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

文書管理番号

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】

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 上で稼動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 サーバを稼動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。

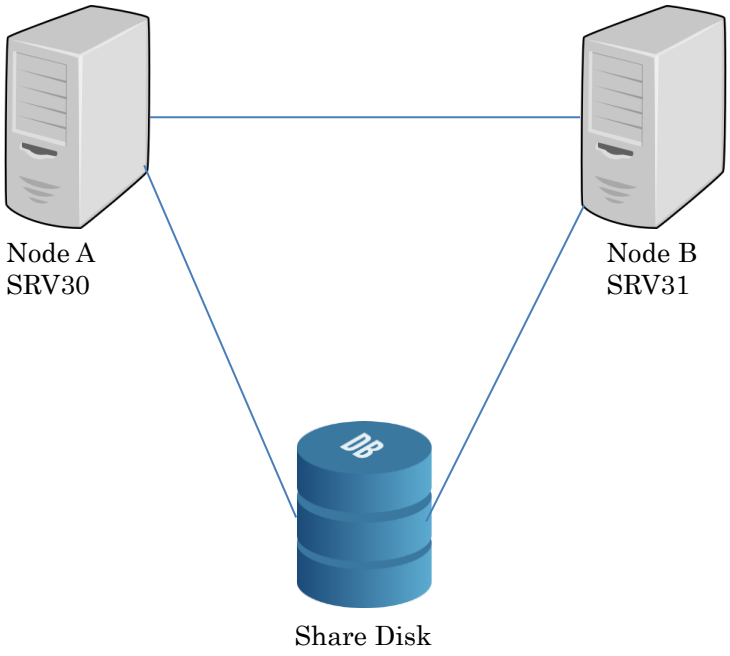
2. 事前準備

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

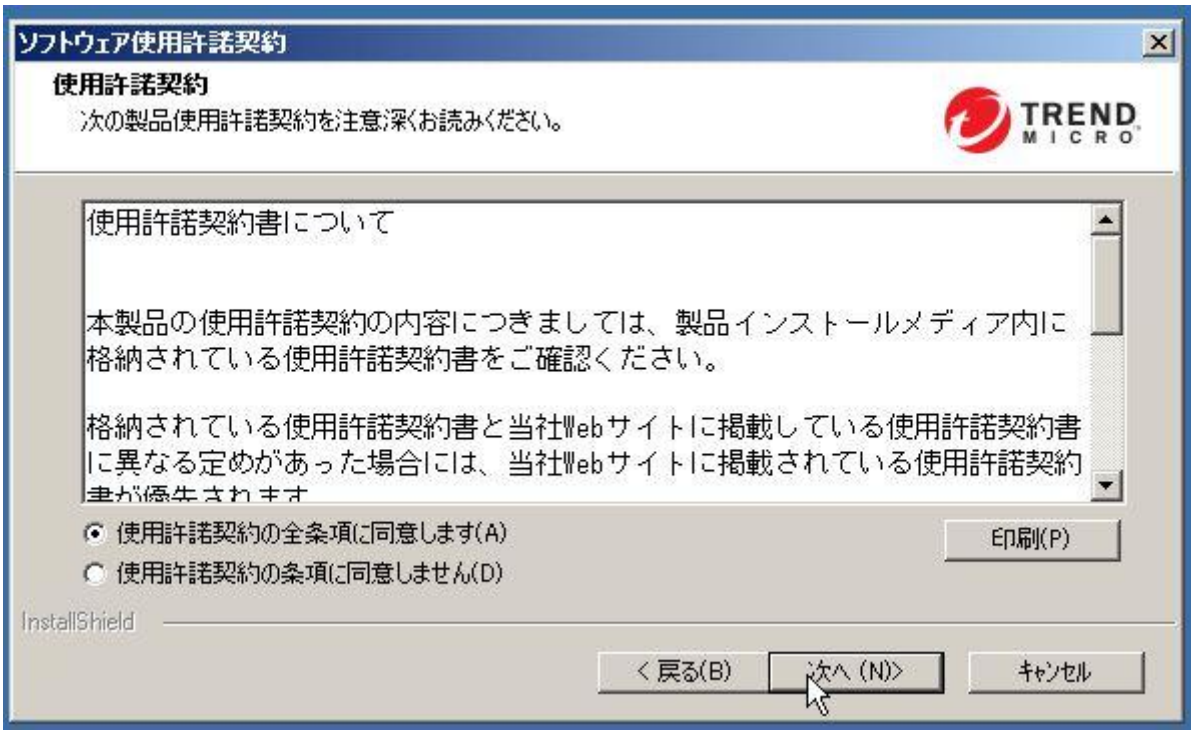
本手順は Node A、Node B それぞれで実施する必要があります。

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

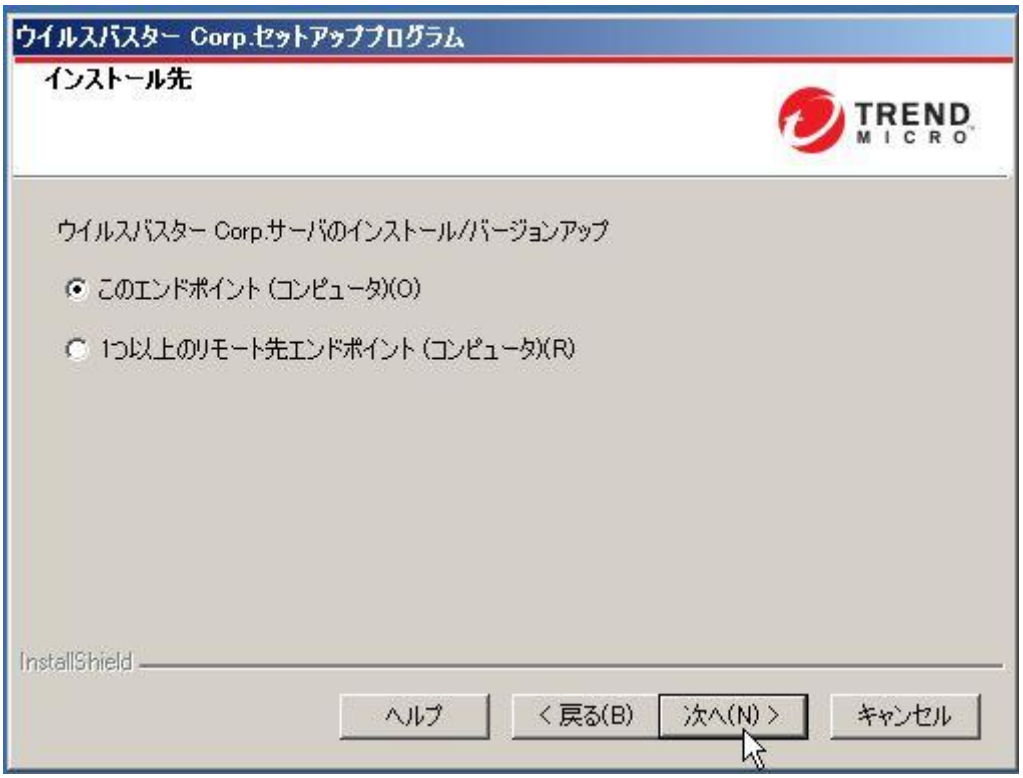
3.1.1. インストーラを起動し、「開始」を選択します。

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。

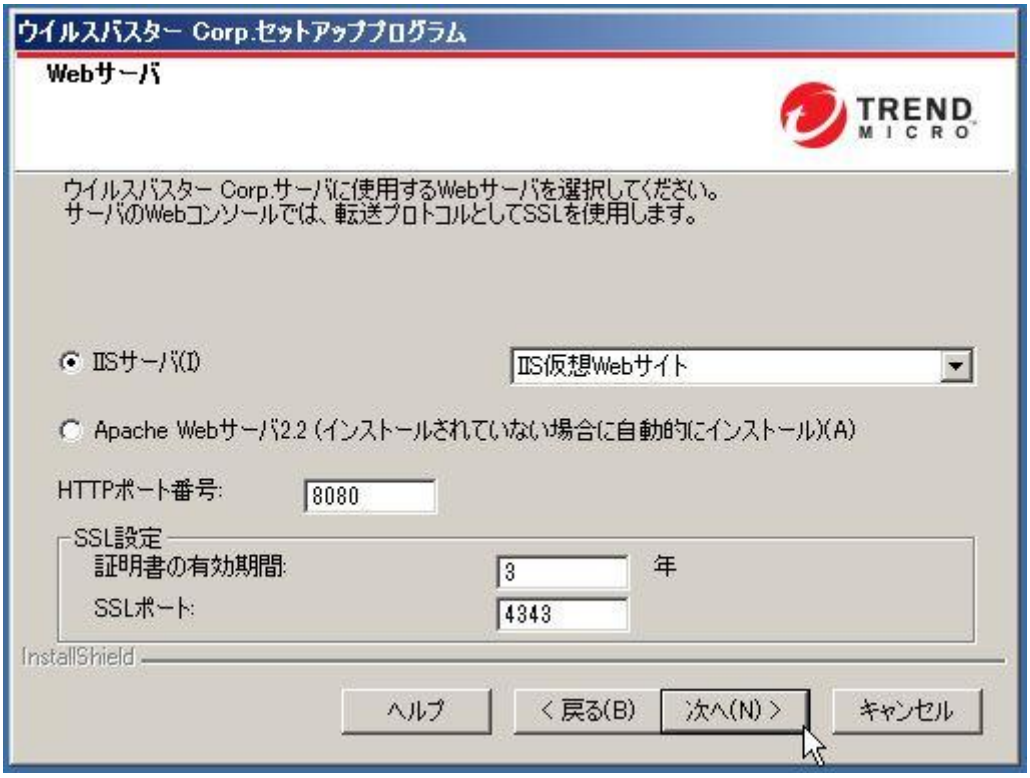
インストール先として、Cluster の共有ディスクを指定するため、「参照」を選択します。

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。

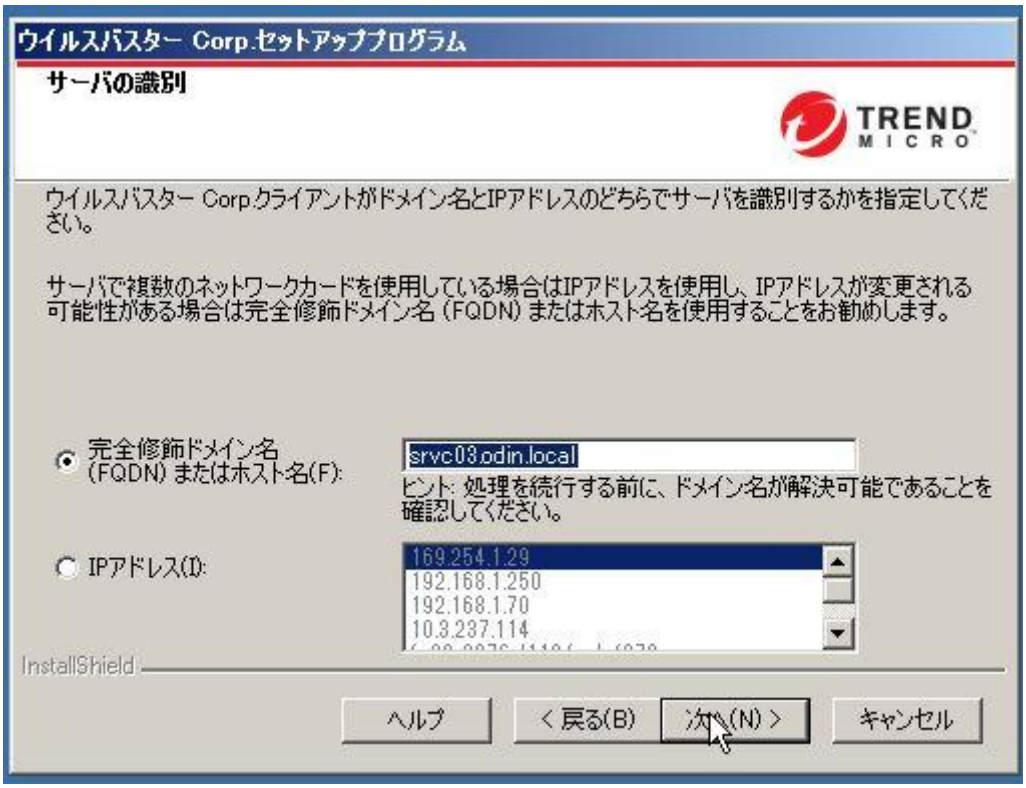
3.1.7. プロキシサーバの利用の有無を選択し、「次へ」を選択します。

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。



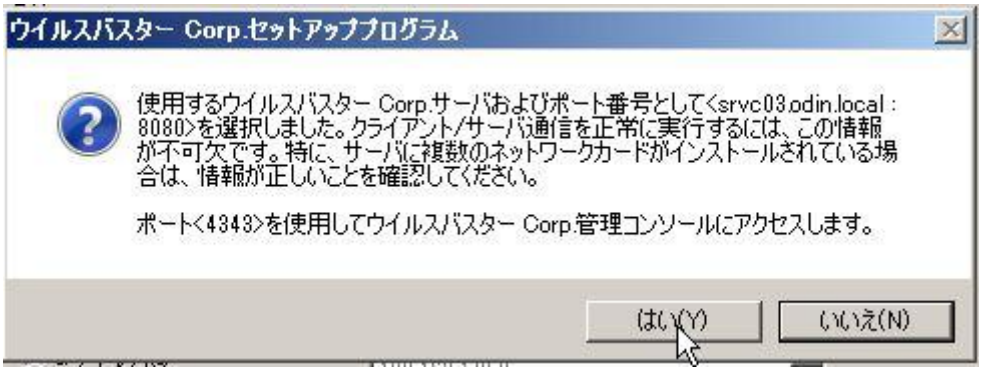
IIS が選択されていない場合、IIS のセットアップが正しく行われていません。
ウイルスバスターCorp.11.0 のインストール前に IIS のセットアップを完了させて下さい。
http://esupport.trendmicro.com/solution/ja-JP/1306142.aspx

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。

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。

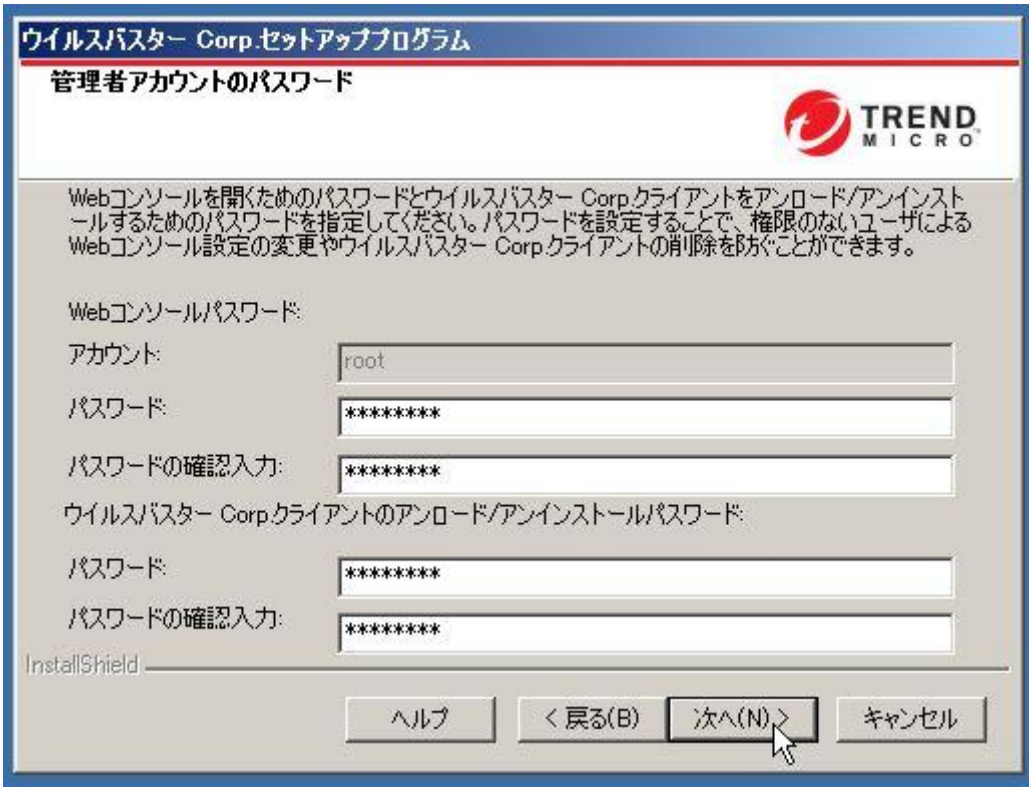
3.1.11. クライアントの方式を選択し、「次へ」を選択します。

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。

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。

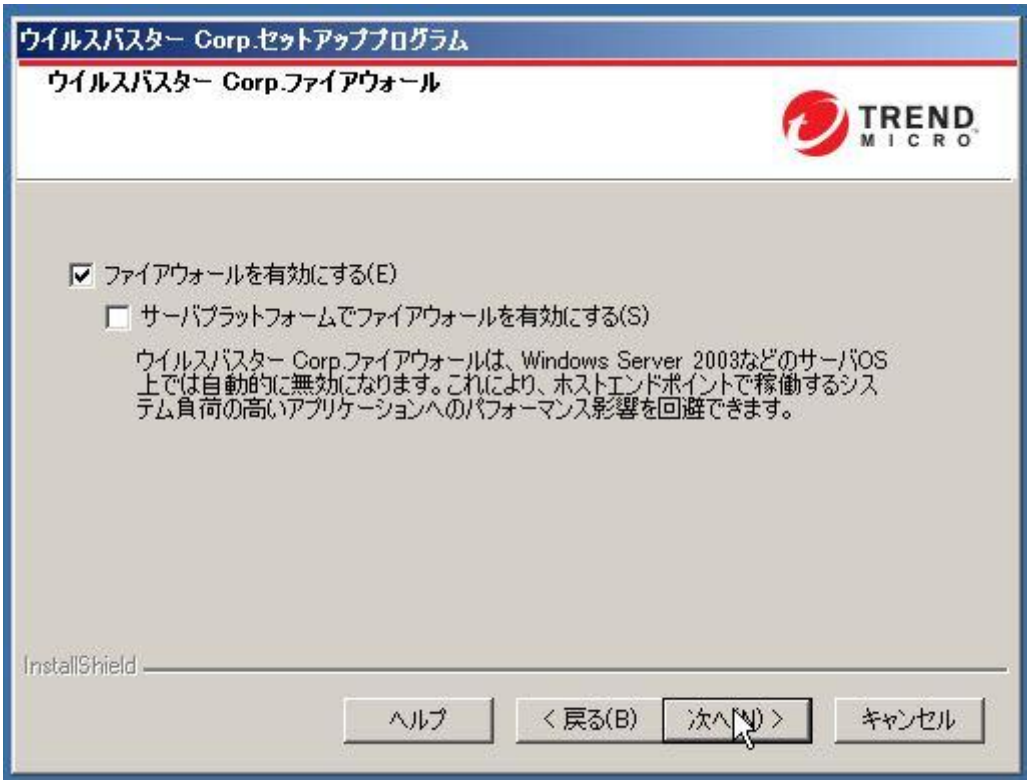
3.1.14. スマートフィードバックを有効にするかを選択し、「次へ」を選択します。

