

# ActiveImage Protector 2022 Server

## セットアップガイド

第6版 2024年2月



# 目次

---

1. はじめに .....	3
システム要件.....	3
2. インストール .....	4
3. アクティベーション .....	6
4. バックアップの設定と実行.....	7
4-1. ポリウム バックアップ：ワンタイム.....	7
4-2. ポリウム バックアップ：スケジュール .....	13
4-3. ファイル バックアップ：スケジュール.....	25
4-4. エージェントレス バックアップ (HyperBack) .....	33
5. 起動環境ビルダー .....	47
Windows RE ベースの起動環境の作成 .....	47
6. リストア .....	52
6-1. ファイル/フォルダー単位のリストア.....	52
6-2. システムリカバリー：標準の Linux ベースの起動環境.....	57
6-3. システムリカバリー：Windows RE ベースの起動環境.....	64
6-4. バックアップから新規仮想マシンを作成 (HyperRecovery) .....	70
6-5. ゼロ タイム リカバリー (HyperRecovery LIVE!) .....	75
6-6. クラウドリカバリー (In-Cloud Recovery) .....	80
7. イメージ管理：イメージ管理.....	88
7-1. バックアップの起動確認 (BootCheck) .....	89
7-2. クイック ベリファイ.....	91
7-3. 結合.....	93
7-4. バックアップのアーカイブ作成.....	95
7-5. バックアップファイルの同一性確認 (MD5 の計算) .....	97
7-6. バックアップファイルの削除.....	99
8. イメージ管理：イメージのマウント .....	100
9. イメージ管理：イメージ ターゲット サーバー.....	102
10. リモート管理コンソール.....	110
11. 仮想スタンバイ (待機) マシンの作成.....	113
11-1. vStandby.....	113
11-2. HyperStandby.....	120
11-3. HyperBoot.....	129
12. 参考情報.....	138

## 1. はじめに

ActiveImage Protector は、物理・仮想・クラウドといった多様なシステム環境に対応したシステム・データ保護ソリューションです。このセットアップガイドでは、「ActiveImage Protector 2022 Server (2024 年 2 月アップデート:バージョン 7.0.3.8919)」の導入から基本的な設定方法などを説明しています。是非、ご一読頂き、正しく運用を行うための知識としてご活用ください。なお、詳細な設定方法や制限事項などについては、オンラインヘルプ ([https://webhelp.actiphly.com/AIP/2022/ja\\_JP/](https://webhelp.actiphly.com/AIP/2022/ja_JP/)) を参照してください。

### システム要件

ActiveImage Protector 2022 Server (バージョン 7.0.3.8919) のシステム要件は下記のとおりです。

インストール先のコンピューターが、以下のシステム要件を満たしていることをご確認ください。

CPU	Pentium 4 または同等以上の CPU
メモリ (RAM)	4GB 以上 (8GB 以上を推奨)
ハードディスク	1.5GB 以上の空き容量が必要
サポート対象 OS (Server Edition)	Windows: ・ Windows Server 2022 ・ Windows Server 2019 ・ Windows Server 2016 ・ Windows Server 2012 R2 ・ Windows Server IoT 2019 / 2022 for Storage ・ Windows Storage Server 2016 ・ Windows Storage Server 2012 R2 ハイパーバイザー: ・ Windows Server 2022 Hyper-V ・ Windows Server 2019 Hyper-V ・ Windows Server 2016 Hyper-V ・ Windows Server 2012 R2 Hyper-V ・ VMware vSphere ESX[i] 6.0 / 6.5 / 6.7 / 7.0 / 8.0 ・ Citrix Hypervisor 8.2 ・ Proxmox VE 7.2-1 ・ Nutanix Acropolis Hypervisor (AHV) 20190916.276

※ 各ハイパーバイザーのゲスト OS として動作する、上記オペレーティングシステムをサポートしています。

※ HyperAgent の対象 OS はナレッジベースを参照してください。

最新のシステム要件は、Web サイトのシステム要件ページ (<https://www.actiphly.com/ja-jp/support/system-requirements/>) よりご確認ください。

