作成してください。

場所(L):

参照(B)...

利用可能なボリューム(A):

ボリューム	容量	空き領域	種類
ボリューム (F:)	35.0 GB	25.6 GB	シンプル

詳細

ボリューム: ボリューム (F:)  
 シャドウ コピー: 不明  
 インデックス: 不明  
 高可用性サーバー: OSCE\_FAILOVER

記憶域の準備(S)...

< 前へ(P)    次へ(N) >    キャンセル



### 3.14.3. PCCSRV フォルダを選択し、次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

共有フォルダーの場所

ステップ:

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- 設定の確認と共有の作成
- 確認

共有するフォルダーを指定します。適切な種類で十分な空き領域のあるボリューム上で、既存のフォルダーを選択するか、または新しいフォルダーを作成してください。適切なボリュームが存在しない場合は、[記憶域の準備] をクリックし、新しいボリュームを作成してください。

場所(L):

F:\Trend Micro\OfficeScan\PCCSRV

参照(B)...

利用可能なボリューム(A):

ボリューム	容量	空き領域	種類
ボリューム (F:)	35.0 GB	25.6 GB	シンプル

詳細

ボリューム: ボリューム (F:)

シャドウ コピー: 不明

インデックス: 不明

高可用性サーバー: OSCE\_FAILOVER

記憶域の準備(S)...

< 前へ(P)    次へ(N) >    キャンセル

#### 3.14.4. NTFS アクセス許可の設定画面では設定を変更せずに、次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

NTFS アクセス許可

**ステップ:**

- 共有フォルダーの場所
- NTFS アクセス許可**
- 共有プロトコル
- 設定の確認と共有の作成
- 確認

NTFS アクセス許可を指定して、このフォルダーに対して各ユーザーおよび各グループがローカルにアクセスする方法を制御します。共有フォルダーへのネットワーク アクセスでは、NTFS アクセス許可や、共有プロトコルを使用するように構成された共有のアクセス許可への制限を強化することで、ユーザーやグループに付与するアクセス レベルを定義します。

パス(A):  
F:\Trend Micro\OfficeScan\POCSR\

このフォルダの NTFS アクセス許可を変更しますか?

☒ いいえ、NTFS アクセス許可を変更しません(O)

☐ はい、NTFS アクセス許可を変更します(Y)

NTFS アクセス許可を変更するには、[アクセス許可の編集] をクリックします。

アクセス許可の編集(E)...

共有およびアクセス許可の詳細については、「[共有フォルダーのアクセス許可を管理する](#)」を参照してください。

### 3.14.5. 共有名に OFCSCAN を指定し、次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

共有プロトコル

**ステップ:**

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- SMB 設定
- SMB アクセス許可
- DFS 名前空間への発行
- 設定の確認と共有の作成
- 確認

ユーザーがこの共有フォルダーへのアクセスに使用するプロトコルを選択します。

☒ SMB(S)


共有名(H):  
OFCSCAN

共有パス(E):  
\\OSCE\_FAILOVER\\OFCSCAN

☐ NFS(F)

共有名(A):  
[ ]

共有パス(R):  
[ ]

 このサーバーには NFS 用のサービスがインストールされていません。

高可用性の共有の作成に関する詳細については、[クラスター アドミニストレーターのヘルプ](#)を参照してください。

< 前へ(P)    次へ(N) >    キャンセル

### 3.14.6. 次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

**SMB 設定**

**ステップ:**

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- SMB 設定**
- SMB アクセス許可
- DFS 名前空間への発行
- 設定の確認と共有の作成
- 確認

SMB プロトコル経由でアクセスするクライアントが、この共有フォルダーをどのように使用するかを指定します。説明を使用して、共有フォルダーの使用方法に関するコメントを追加できます。最大接続数、アクセス ベースの列挙、オフラインでの利用など、詳細な SMB 設定も制御できます。

共有パス(S):  
\\OSCE\_FAILOVER\OFOSCAN

説明(D):

**詳細設定**

ユーザー数制限(U): 最大許容値

アクセス ベースの列挙(E): 無効

オフラインの設定(O): 選択されたファイルとプログラムのみオフライン利用可能

これらの設定を変更するには、[詳細設定] をクリックしてください。

詳細設定(A)...