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。



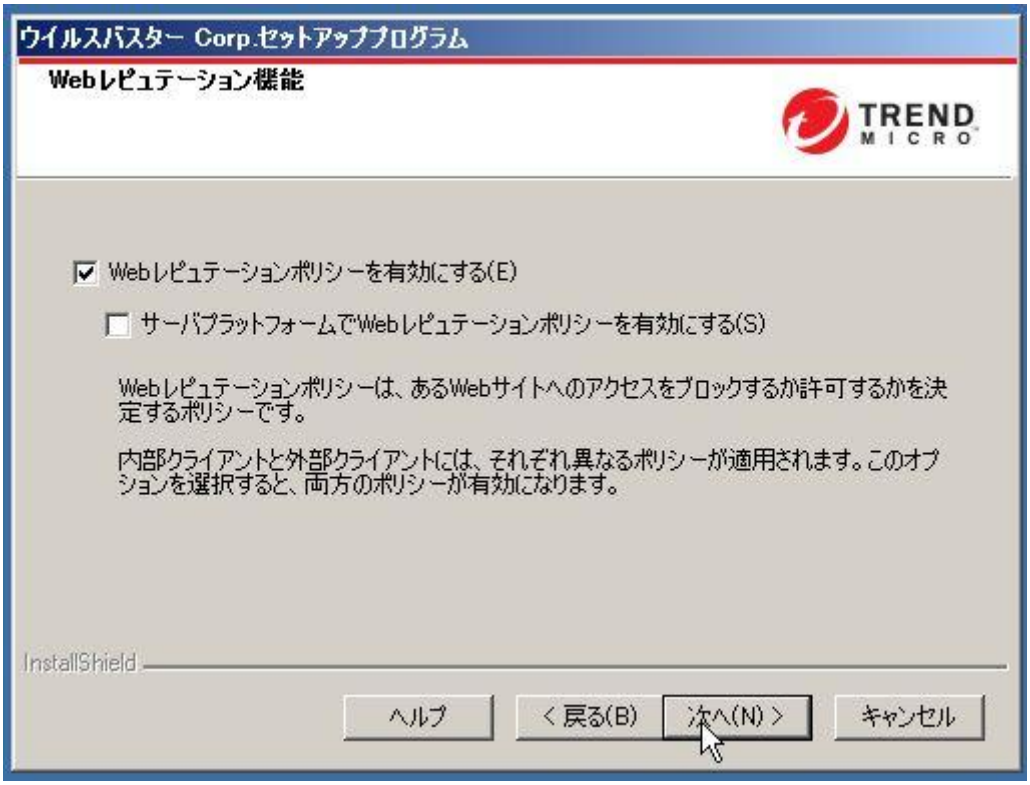
3.1.16. ウイルスバスターCorp.クライアントのインストールパス、接続ポートを設定し、「次へ」を選択します。

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。

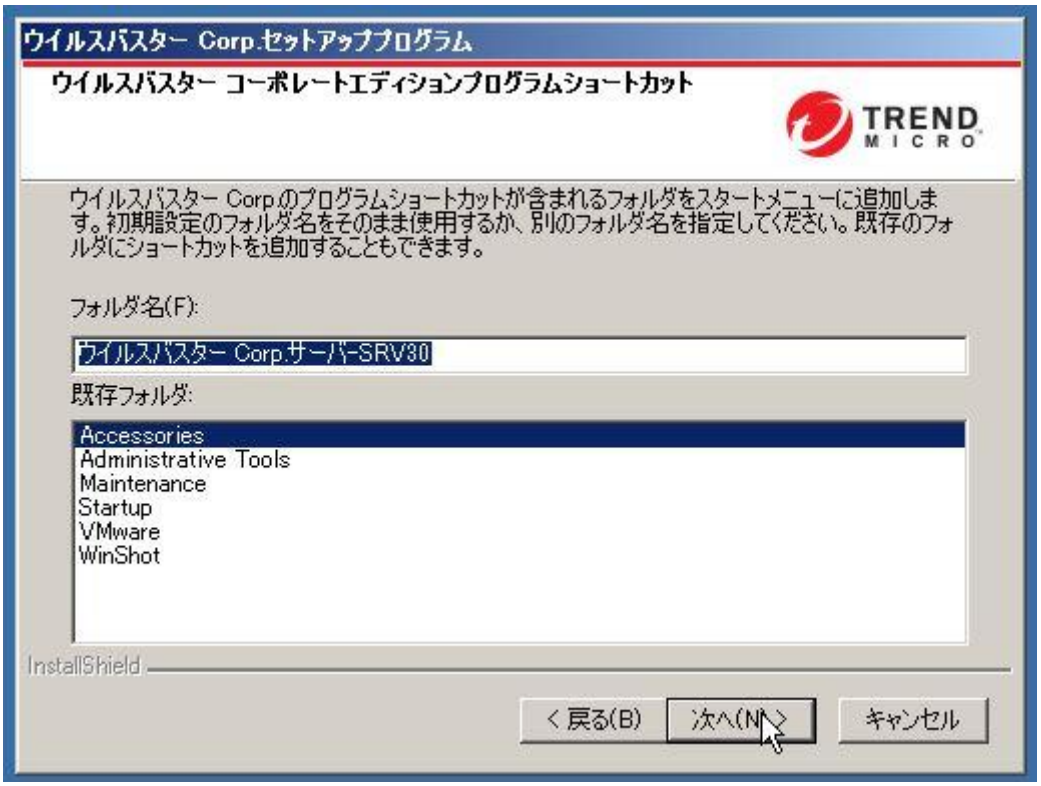
3.1.19. Web レピュテーションを有効にするかを選択し、「次へ」を選択します。



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。

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。

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、Plugin 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下さい。

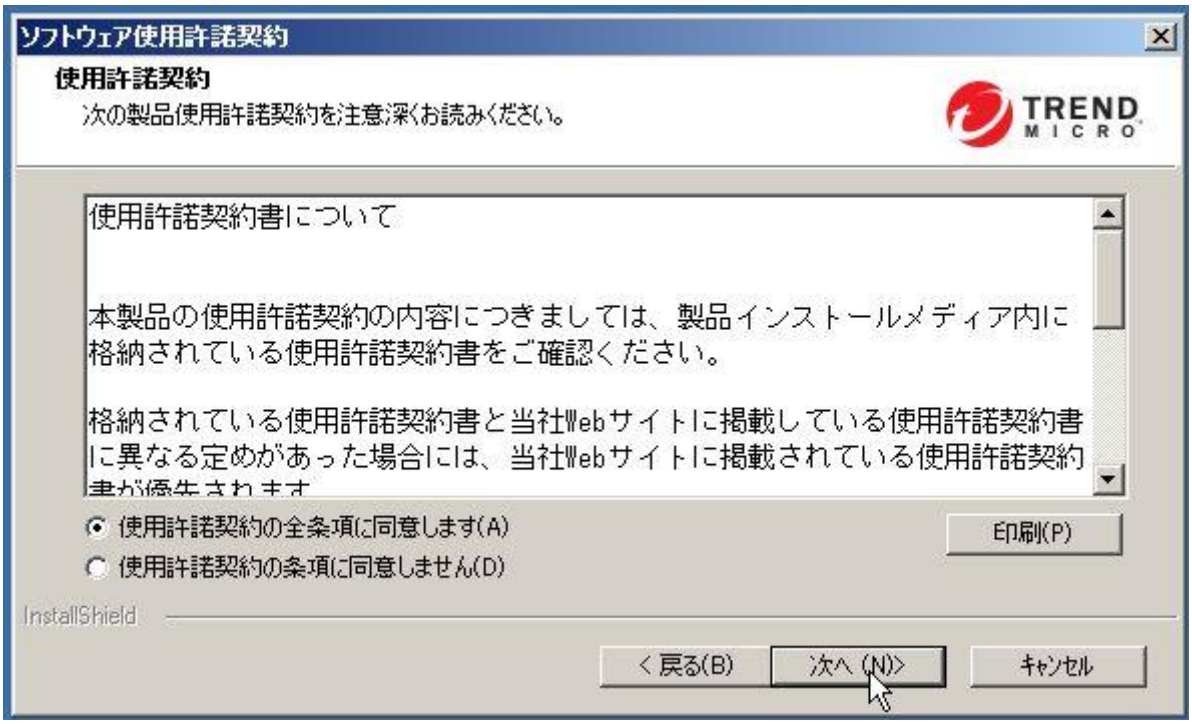
AuthCertBackup フォルダは NodeA インストール時に作成したサーバ証明書のバックアップが保存されているので、そのまま残しておきます。

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

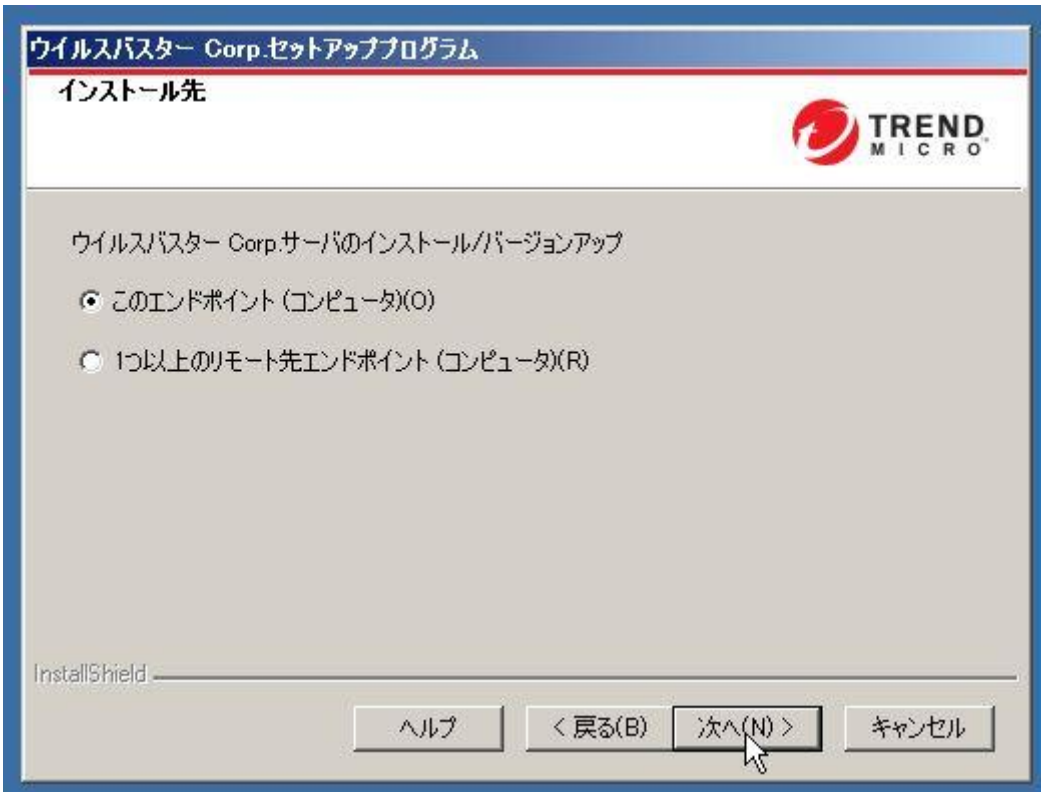
3.4.1. インストーラを起動し、「開始」を選択します。

3.4.2. 「次へ」を選択します。

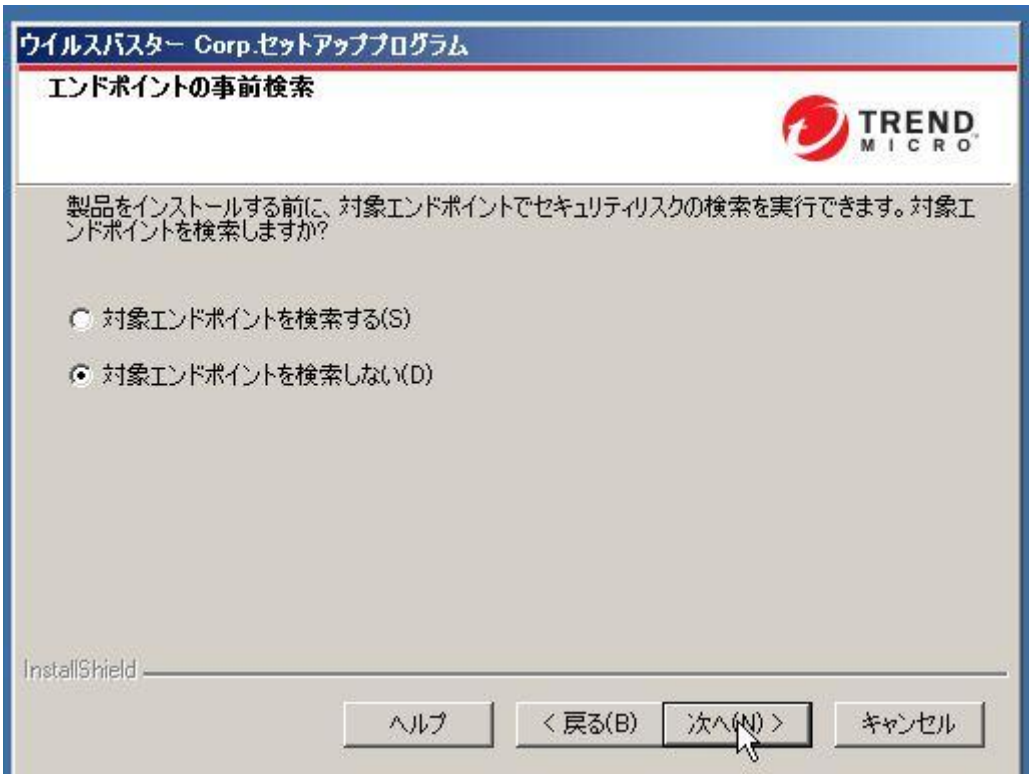
3.4.3. 使用許諾を読み、「同意します」にチェックを入れ「次へ」を選択します。



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。

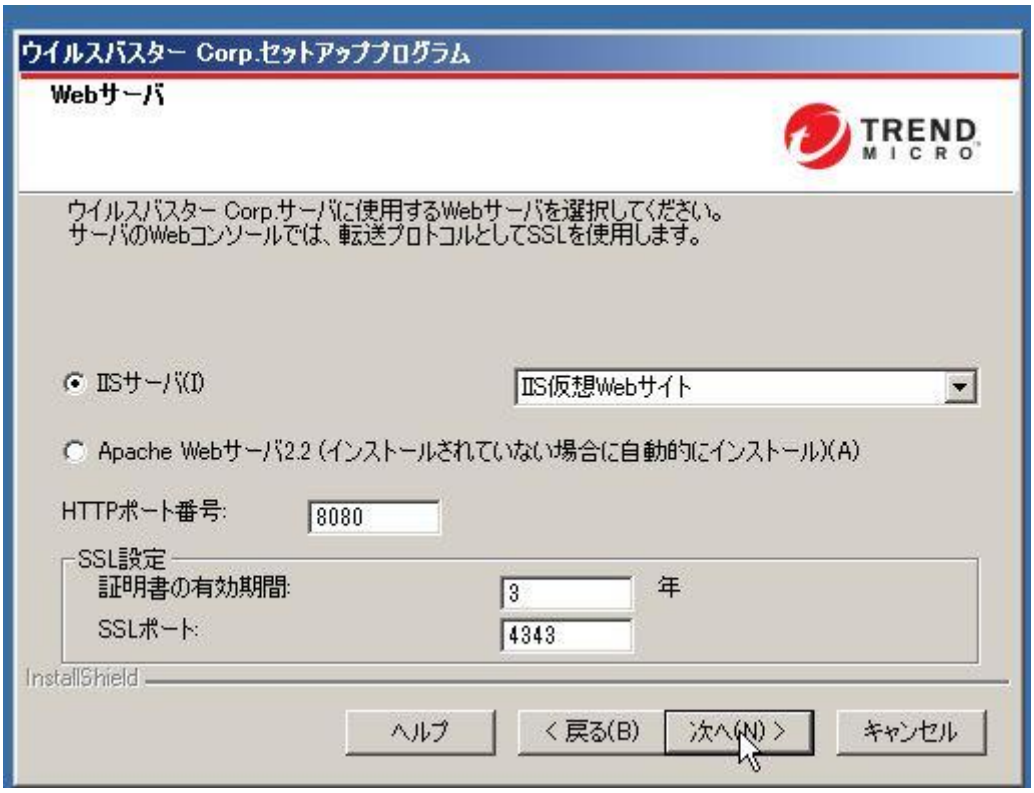
ここではインストール先として、Cluster の共有ディスクを指定するため、「参照」を選択します。