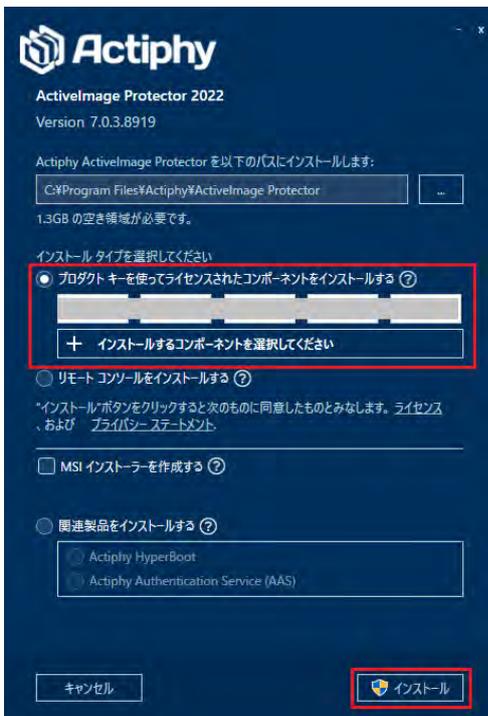
## 2. インストール

対象コンピューターへの ActivelImage Protector のインストール手順について説明します。

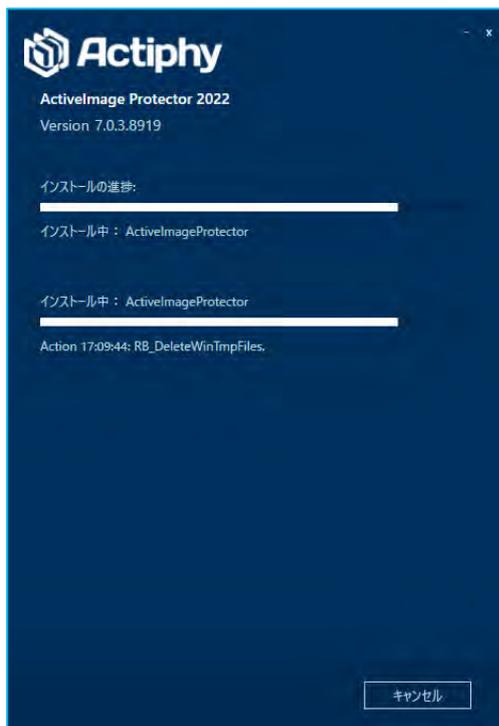
1. 製品メディアをセットすると、インストールのランチャーが表示されますので、「ActivelImage Protector」の [インストール] をクリックしてインストーラーを起動します。ランチャーが表示されない場合は、製品メディア内の「Launch.exe」を直接実行してください。または、製品メディアから「Setup」フォルダー内の「Setup.exe」を実行して、直接インストーラーを起動します。



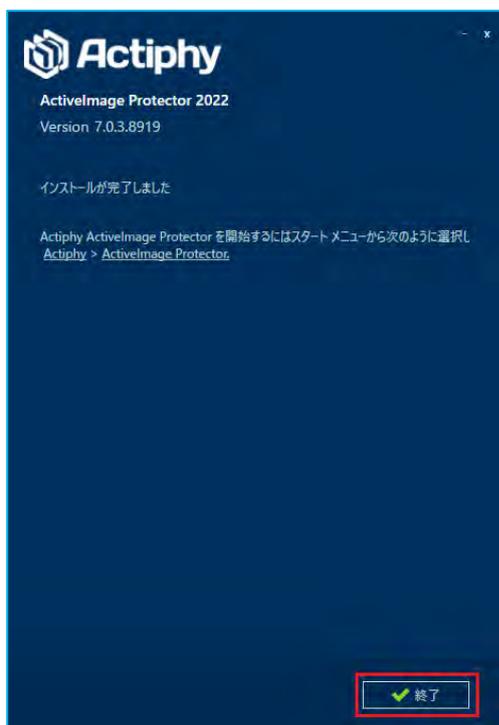
2. インストーラーが起動したら、「[プロダクトキーを使ってライセンスされたコンポーネントをインストールする]」を選択して、プロダクトキーを入力します。「インストール」をクリックするとインストールが開始されます。



3. インストールの進捗状況が表示されます。



4. インストールが完了したら [終了] をクリックします。システムの再起動は不要です。



### 3. アクティベーション

---

ActiveImage Protector のアクティベーション(ライセンス認証)には、「オンライン認証」、「Actiphy Authentication Service (AAS) 認証」、「ライセンスファイル認証」の3種類を用意しています。基本的には、インターネットを経由してアクティブファイのライセンスサーバーに接続して、自動的にアクティベーションが行われるため、アクティベーションのための作業は特に必要ありません。

インターネットに接続されていないコンピューターに導入する場合は、「Actiphy Authentication Service (AAS) 認証」、または「ライセンスファイル認証」により、アクティベーションを行ってください。

アクティベーション方法については、Web サイトにアクティベーションガイドをアップしていますので参照してください。

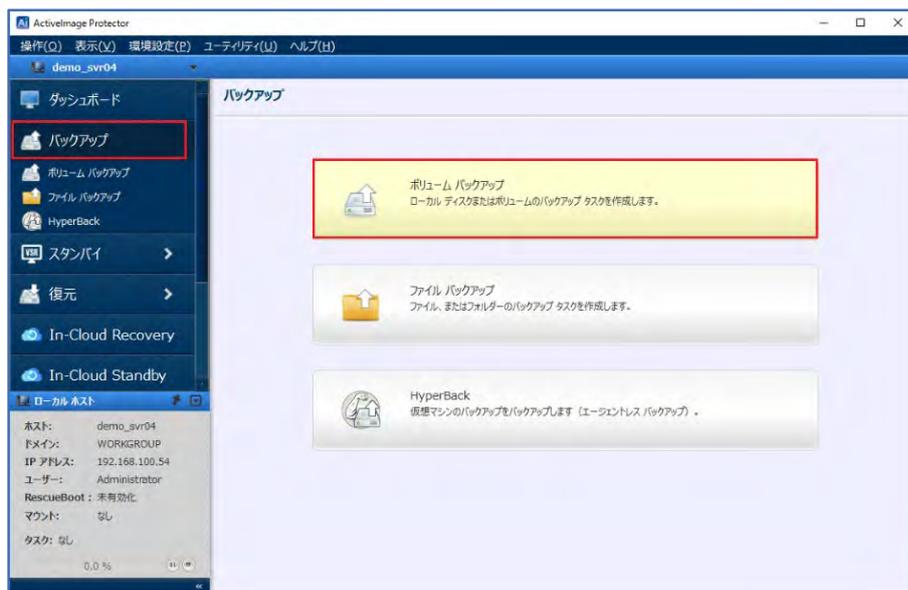
- ActiveImage Protector 2022 Server  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_server](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_server)
- ActiveImage Protector 2022 Desktop  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_desktop](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_desktop)
- ActiveImage Protector 2022 Linux  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_linux](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_linux)
- ActiveImage Protector 2022 Virtual (オンライン)  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_virtual\\_online](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_virtual_online)
- ActiveImage Protector 2022 Virtual (オフライン)  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_virtual](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_virtual)
- AAS Docker  
[https://www.actiphy.com/ja-jp/activation\\_guide/aas\\_docker/](https://www.actiphy.com/ja-jp/activation_guide/aas_docker/)
- ライセンス / バンドル ファイルの解除  
[https://www.actiphy.com/ja-jp/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_license\\_recovery\\_guide](https://www.actiphy.com/ja-jp/activation_guide/actiphy_activeimage_protector_2022_license_recovery_guide)