< 前へ(P)    次へ(N) >    キャンセル

### 3.14.7. SMB アクセス許可で Administrators がフルコントロールを持ち、他のすべてのユーザとグループは読み取りのアクセス権を持つ にチェックを要れ、次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

**SMB アクセス許可**

**ステップ:**

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- SMB 設定
- SMB アクセス許可**
- DFS 名前空間への発行
- 設定の確認と共有の作成確認

共有フォルダーへの SMB ベースのアクセスについて共有のアクセス許可を指定します。共有フォルダーへのネットワーク アクセスでは、共有のアクセス許可や NTFS アクセス許可への制限を強化することで、ユーザーやグループに付与するアクセス レベルを定義します。

共有パス(S):

次の基本的な共有のアクセス許可から選択するか、またはカスタムの共有アクセス許可を作成してください。

- ☐ すべてのユーザーとグループは読み取りのみのアクセス権を持つ(A)
- ☒ Administrators がフル コントロールを持ち、他のすべてのユーザーとグループは読み取りのみのアクセス権を持つ(D)
- ☐ Administrators がフル コントロールを持ち、他のすべてのユーザーとグループは読み取りと書き込みのみのアクセス権を持つ(M)
- ☐ ユーザーとグループはカスタムの共有アクセス許可を持つ(U):

共有およびアクセス許可の詳細については、「[共有フォルダーのアクセス許可を管理する](#)」を参照してください。

### 3.14.8. 次へを選択します。

共有フォルダーの準備ウィザード (osce\_failover)

DFS 名前空間への発行

**ステップ:**

- 共有フォルダーの場所
- NTFS アクセス許可
- 共有プロトコル
- SMB 設定
- SMB アクセス許可
- DFS 名前空間への発行**
- 設定の確認と共有の作成
- 確認

既存の名前空間および名前空間に作成するフォルダーを指定して、DFS 名前空間に SMB 共有を発行できます。名前空間パスの最後のフォルダーに、フォルダーターゲットとして新しい共有が設定されます。

☐ DFS 名前空間への SMB 共有の発行(U)

名前空間での親フォルダー(F):  
 参照(B)...

例: \\\*Domain\*Name\*Folder

新規フォルダー名(E):