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。

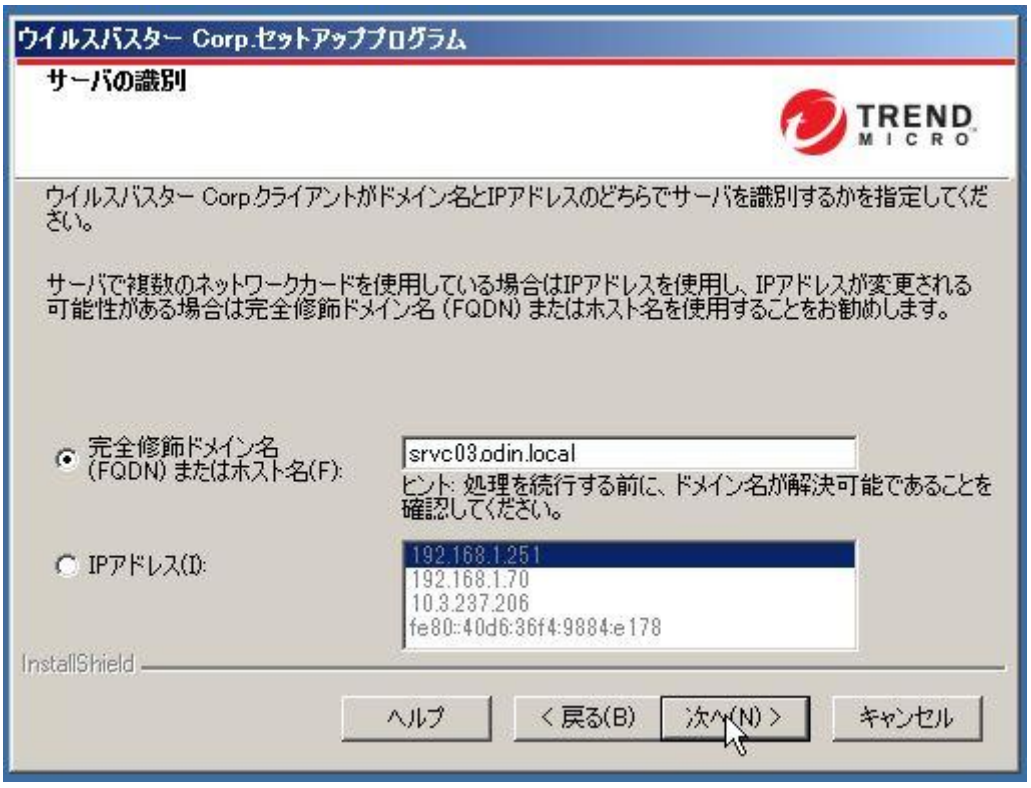
Cluster の共有ディスクが見えない場合、共有ディスクの所有者が Node B に移っていることを確認してください。

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。

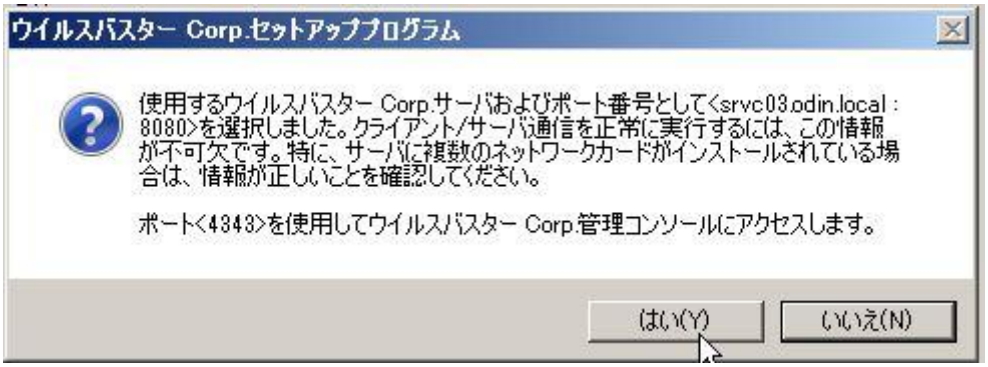
3.4.8. Web サーバとして IIS が選択されている事を確認し、「次へ」を選択します。



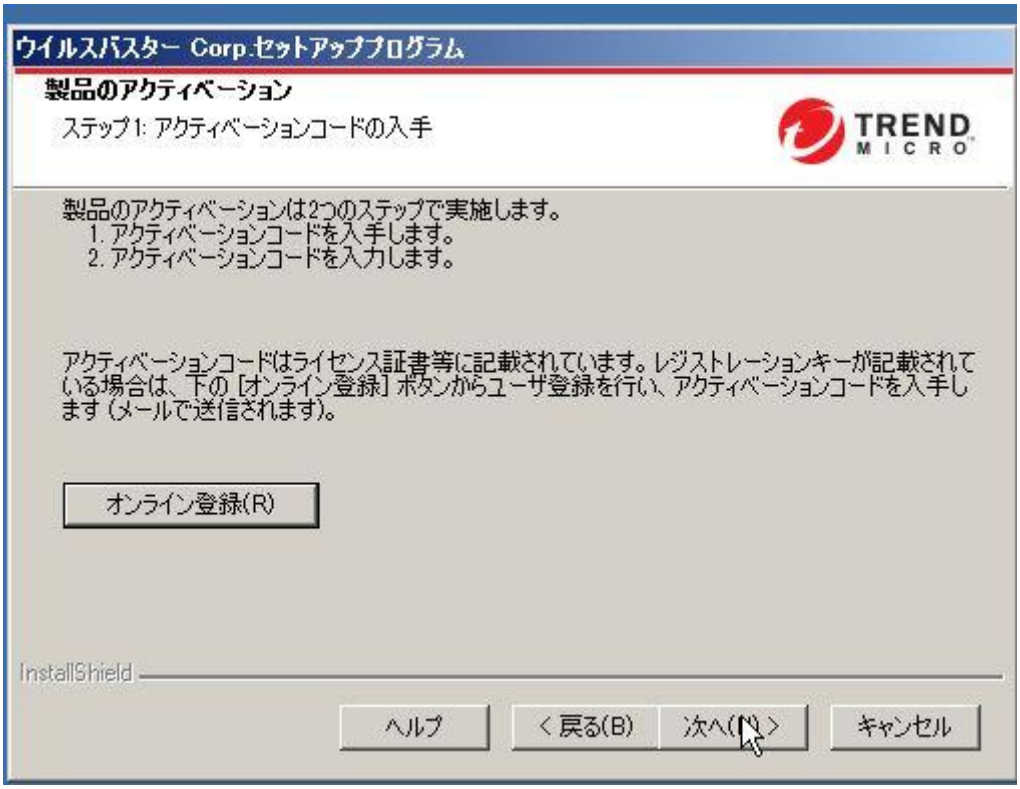
3.4.9. サーバの識別名として、Cluster の FQDN または IP アドレスを指定し、「次へ」を選択します。



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。

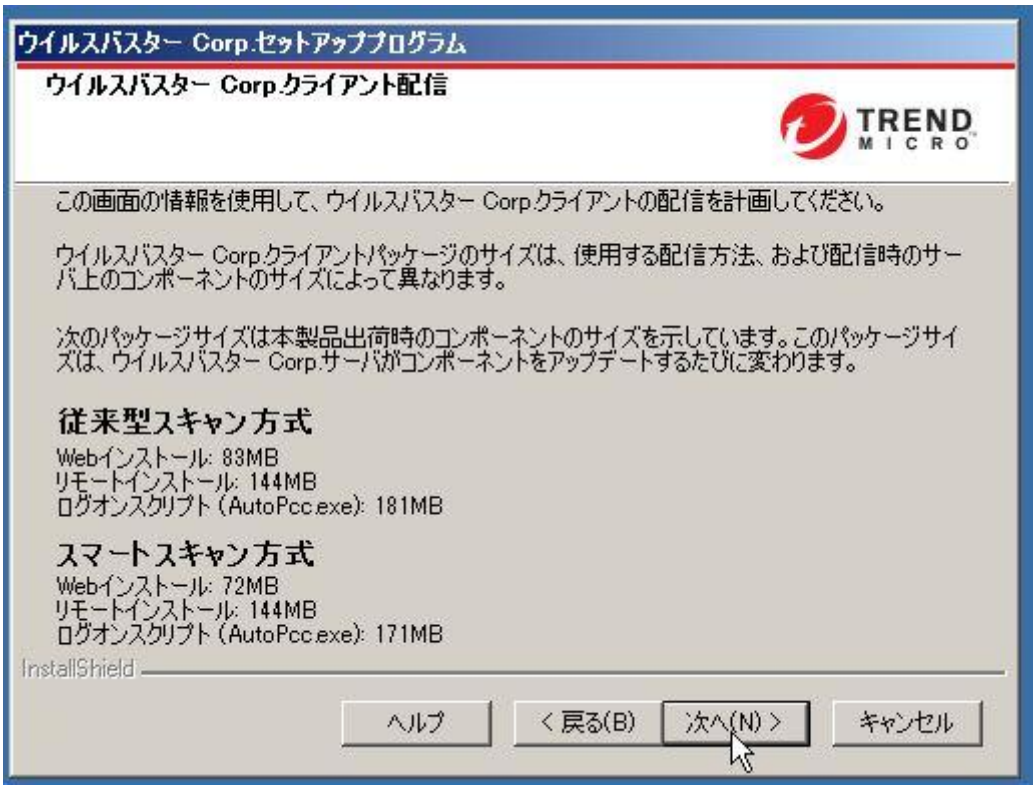


3.4.10. 製品のアクティベーションコードを入力します。「次へ」を選択します。

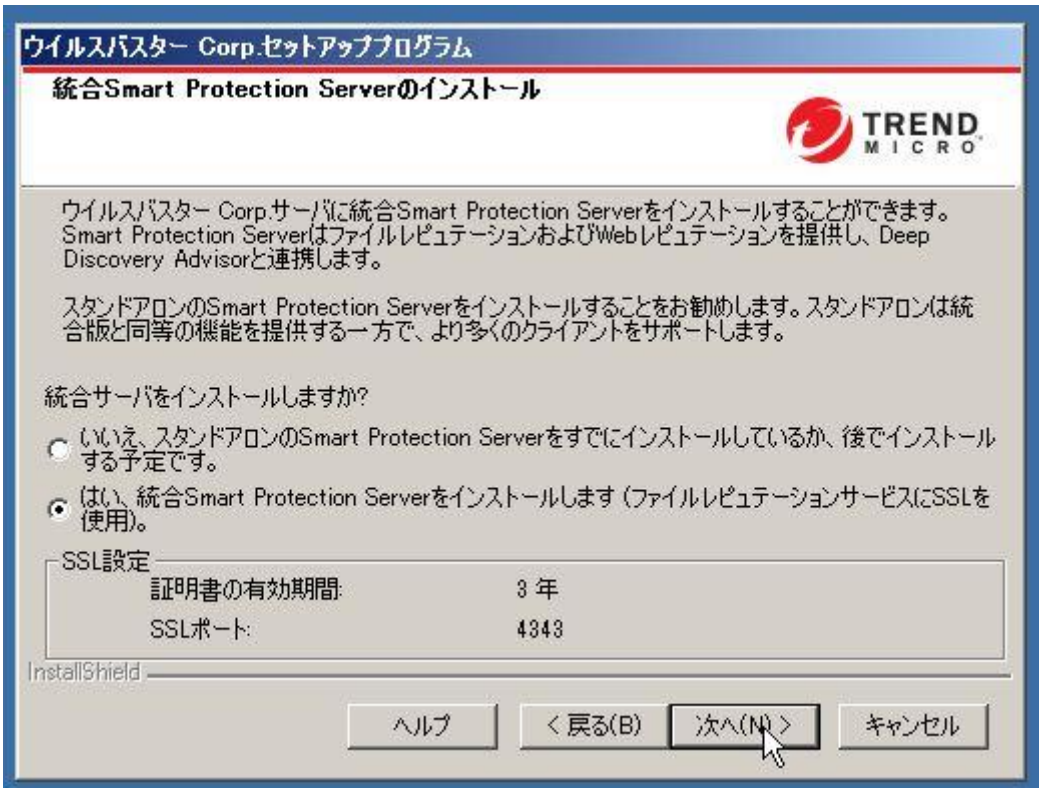


事前に準備済みのアクティベーションコードを入力し、「次へ」を選択します。

3.4.11. クライアントの方式を選択し、「次へ」を選択します。



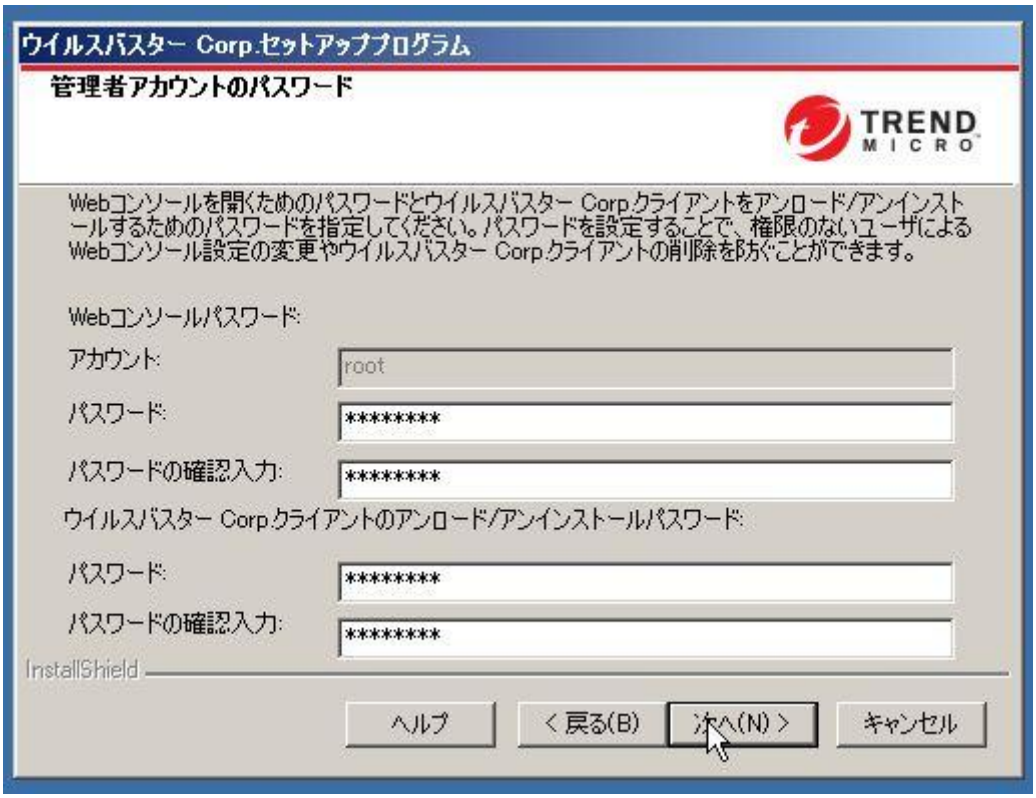
3.4.12. 統合 Smart Protection Server のインストールの有無を選択し、「次へ」を選択します。



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。

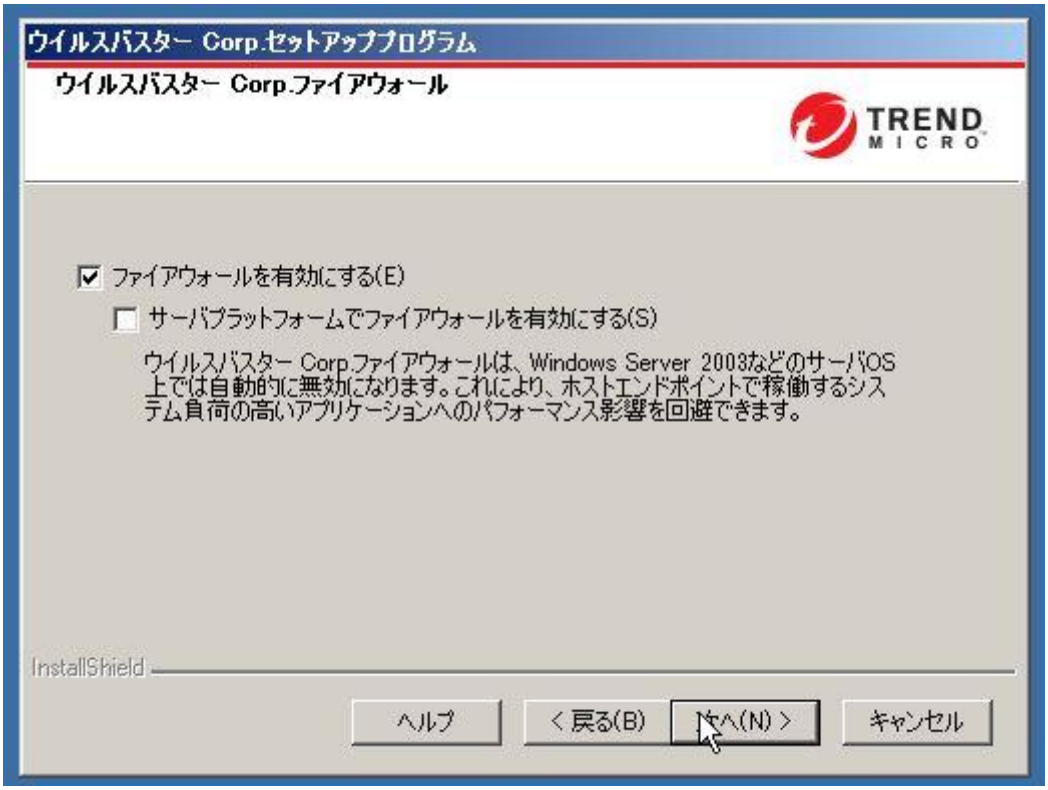
3.4.14. スマートフィードバックを有効にするかを選択し、「次へ」を選択します。

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。



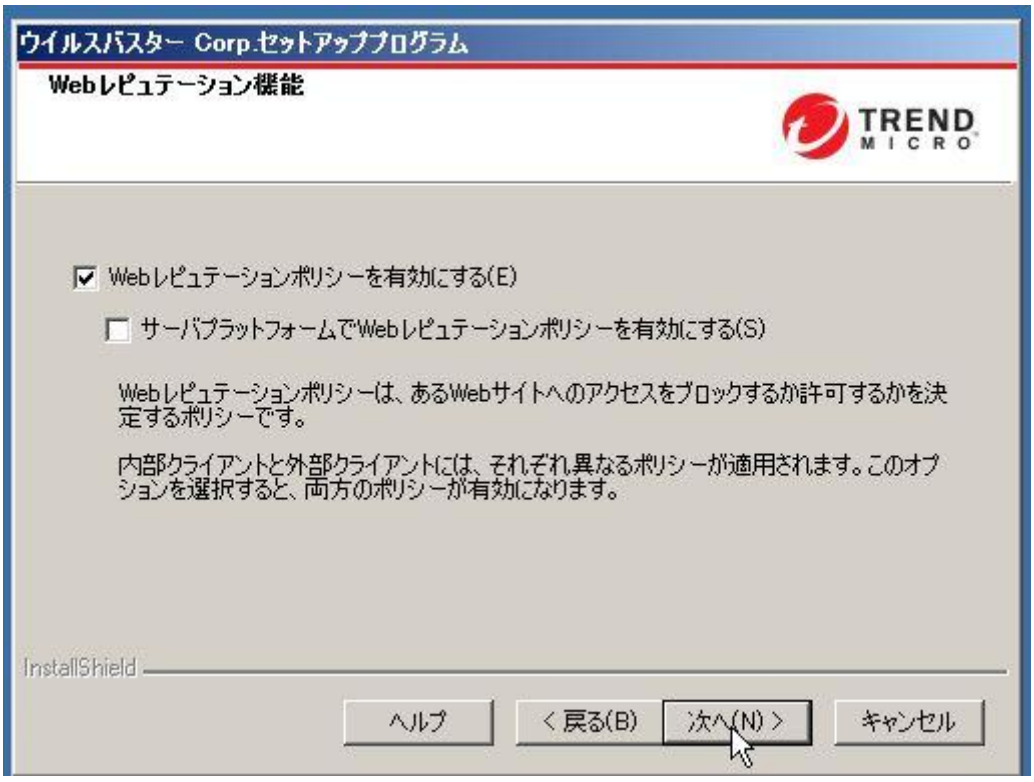
3.4.16. ウイルスバスターCorp.クライアントのインストールパス、接続ポートを設定し、「次へ」を選択します。