## 4. バックアップの設定と実行

### 4-1. ボリューム バックアップ：ワンタイム

今すぐバックアップを実行する、ワンタイム バックアップの手順について説明します。

1. ActiImage Protector を起動します。  
Windows スタートメニューから [ActiPhy] → [ActiImage Protector] をクリックします。
2. [バックアップ] → [ボリュームバックアップ] をクリックします。



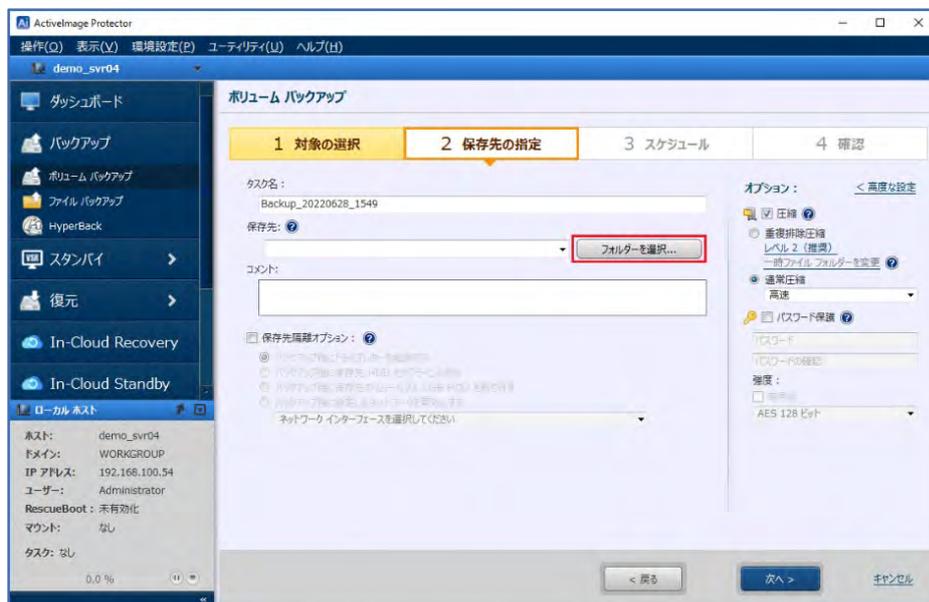
3. バックアップ対象を選択します。  
ここでの例として、バックアップ対象は [ディスク] を選択します。  
[ディスク] を選択してから、[ディスク 0] と [ディスク 1] のチェックボックスにチェックを入れます。  
バックアップ対象の選択が完了したら、[次へ] をクリックします。



## バックアップの設定と実行

### 4. バックアップの保存先を指定します。

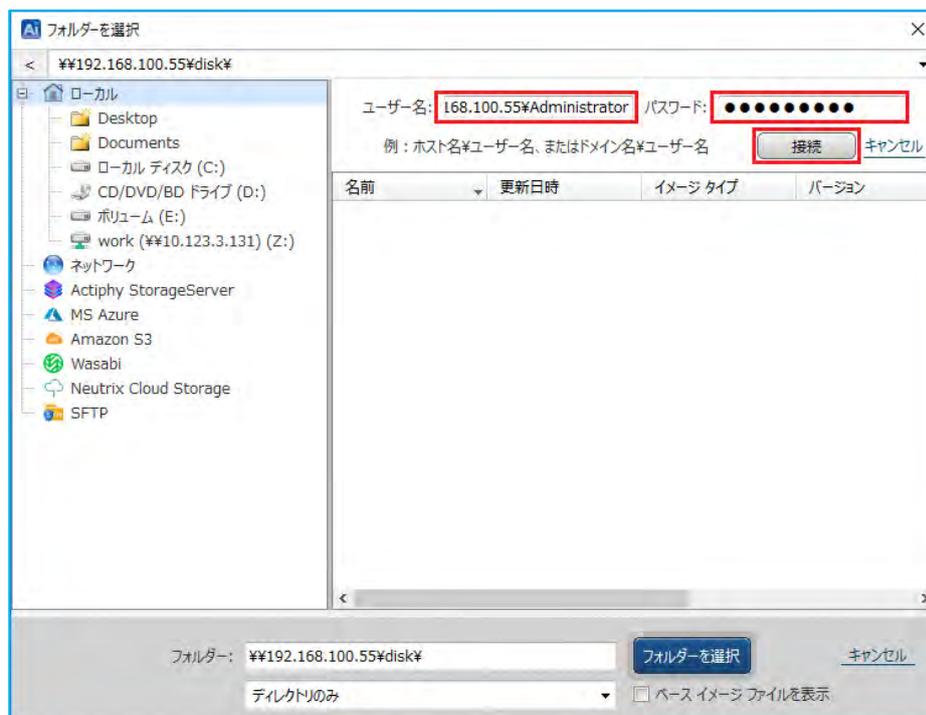
ここでの例として、ネットワーク共有フォルダー「¥¥192.168.100.55¥disk」を保存先として説明します。[フォルダーを選択] をクリックします。