例: <名前> または <新規フォルダー>\*<名前>

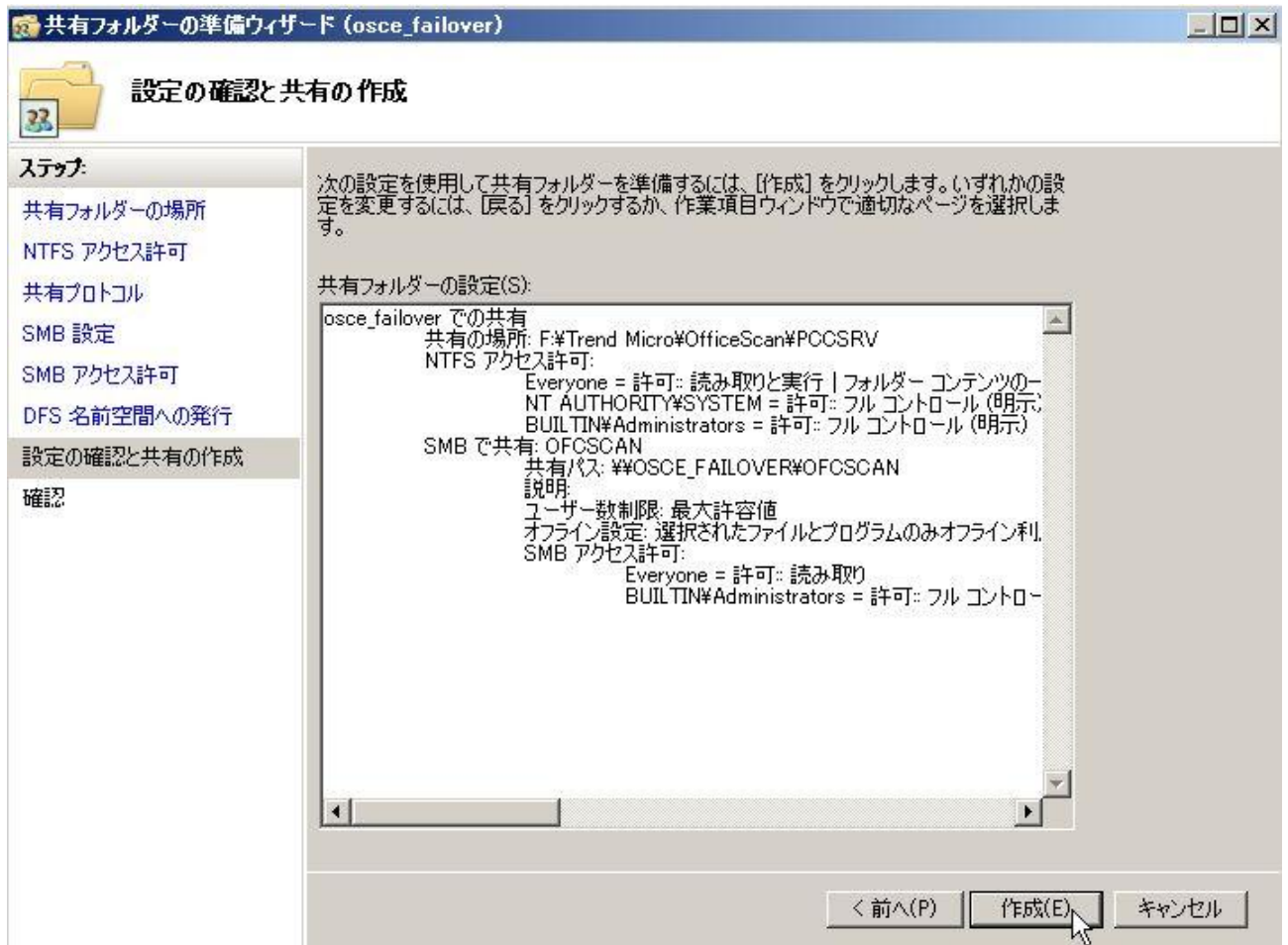
名前空間パスのプレビュー(R):