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。

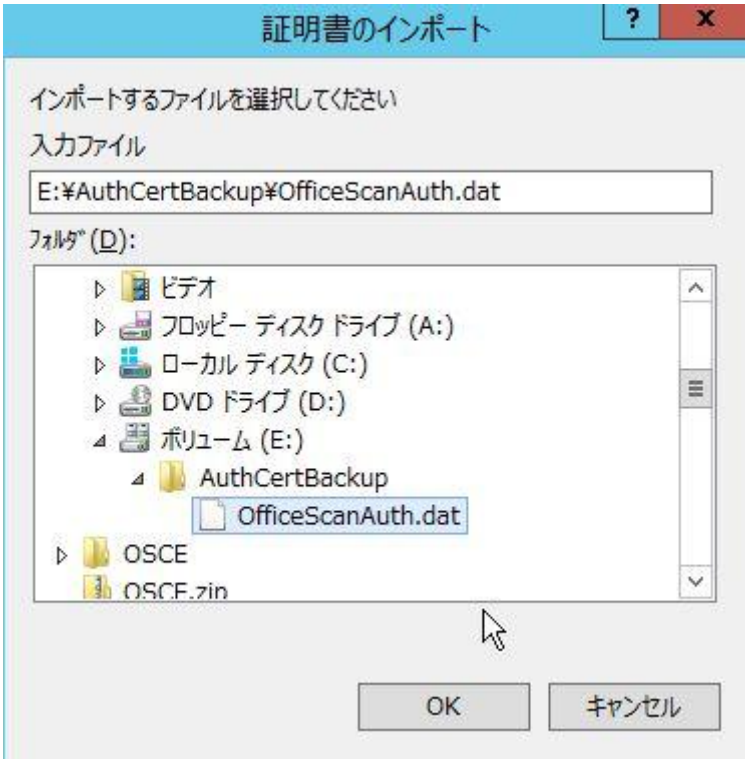
3.4.19. Web レピュテーションを有効にするかを選択し、「次へ」を選択します。



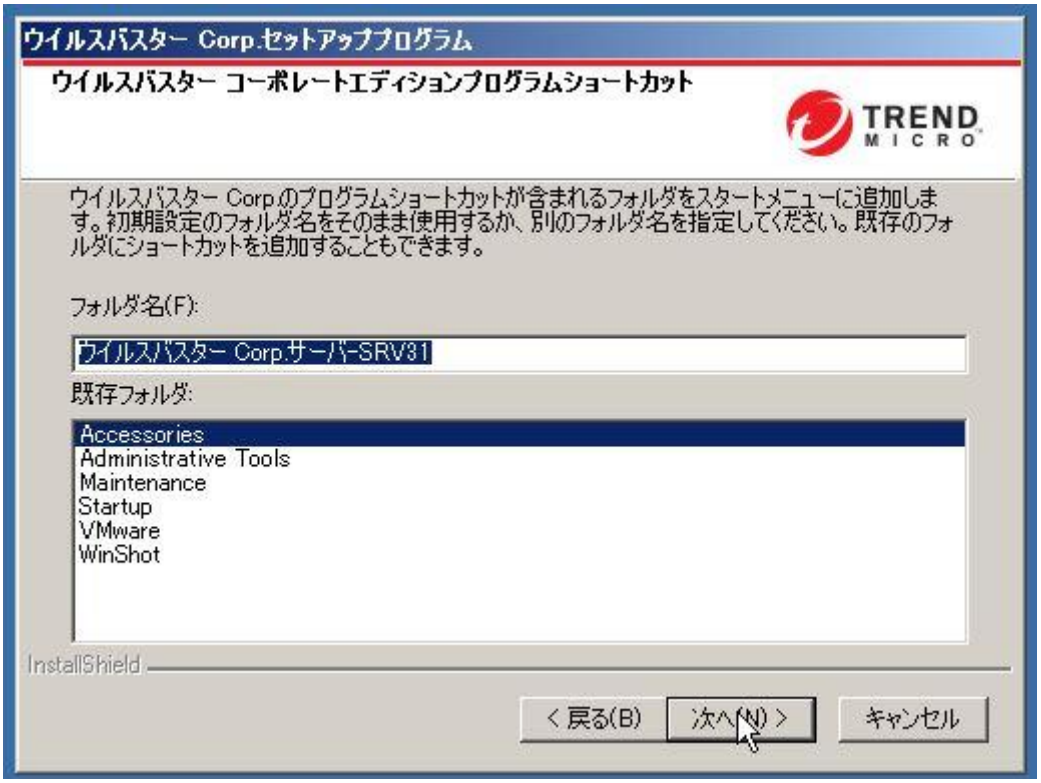
3.4.20. サーバ証明書を設定し、「次へ」を選択します。

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確認します。

「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。

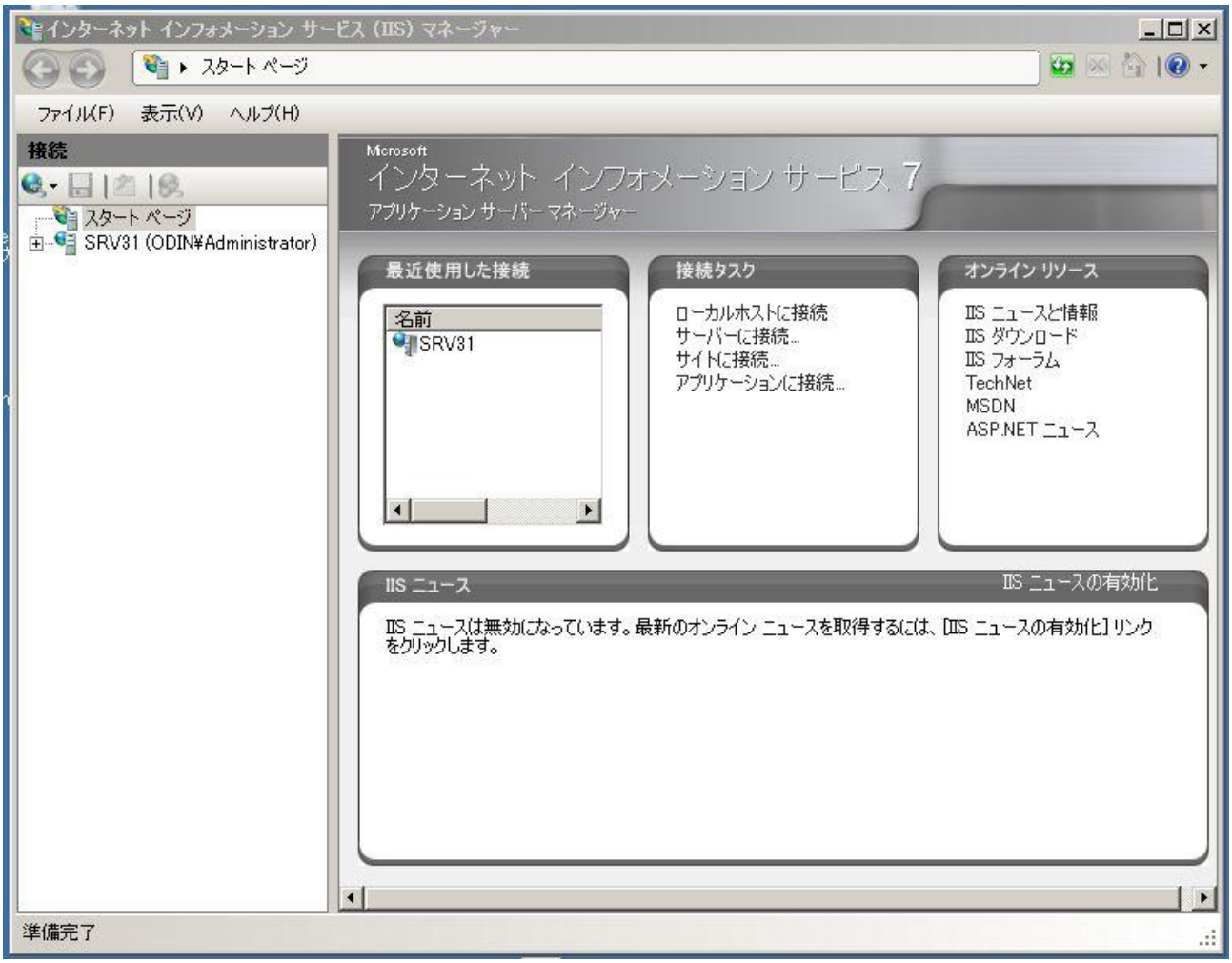
3.5. IIS の認証設定

IIS の管理コンソールを起動し、認証設定を変更します。

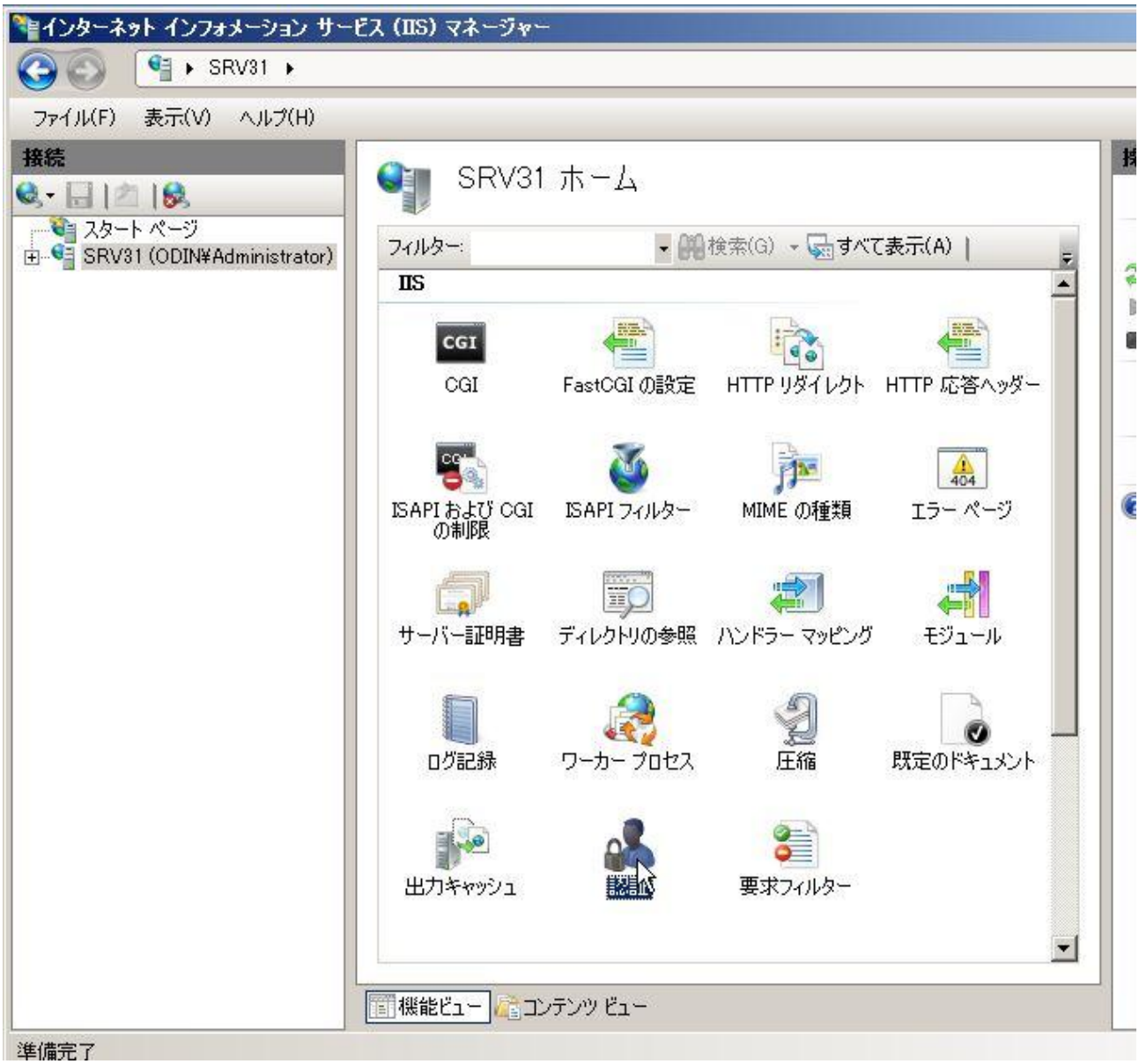
この操作は Node A、Node B でそれぞれ実施します。

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。

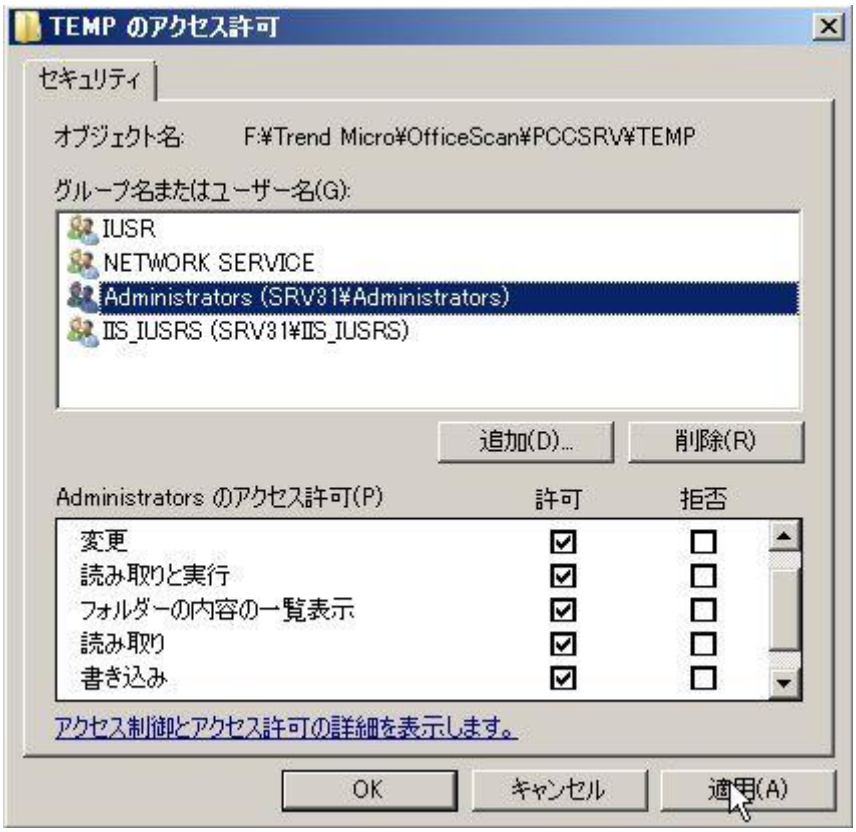
3.5.6. ドメインユーザ情報が設定されたことを確認し、「OK」を選択します。