### 5. 保存先の共有フォルダーを指定します。

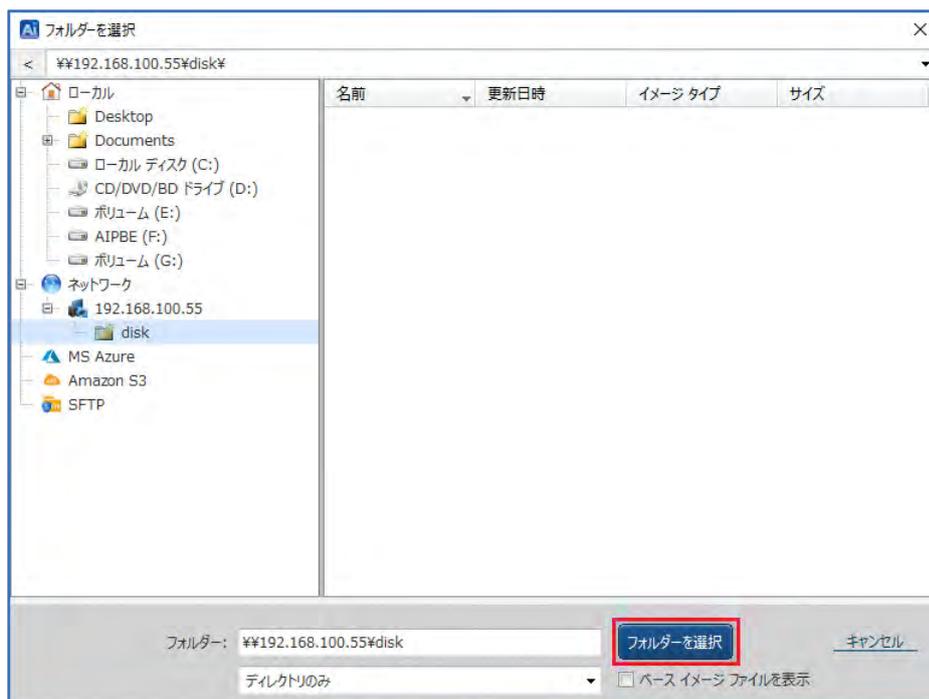
下記の場所に保存先の共有フォルダーの直接パス「¥¥192.168.100.55¥disk」を入力して、Enter キーを押します。次に、保存先の共有フォルダーに対する認証情報を入力します。

ここでの例として、[ユーザー名:] に「192.168.100.55¥Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。