DFS 名前空間の詳細については、「[名前空間](#)」を参照してください。

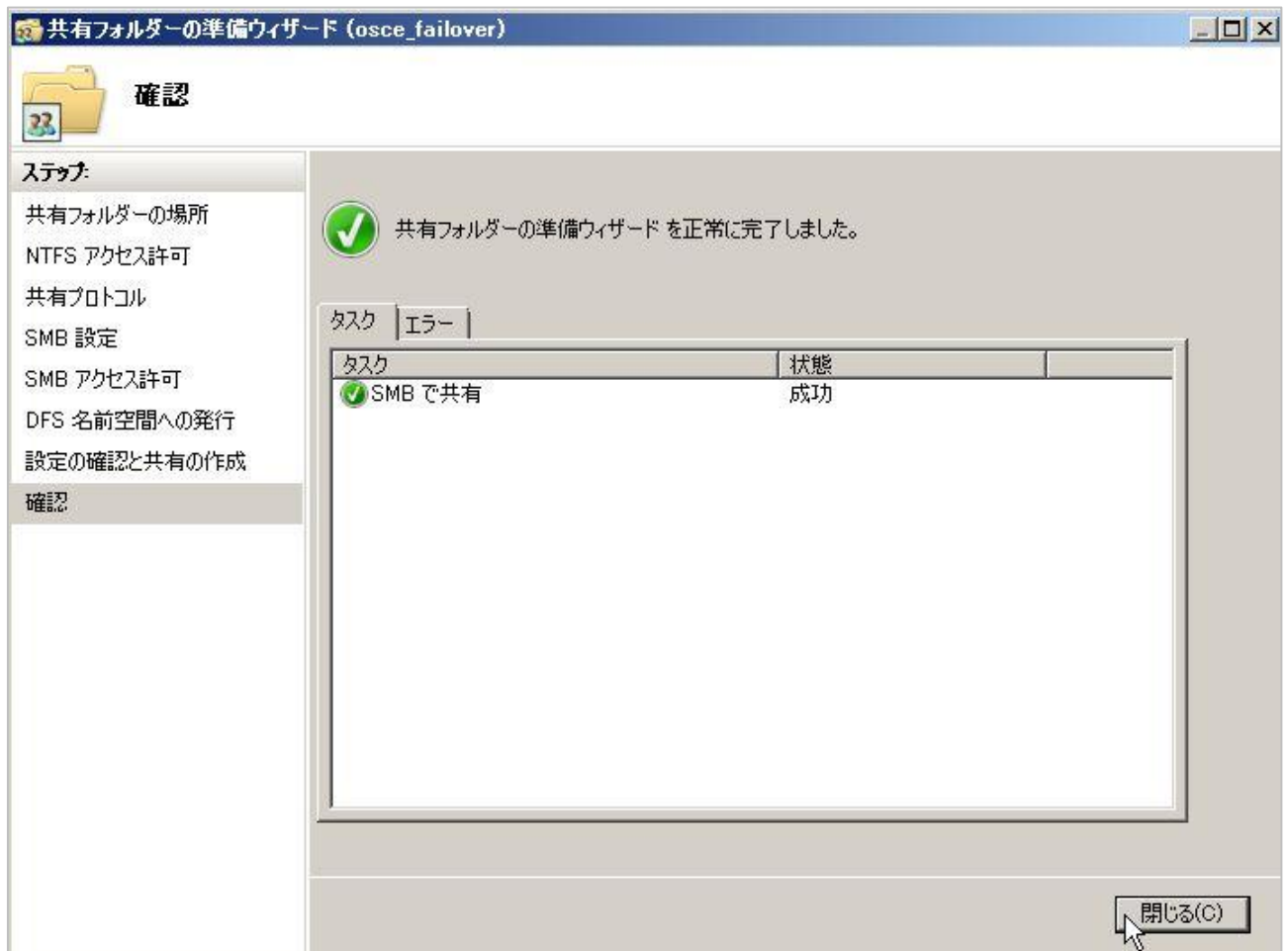
< 前へ(P)    次へ(N) >    キャンセル

















### 3.14.9. 作成を選択します。





### 3.14.10. 閉じるを選択します。



以下のような状態になることを確認します。

名前	状態
サーバー名	
 名前: osce_failover	 オンライン
ファイル サーバー	
 FileServer-(osce_failover)(クラスター ディ...	 オンライン
ディスク ドライブ	
 クラスター ディスク 1	 オンライン
その他のリソース	
 Clusweb7 スクリプト	 オンライン
 OfficeScan Active Directory Integration ...	 オンライン
 OfficeScan Master Service	 オンライン
 OfficeScan Plug-in Manager	 オンライン
 OfficeScan Log Receiver Service	 オンライン

共有フォルダー:				
共有名	フォルダー パス	種類	クライアント接続数	説明
 F\$	F:\	Windows	0	
 OFCSCAN	F:\Trend Micro\Offic...	Windows	0	

### 3.15. ウイルスバスターCorp.クライアントの設定

クラスタ環境では、ウイルスバスターCorp.サーバは複数の NIC を使用します。そのため、ウイルスバスターCorp.クライアントが適切ではない NIC の IP アドレスをウイルスバスターCorp.サーバの IP アドレスとして認識してしまう場合が想定されます。

そこで、クラスタ環境においてはウイルスバスターCorp.クライアントにてウイルスバスターCorp.サーバの IP を正しく認識できるよう設定を追加します。

#### 3.15.1. ウイルスバスターCorp.サーバの<インストールフォルダ>\ofcscan.ini を編集します。

以下のように[Global Setting]の項目で、IPTemplate の設定を有効にします。

```
[Global Setting]
IPTemplateDeployEnable=1
IPTemplateDeploy0=192.168.1.X
IPTemplateDeploy1=192.168.2.X
...
```

※ウイルスバスターCorp.サーバがウイルスバスターCorp.クライアントと通信する可能性のある IP アドレスの範囲を IPTemplateDeployX=X.X.X.X で指定します。

#### 3.15.2. ファイルを保存後、ウイルスバスターCorp.の管理コンソールにログインし、クライアント>グローバルクライアント設定>保存を選択します。