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限を確認します。

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）

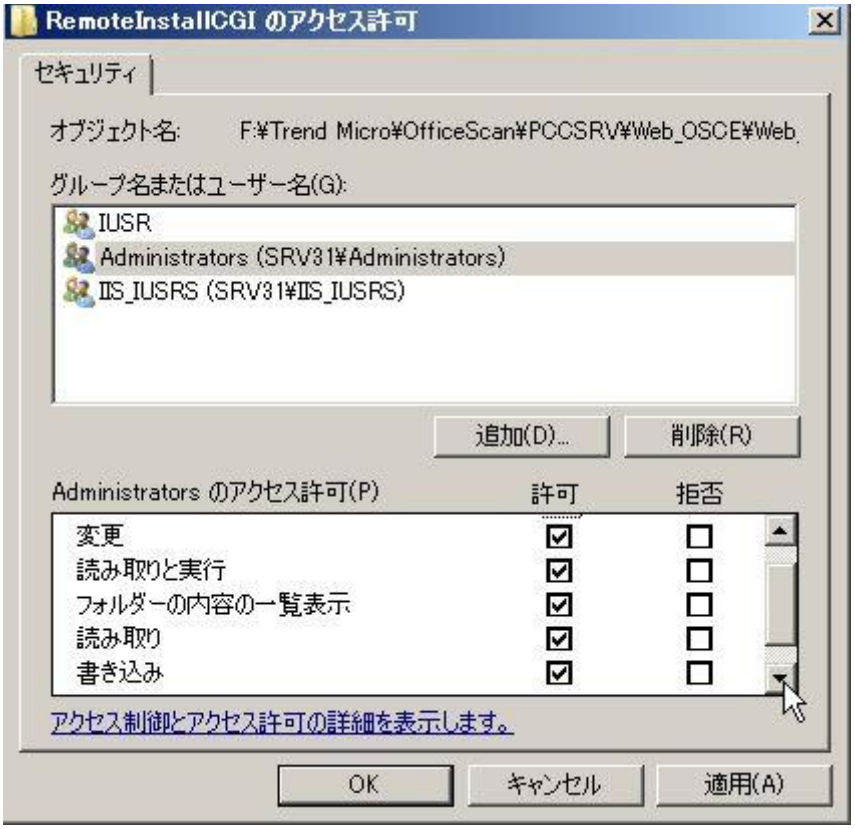


3.6.3. PCCSRV¥Web（読み取り）

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）

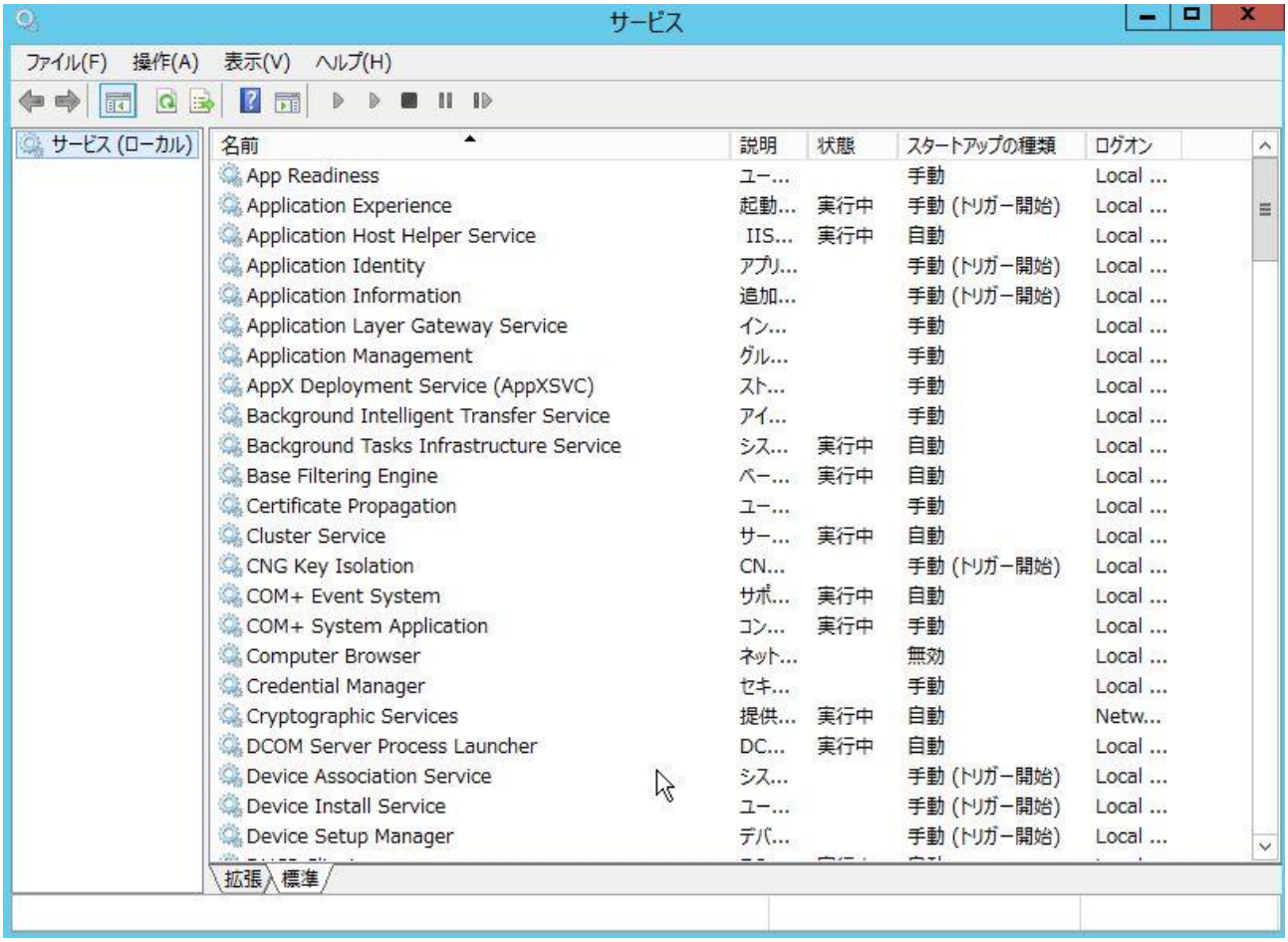


3.7. ウイルスバスターCorp. サービススタートアップ設定

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。

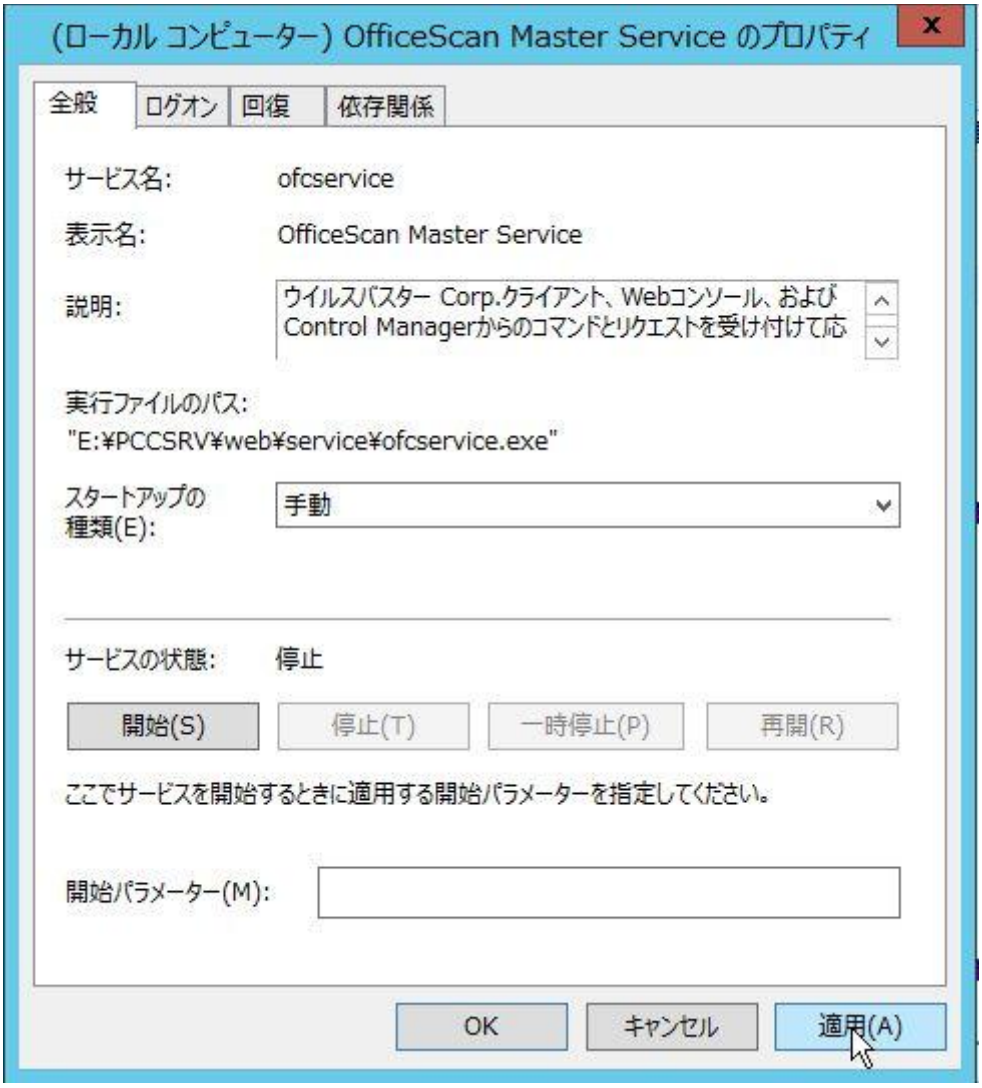
この操作は Node A、Node B でそれぞれ実施します。

3.7.1. サービスを起動します。

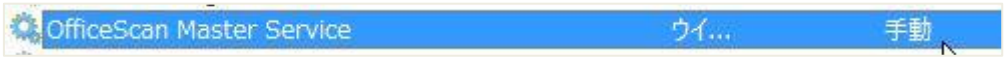


3.7.2. OfficeScan Master Service を選択します

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。

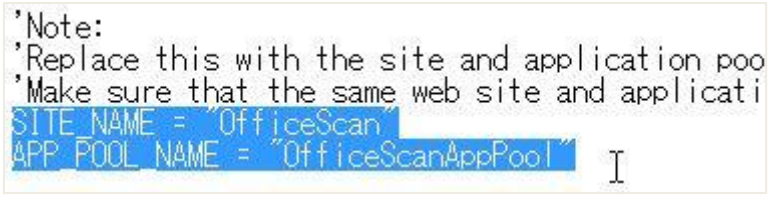
本操作は Node A、Node B のそれぞれで実施します。

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。

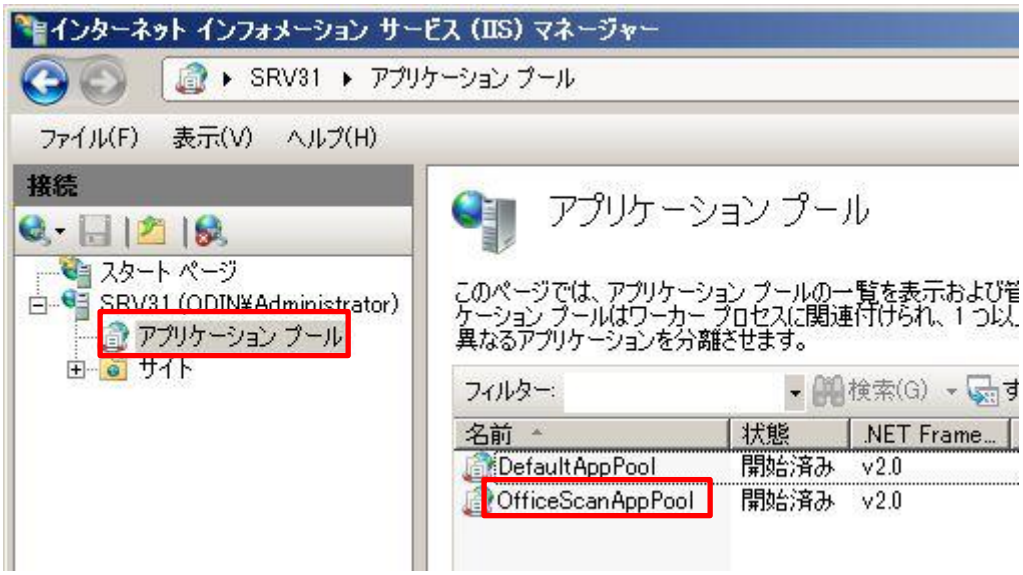
3.8.2. SITE_NAME、APP_POOL_NAME の確認

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。



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。

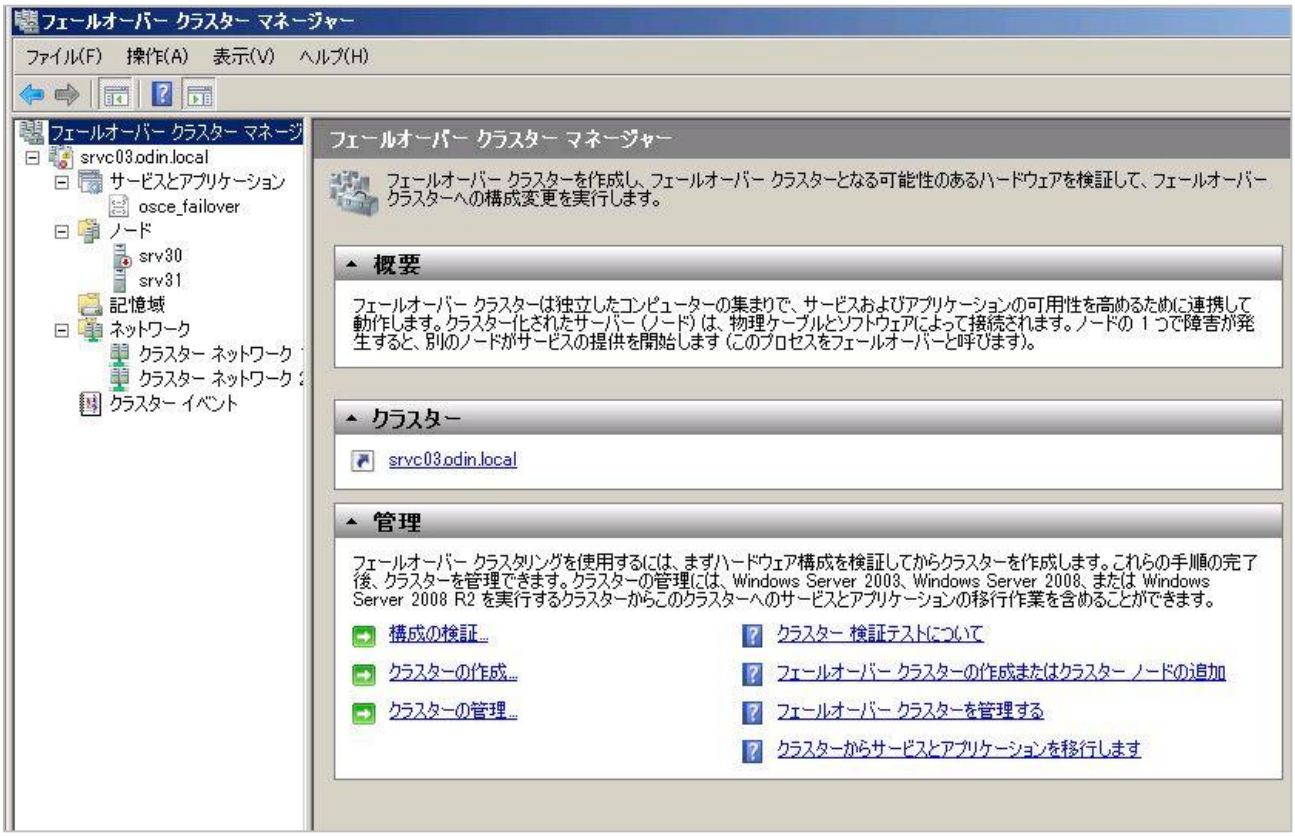


3.8.4. Generic Script を System32¥inetsrv に保存します。

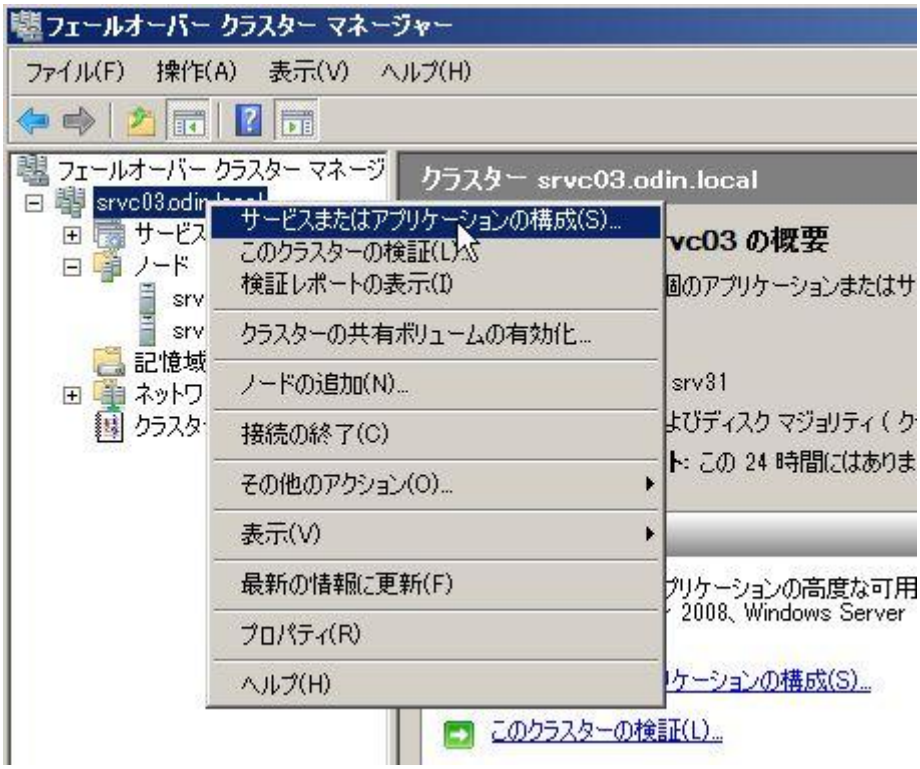
3.9. High availability Cluster Generic Script の作成