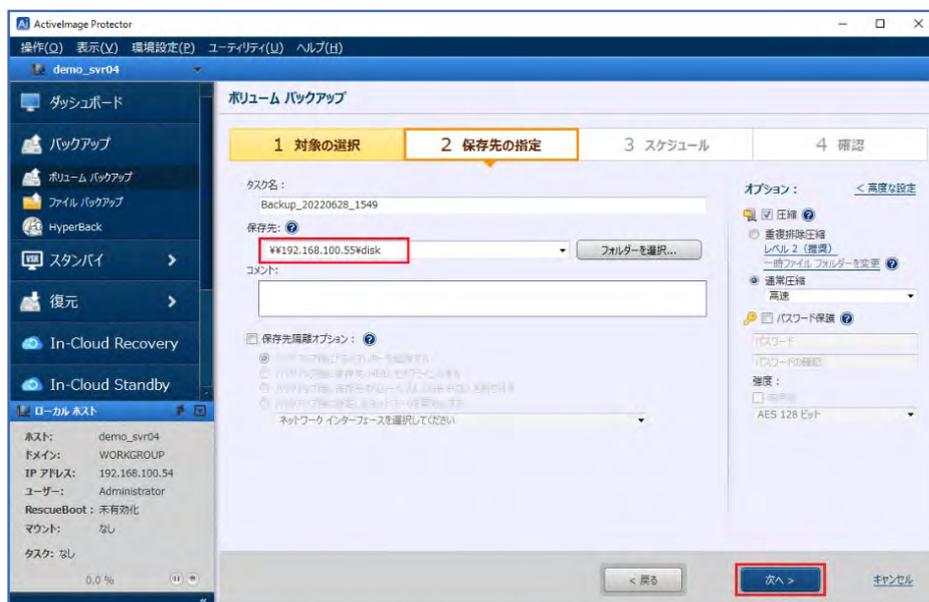


## バックアップの設定と実行

6. 保存先の共有フォルダーが選択されていることを確認してから、[フォルダーを選択] をクリックします。



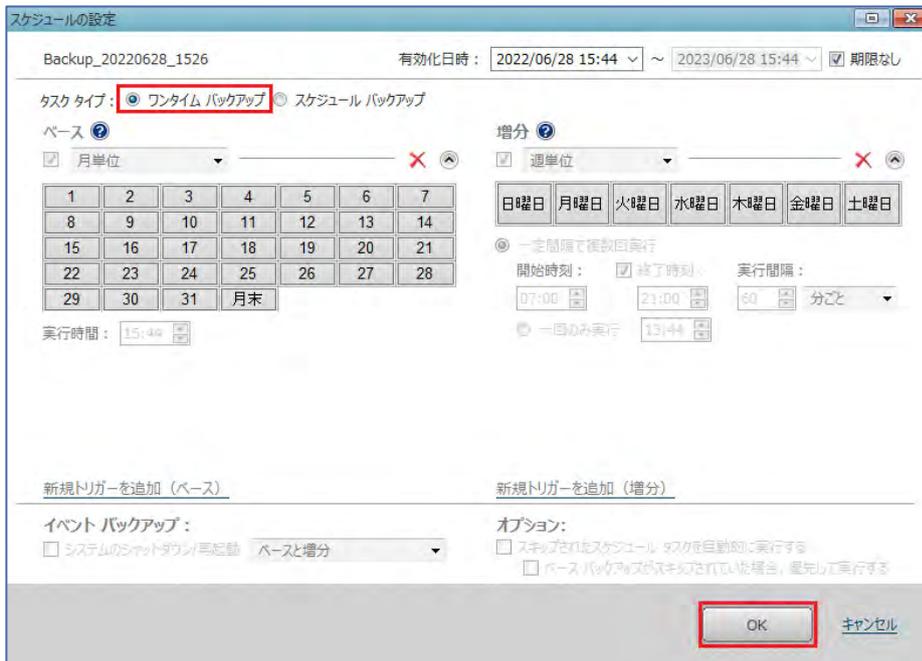
7. 保存先の共有フォルダーが登録されていることを確認してから、[次へ] をクリックします。  
[保存先隔離オプション]、[オプション] の設定は、次項 (P.20) を参照してください。



## バックアップの設定と実行

### 8. ワンタイム（単体）バックアップを選択します。

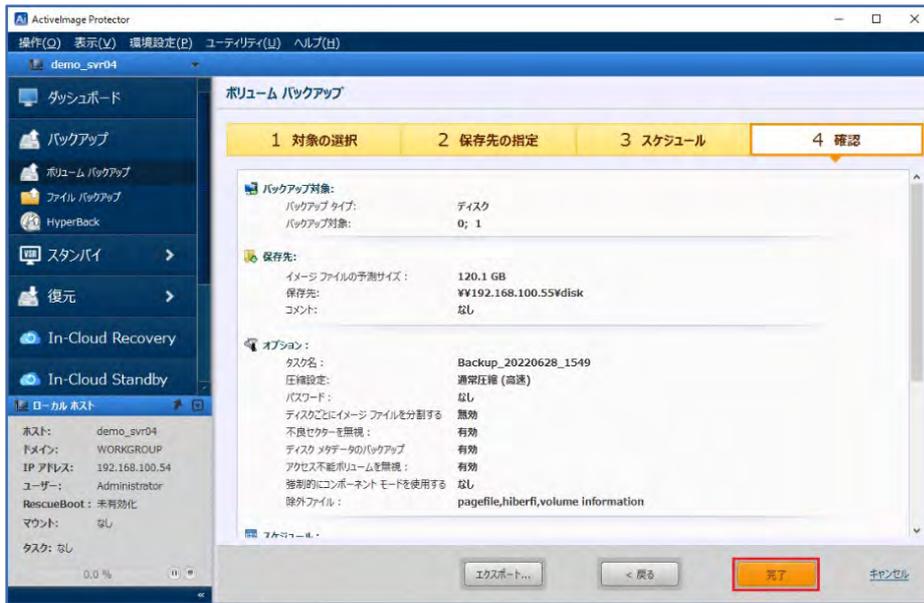
スケジュールの設定から [タスク タイプ] に、[ワンタイム バックアップ] を選択して、[OK] をクリックします。



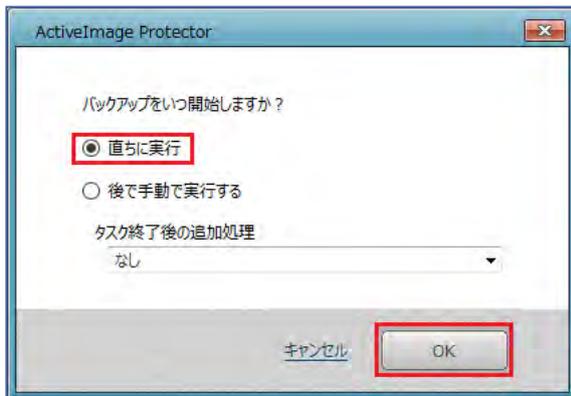
ここでは、このまま [次へ] をクリックします。



9. バックアップの内容を確認してから、[完了] をクリックします。

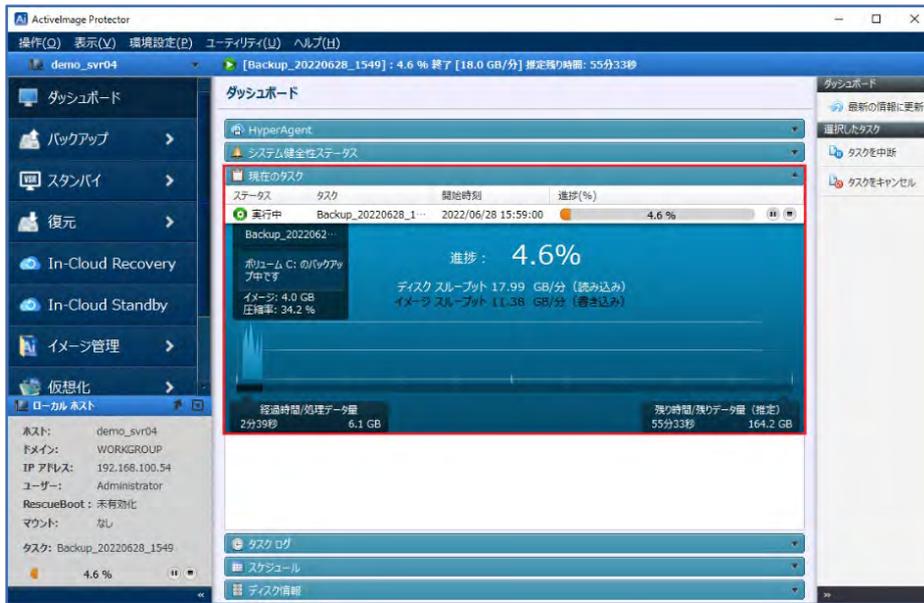


10. [直ちに実行] を選択してから、[OK] をクリックするとバックアップが開始されます。  
[タスク終了後の追加処理] は、バックアップ完了後にシステムのシャットダウンや再起動が必要な場合に設定します。