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。

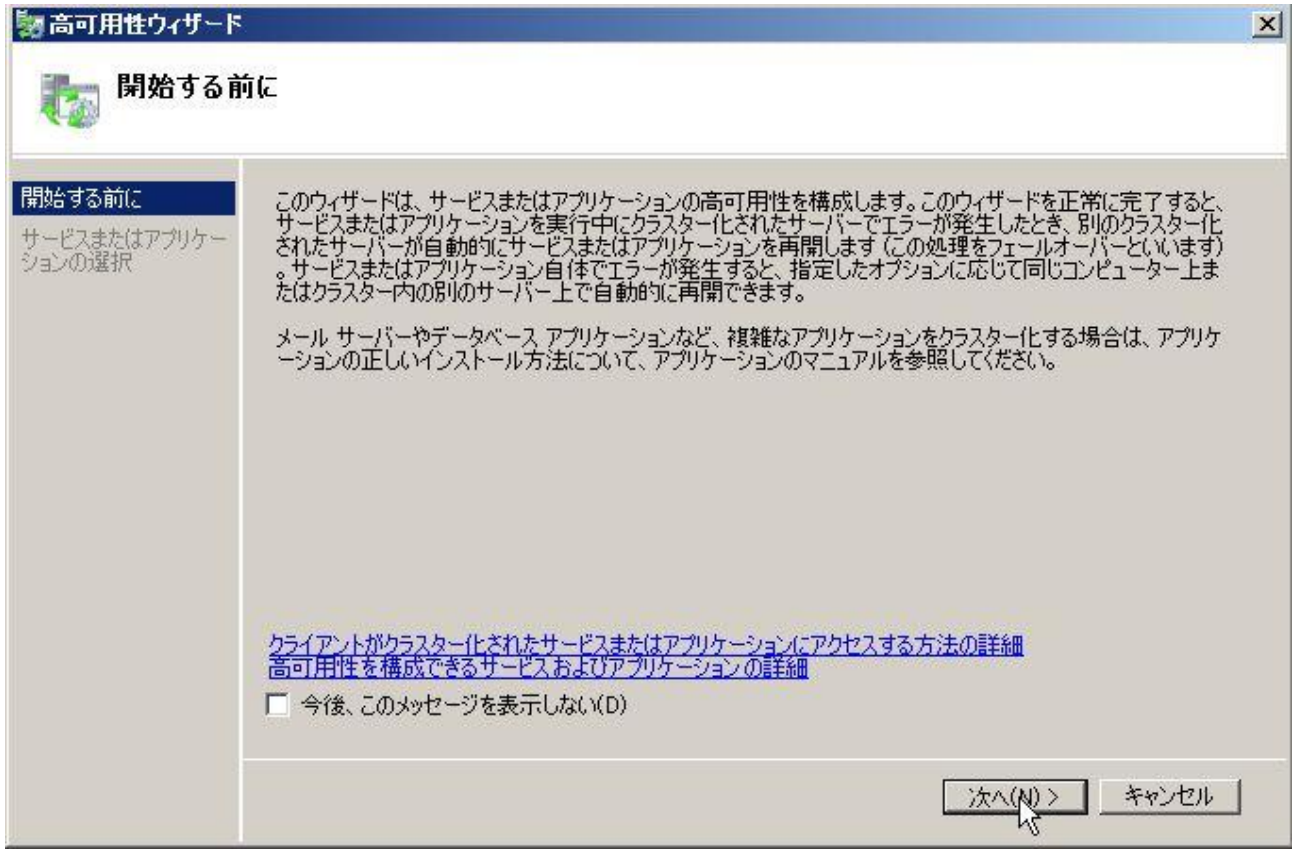
3.9.1. Failover Cluster Manager を起動します。



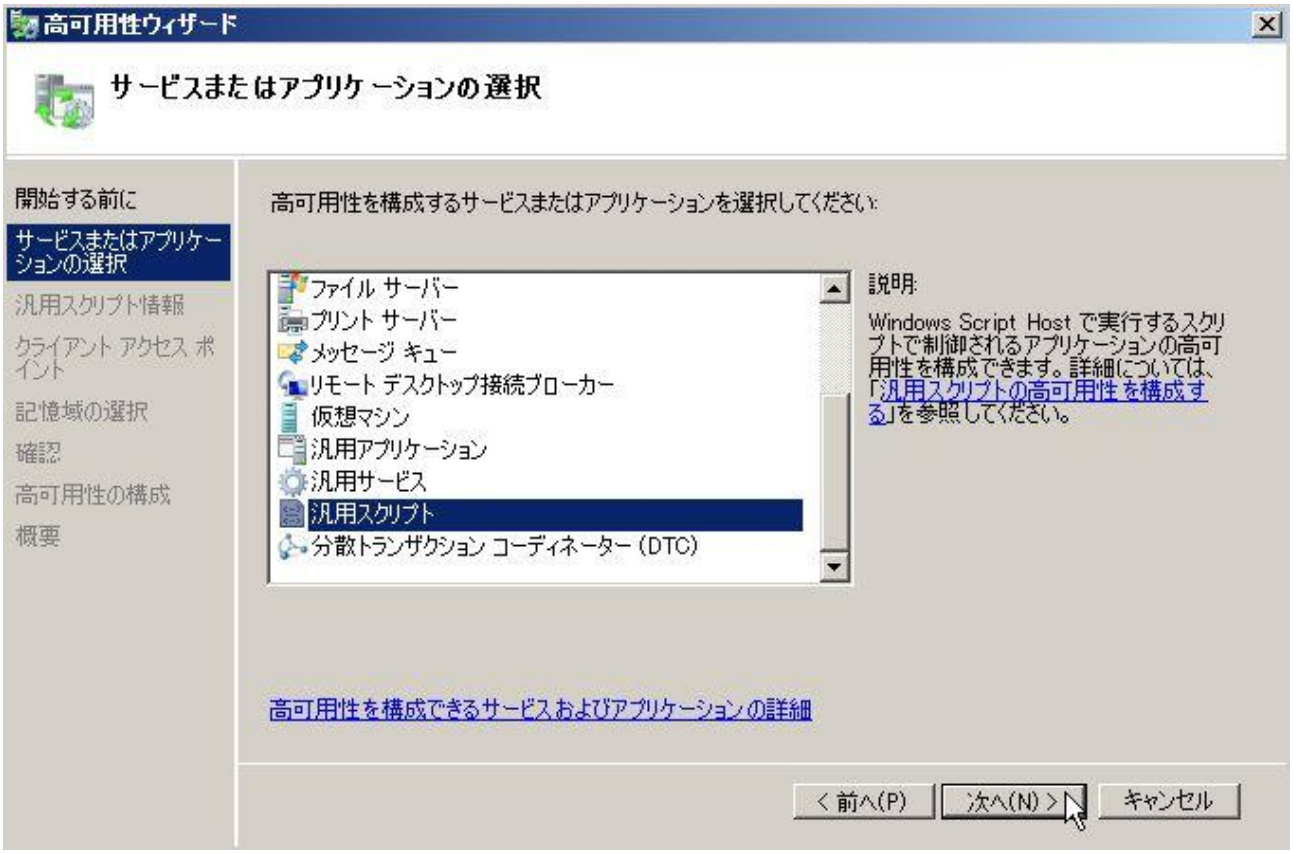
3.9.2. Cluster を選択し、右クリック＞サービスまたはアプリケーションの構成を選択します。



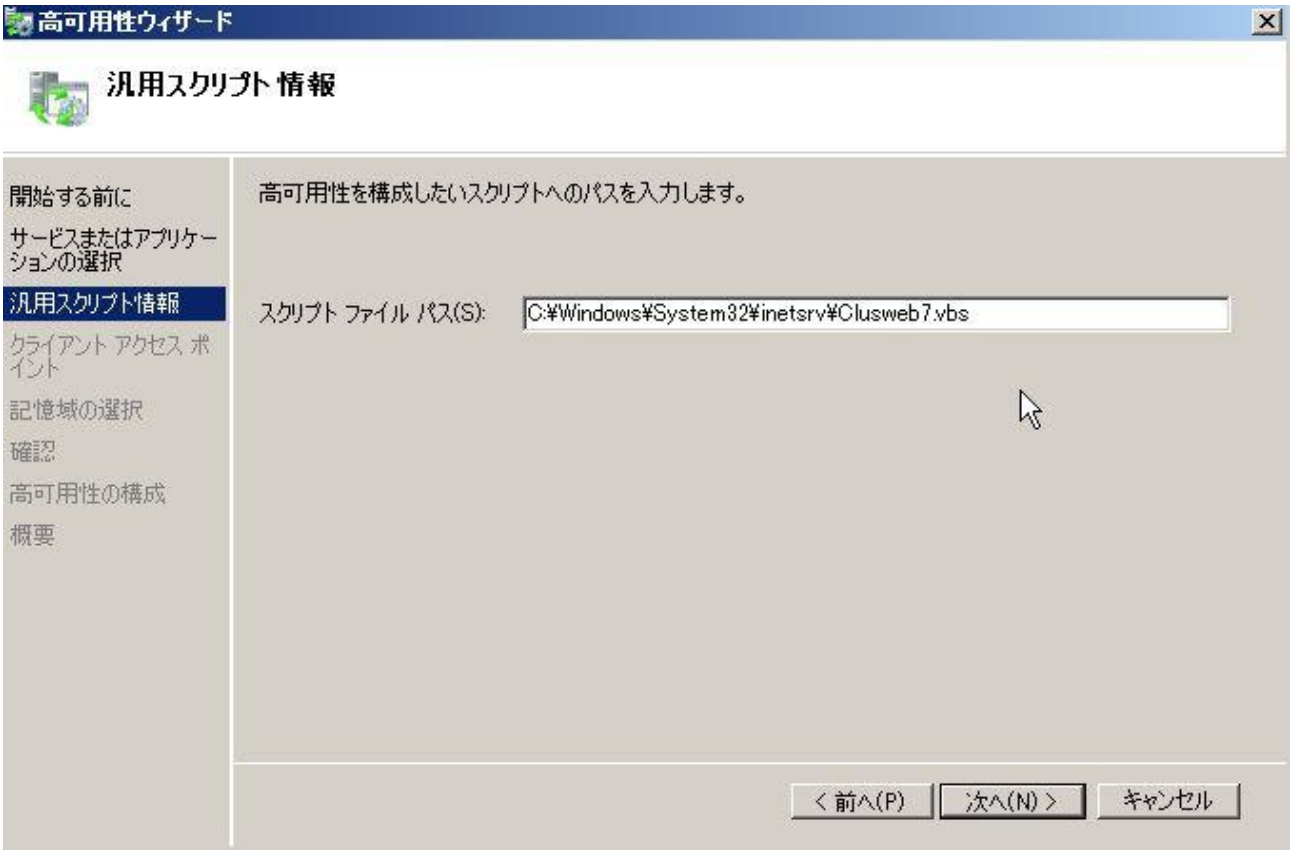
3.9.3. 高可用性ウィザードに従って設定を進めます。 「次へ」を選択します



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。

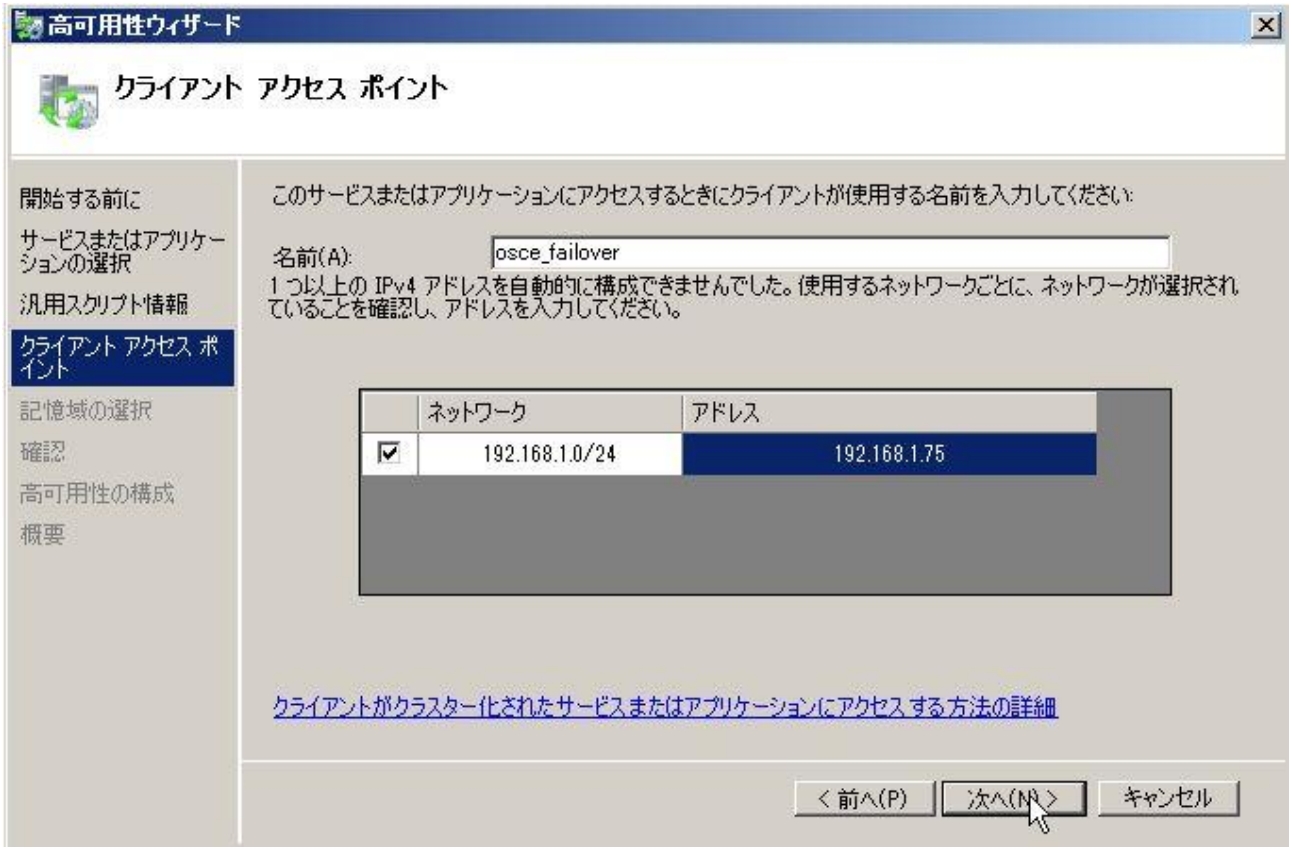


3.9.5. 汎用スクリプトの場所を指定します。



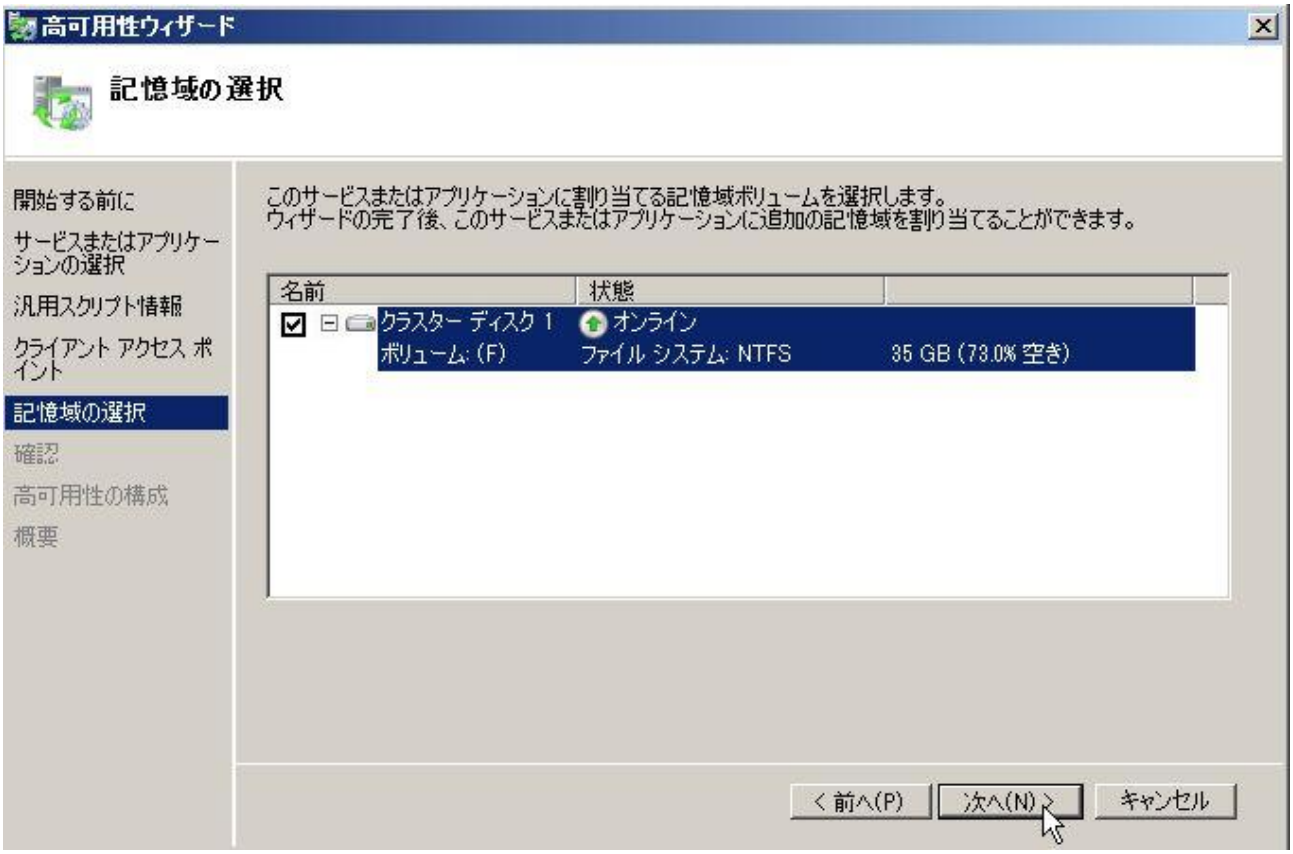
スクリプトファイルパスは 3.8 Cluster Generic Script の準備で保存したファイルパスを指定します。