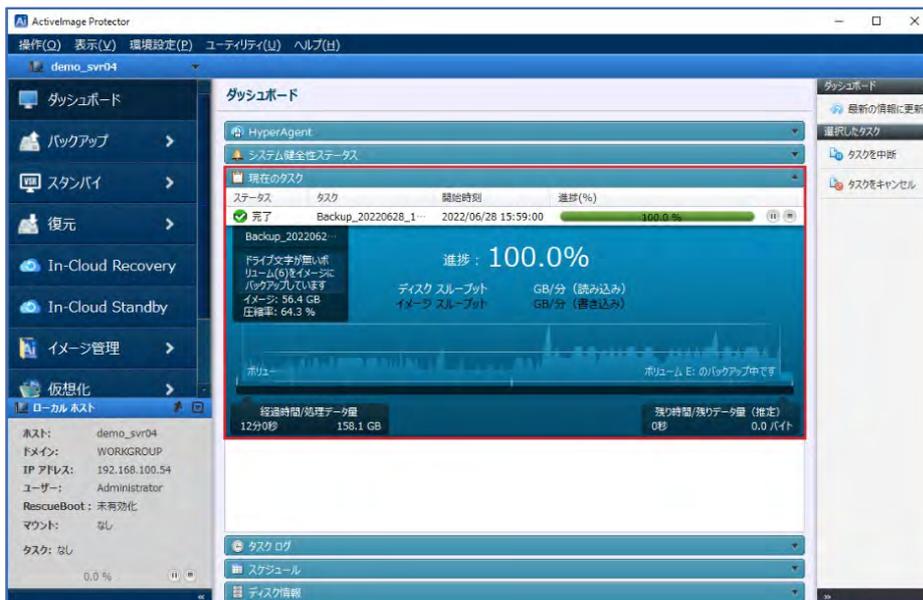


## バックアップの設定と実行

11. バックアップが開始されると、バックアップタスクの進捗状況が表示されます。



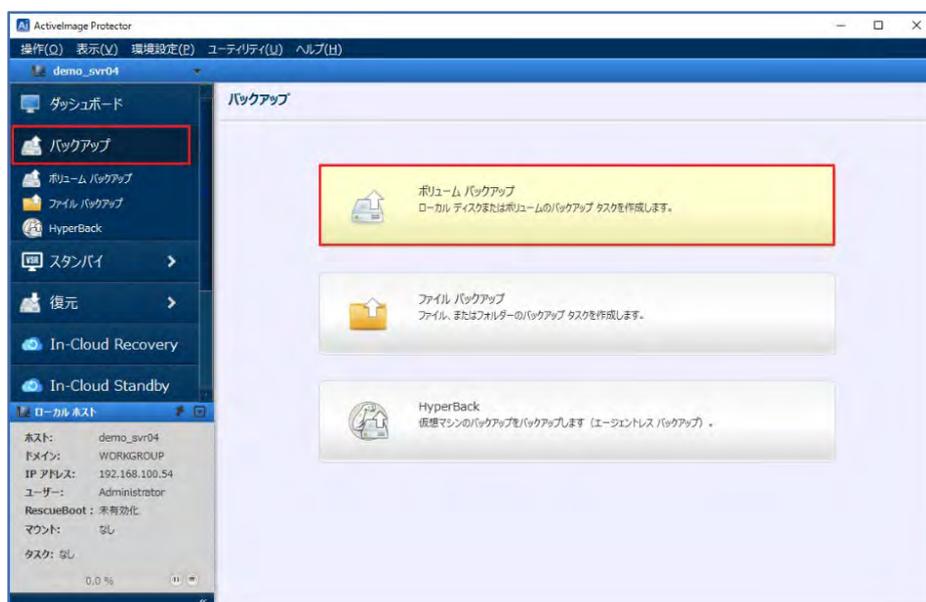
12. 進捗が100%になるとバックアップは完了です。



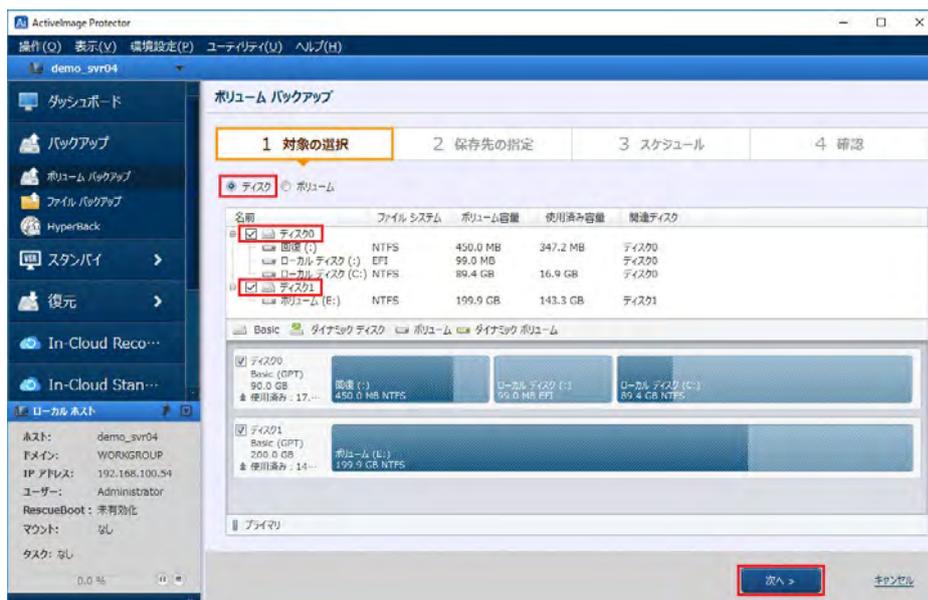
## 4-2. ボリューム バックアップ：スケジュール

定期的にバックアップを実行する、スケジュール バックアップの設定手順について説明します。

1. ActiImage Protector を起動します。  
Windows スタートメニューから [ActiPhy] → [ActiImage Protector] をクリックします。
2. [バックアップ] → [ボリュームバックアップ] をクリックします。