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。

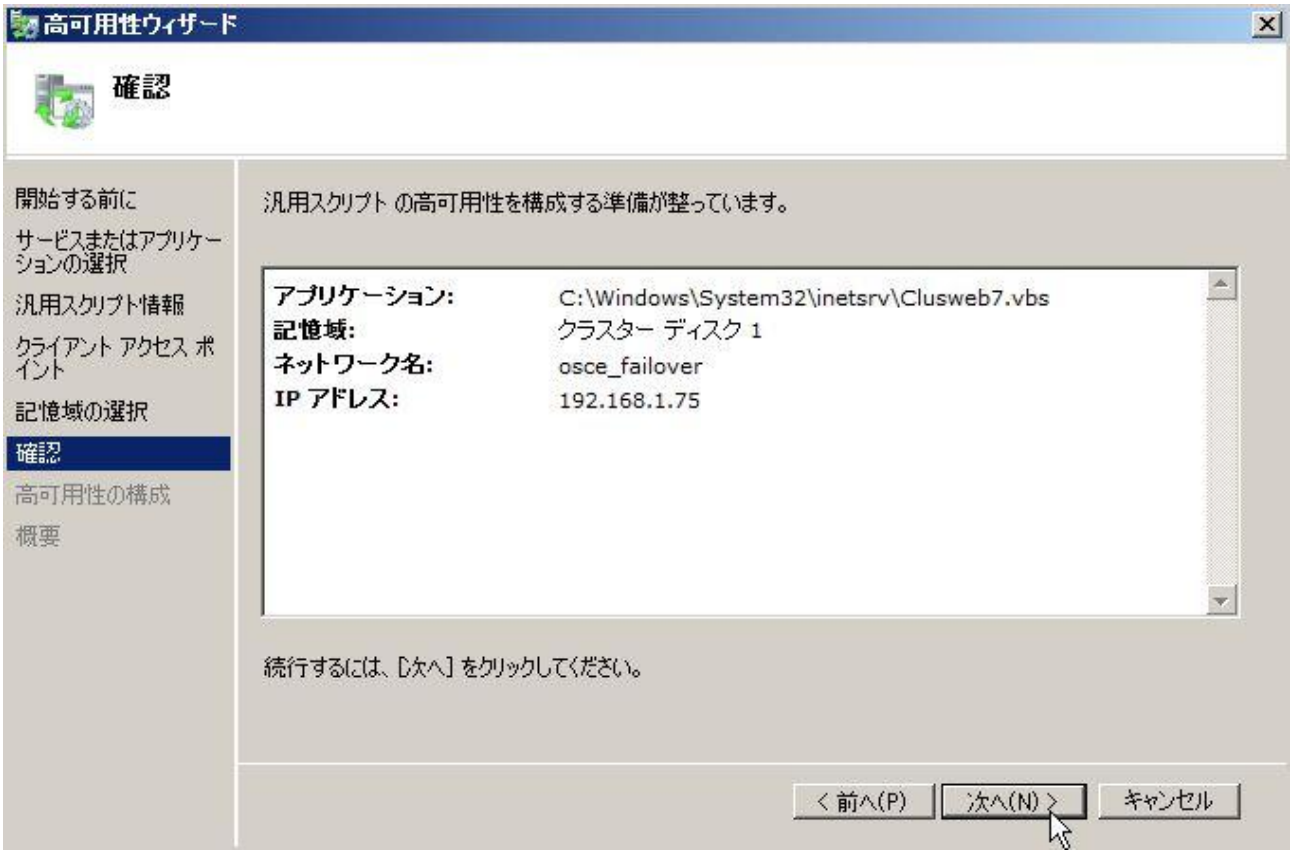


ウイルスバスターCorp. クライアントを Autopcc.exe でインストールする際など、このアドレス宛の共有フォルダにアクセスします。

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。

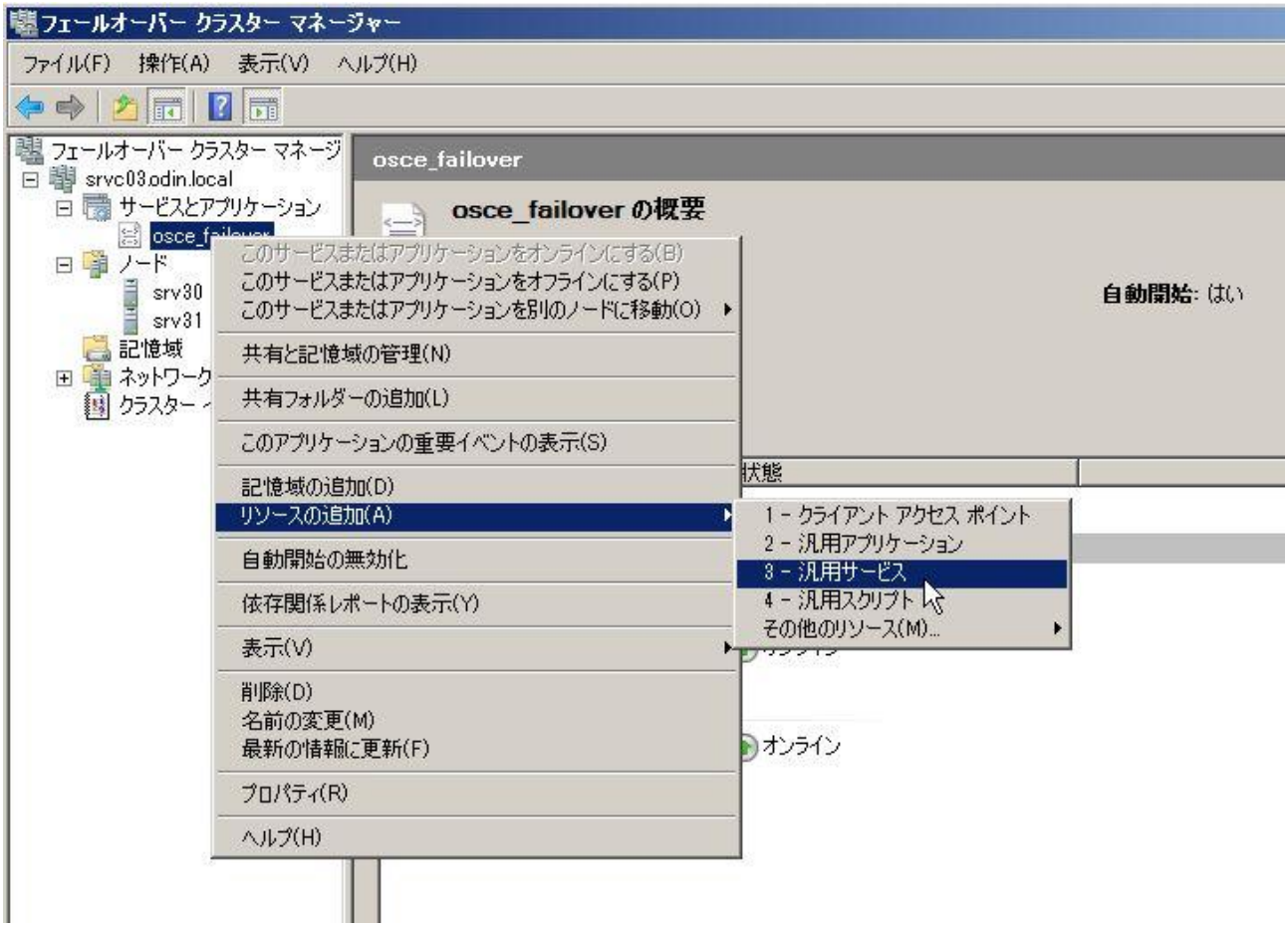


3.9.9. 役割が正しく構成されることを確認し、「完了」を選択します。

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。

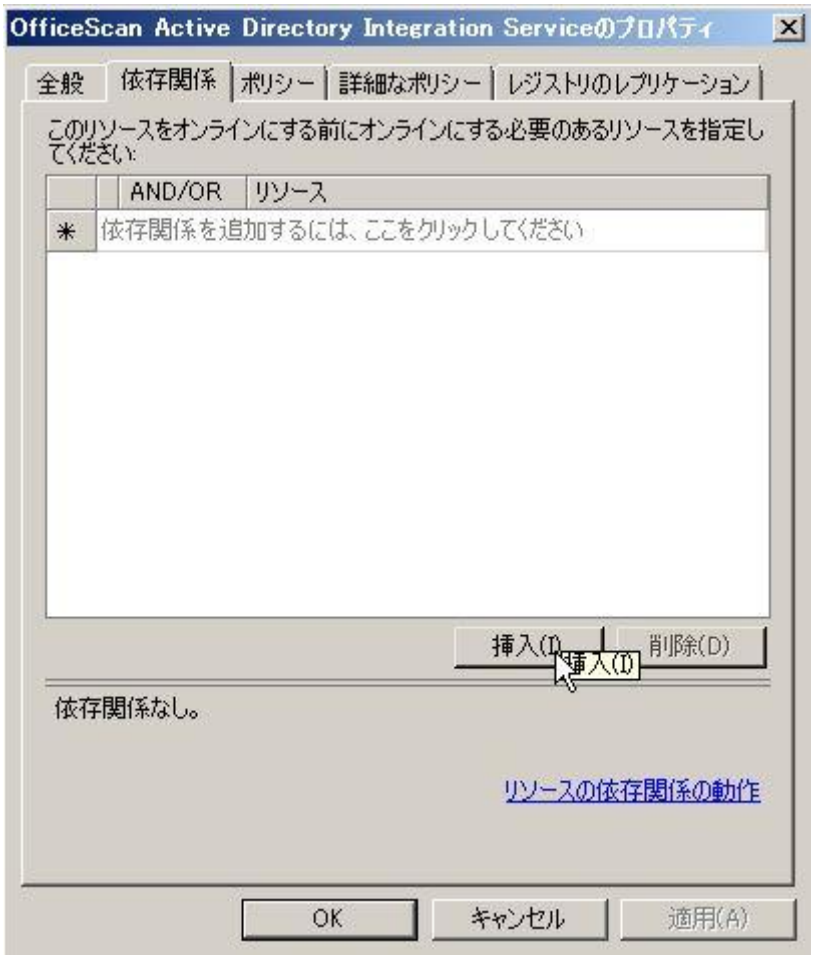
Trend Micro Local Web Classification Server サービスと Trend Micro Smart Scan Server サービスは登録の必要はありません。これらのサービスは OfficeScan Master Service の起動時に自動的に起動します。

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。

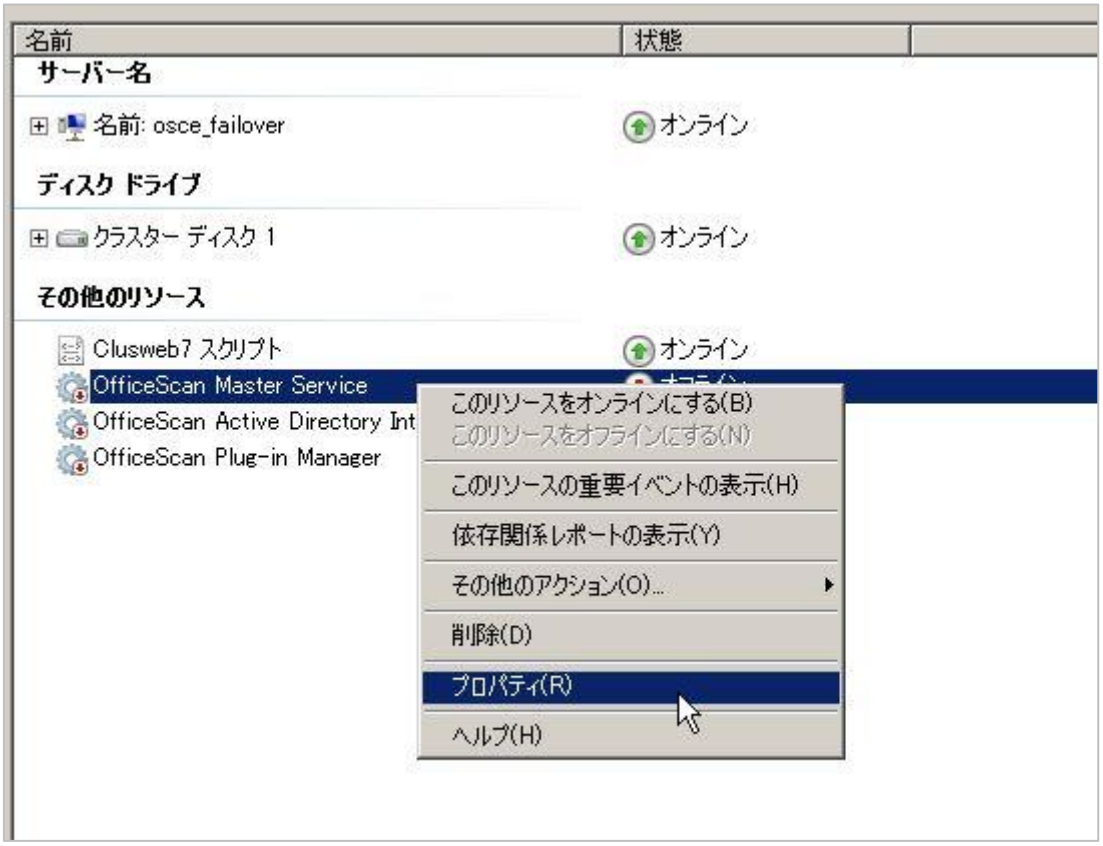
3.11.2. 依存関係のタブを表示します。



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。

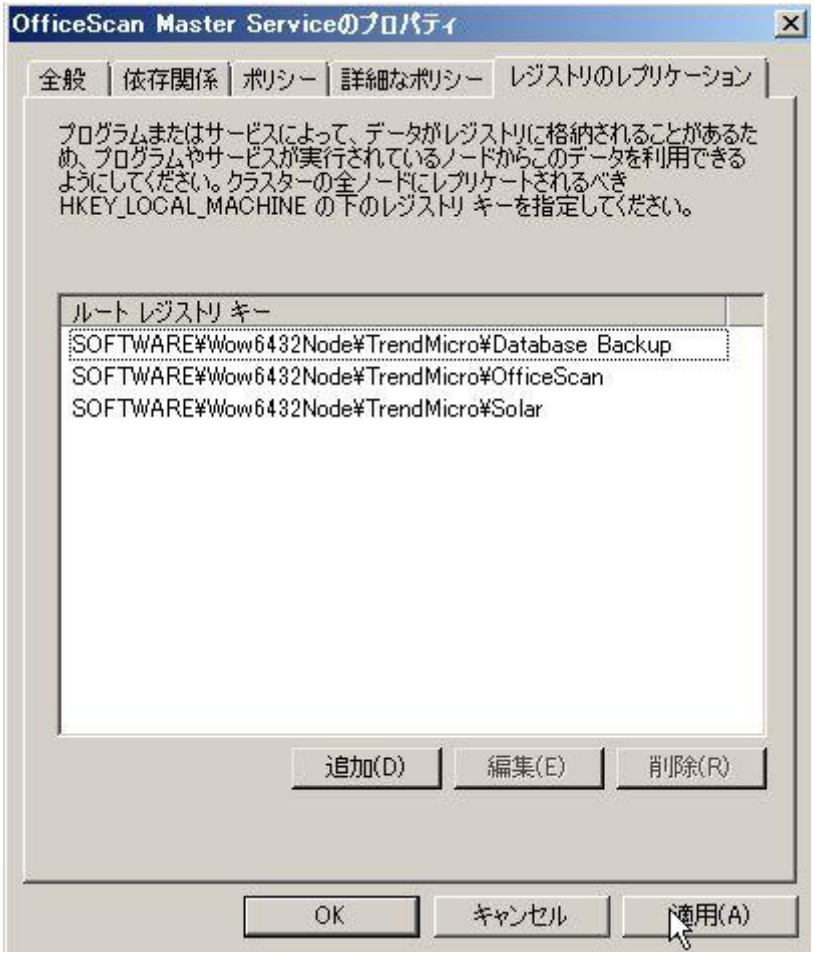
3.11.8. 共有ディスクを選択し、「挿入」を選択します。

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 Mangaer 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。