3. バックアップ対象を選択します。  
ここでの例として、バックアップ対象は [ディスク] を選択します。  
[ディスク] を選択してから、[ディスク 0] と [ディスク 1] のチェックボックスにチェックを入れます。  
バックアップ対象の選択が完了したら、[次へ] をクリックします。



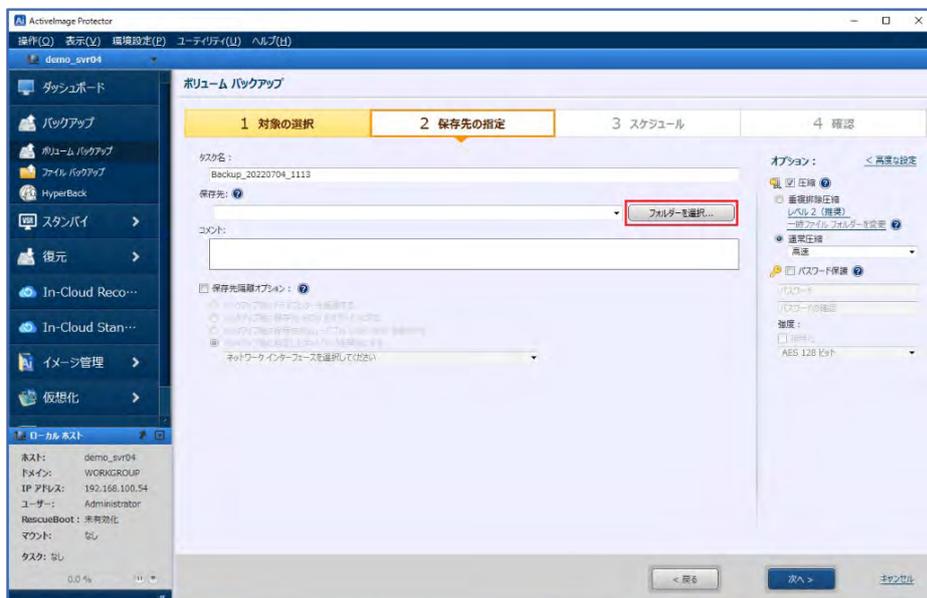
## バックアップの設定と実行

### 4. バックアップの保存先を指定します。

ここでの例として、ネットワーク共有フォルダー「¥¥192.168.100.55¥disk」を保存先として説明します。

[フォルダーを選択] をクリックします。

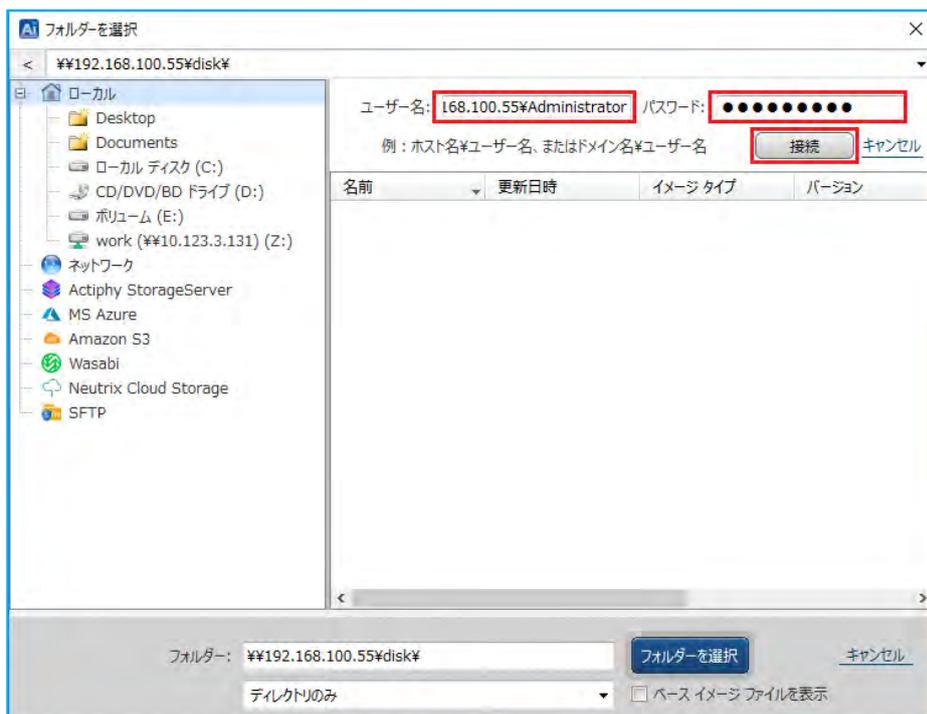
テキストボックスの右にある [▼] をクリックすると、これまでのバックアッププロセスやバックアップで使用した保存先が表示されますので、ここから選択もできます。