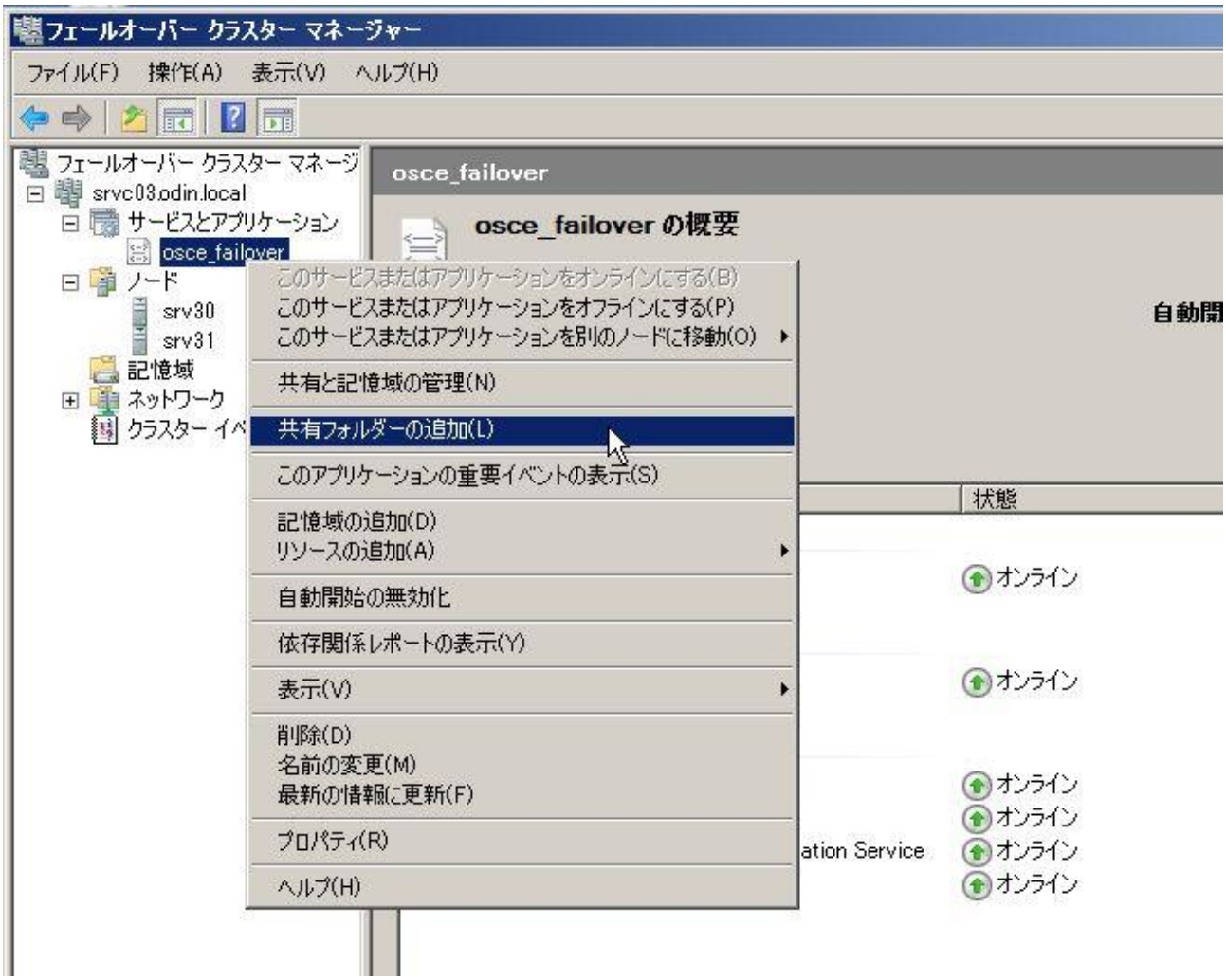
3.13.3. 全てのサービスがオンラインとなることを確認します。

※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。

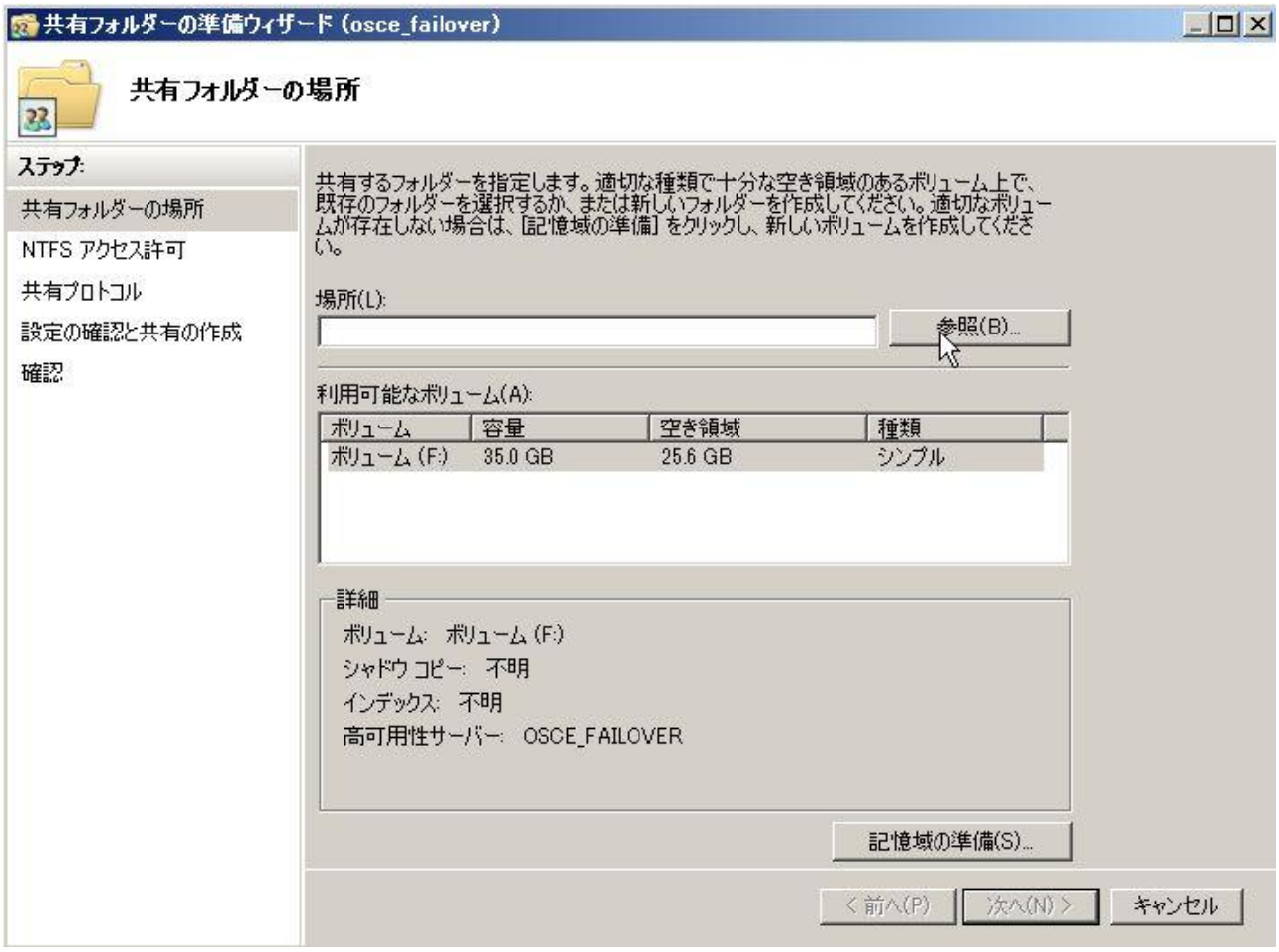
3.14. 共有フォルダの設定

ウイルスバスターCorp.の共有フォルダを設定します。

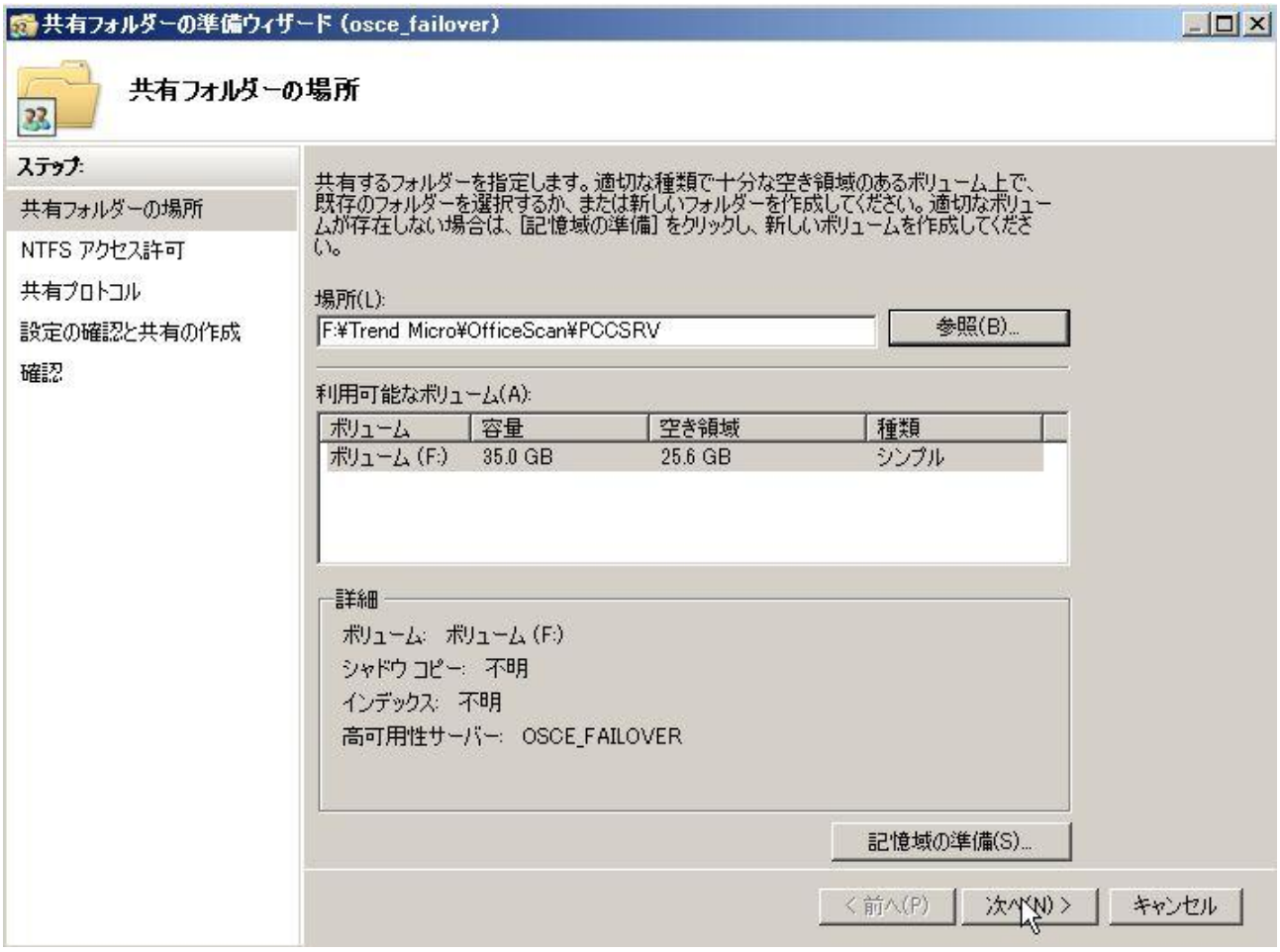
3.14.1. Failover Cluster Manager を起動し、サービスを選択し、右クリック＞共有フォルダーの追加を選択します。



3.14.2. 共有フォルダーの場所の参照を選択します。

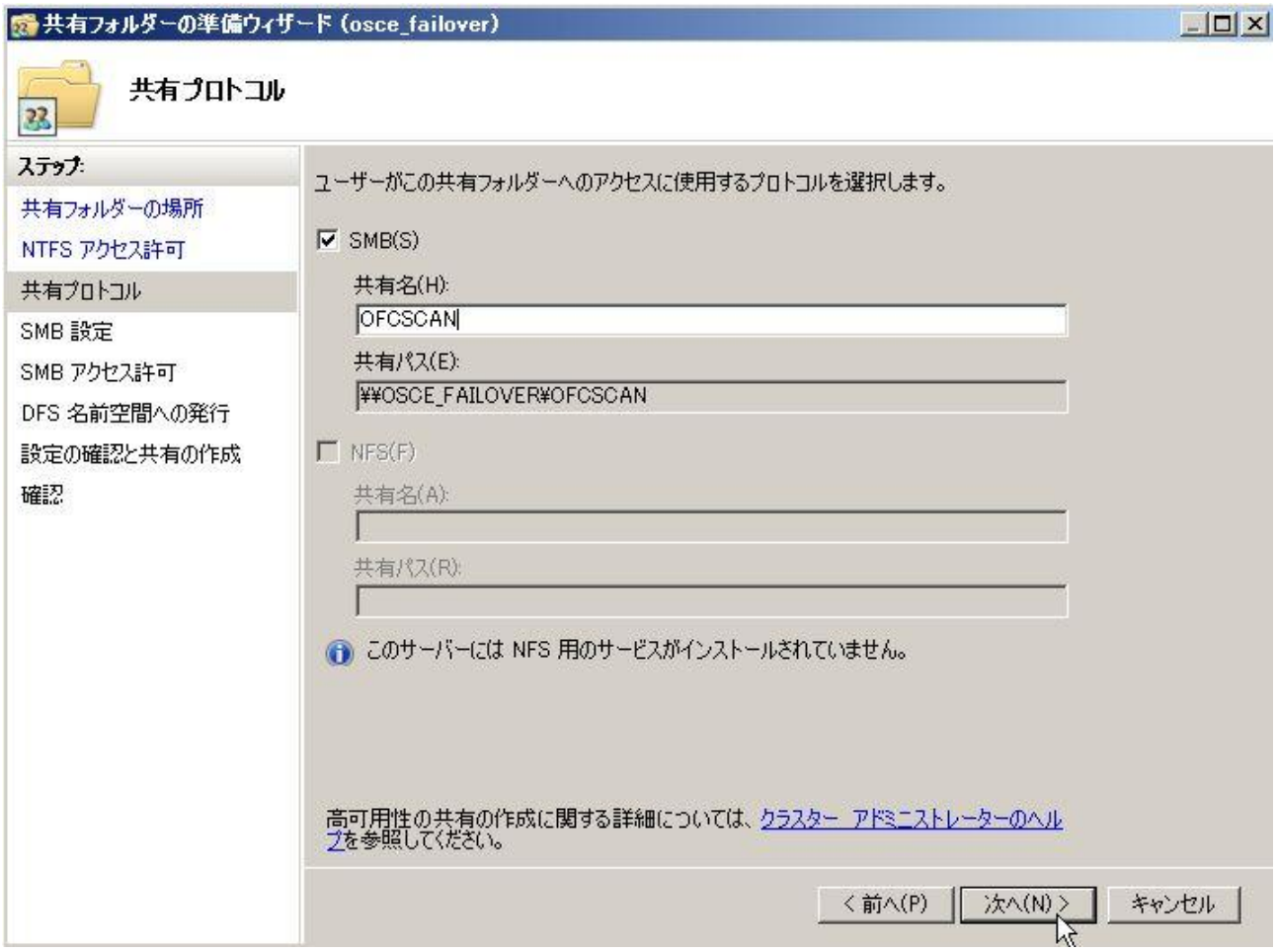


3.14.3. PCCSRV フォルダを選択し、次へを選択します。



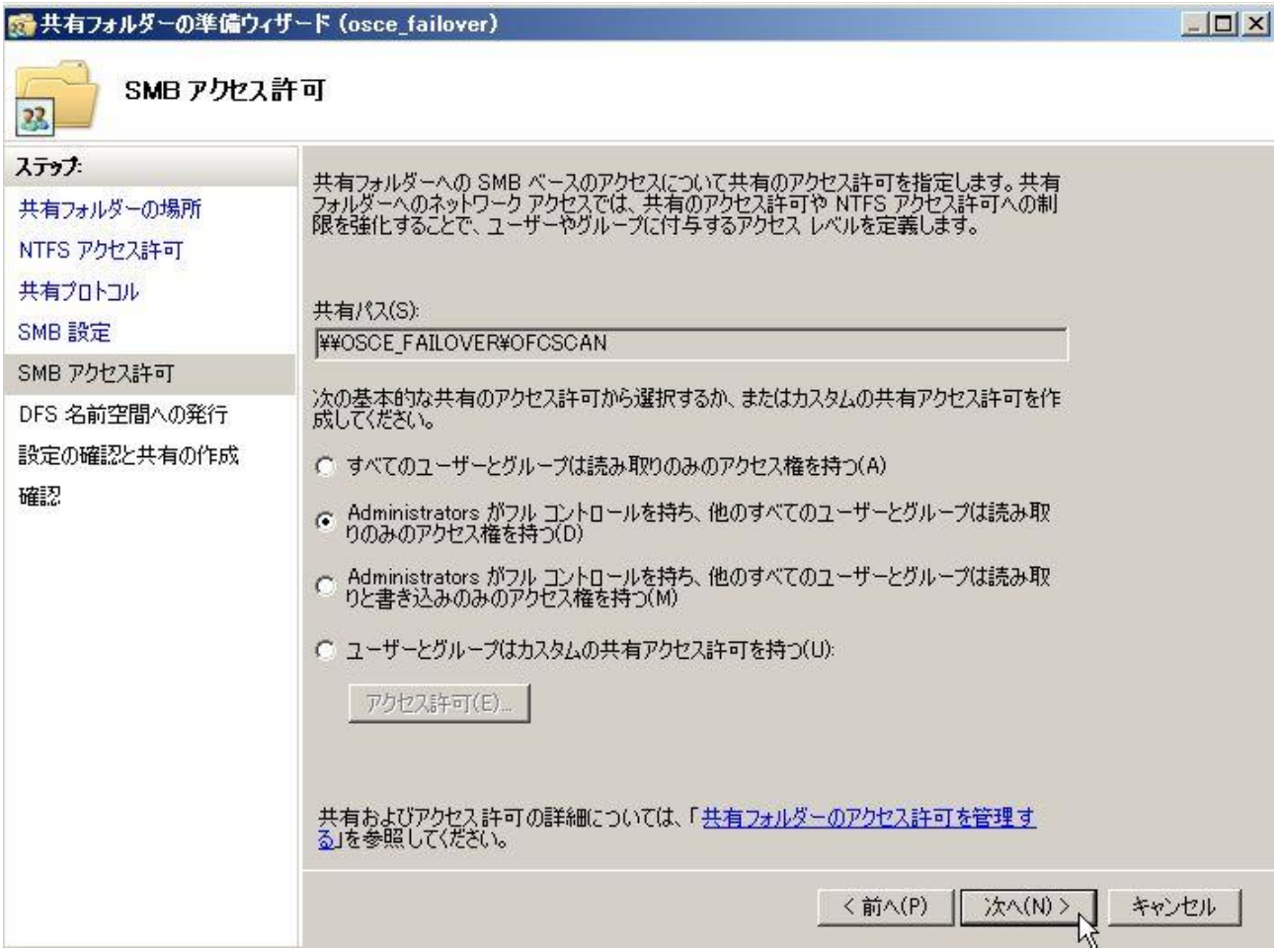
3.14.4. NTFS アクセス許可の設定画面では設定を変更せずに、次へを選択します。

3.14.5. 共有名に OFCSCAN を指定し、次へを選択します。



3.14.6. 次へを選択します。

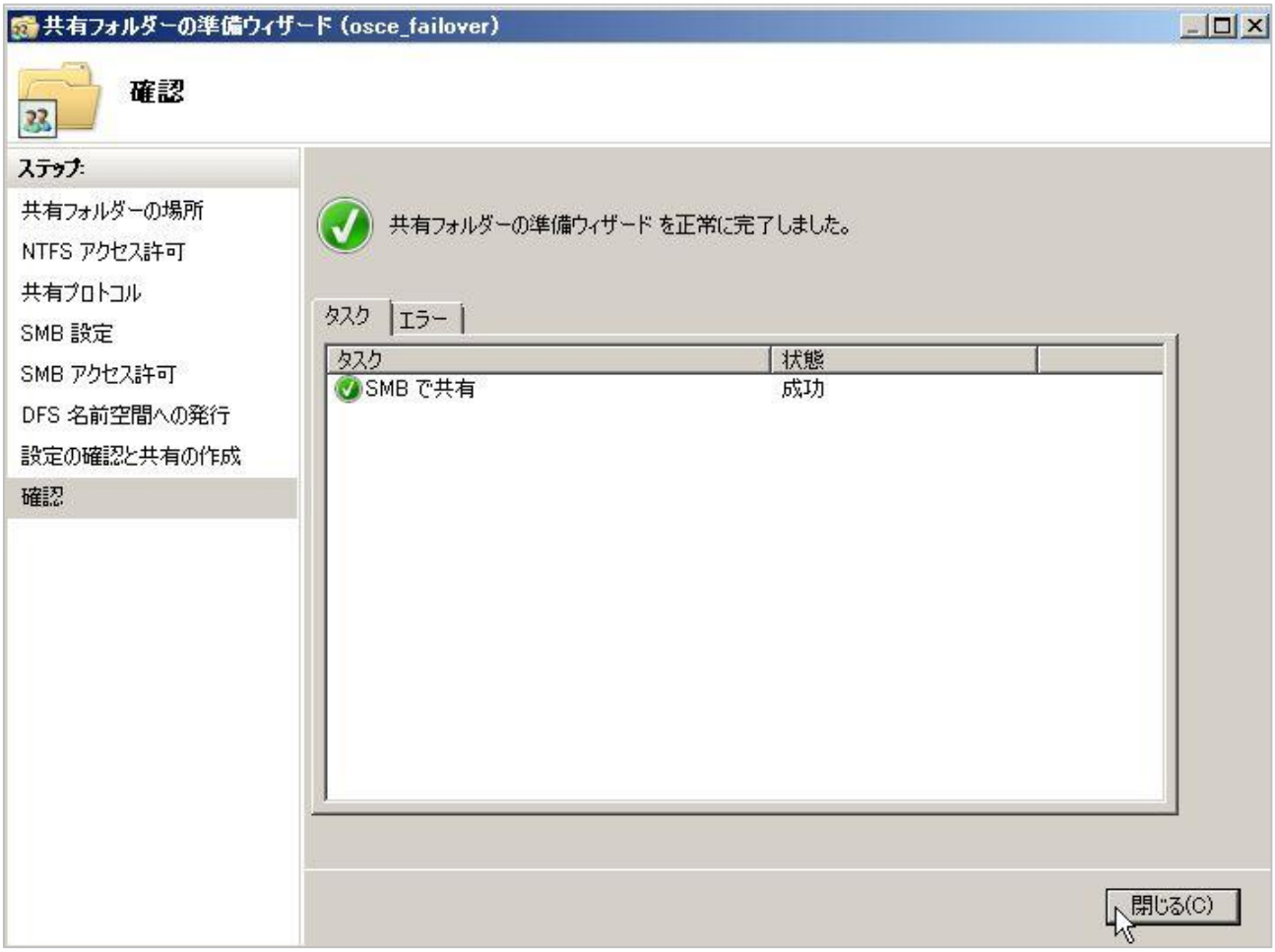
3.14.7. SMB アクセス許可で Administrators がフルコントロールを持ち、他のすべてのユーザとグループは読み取りのアクセス権を持つ　にチェックを要れ、次へを選択します。



3.14.8. 次へを選択します。

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。

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。