### 5. 保存先の共有フォルダーを指定します。

下記の場所に保存先の直接パス「¥¥192.168.100.55¥disk」を入力して、Enter キーを押します。次に、保存先に対する認証情報を入力します。

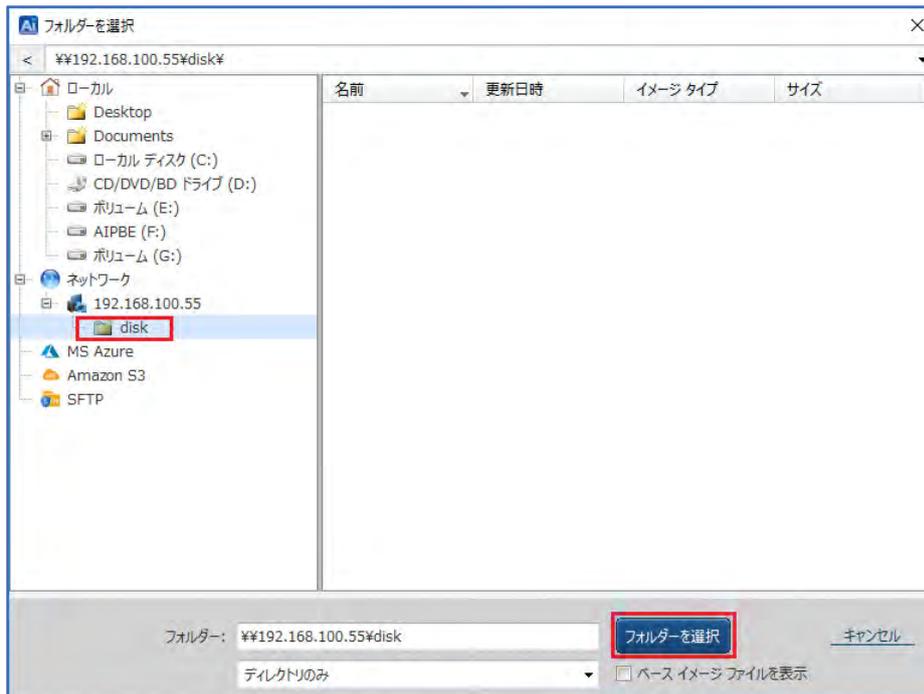
ここでの例として、[ユーザー名:] に「192.168.100.55¥Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。



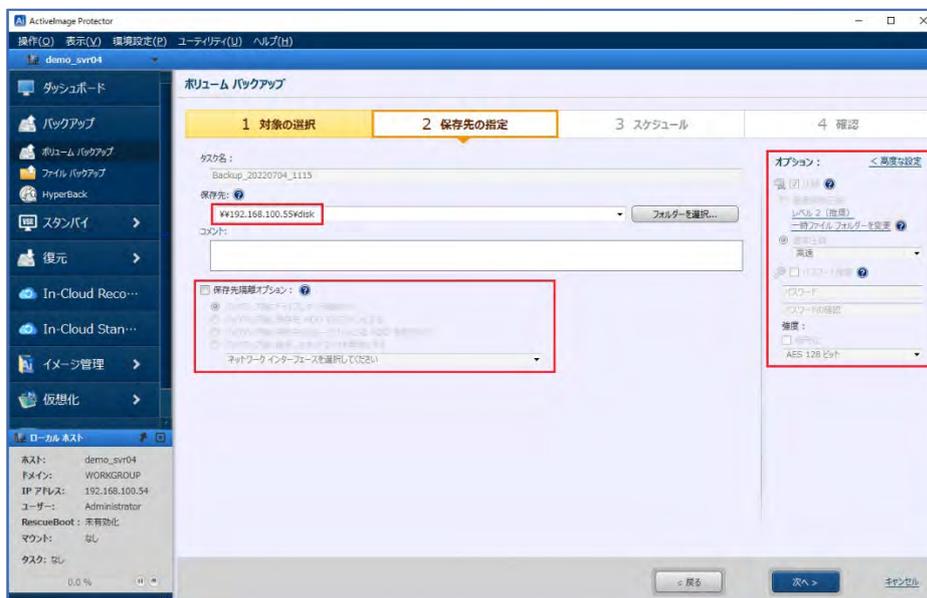
## バックアップの設定と実行

### 6. 保存先の共有フォルダーを登録します。

保存先の共有フォルダーを指定してしてから、[フォルダーを選択] をクリックします。



### 7. 保存先の共有フォルダーが登録されていることを確認後に、[次へ] をクリックします。「保存先隔離オプション」、「オプション」の設定は、次項 (P.20) を参照してください。



## バックアップの設定と実行

### 8. バックアップのスケジュール設定を行います。

ここでの例として、タスク タイプに [スケジュールバックアップ] を選択して、下記の設定で週単位のバックアップスケジュールを作成します。

- ・ ベースバックアップ：週単位
- ・ 増分バックアップ：週単位
- ・ ベースバックアップ：日曜日の午前1時
- ・ 増分バックアップ：月曜日から土曜日までの午前1時

すべての項目を設定したら、[OK] をクリックします。

スケジュールの設定

Backup\_20220704\_1115 有効化日時: 2022/07/04 11:27 ~ 2023/07/04 11:27 期限なし

タスクタイプ:  ワンタイムバックアップ  スケジュールバックアップ

**ベース**

週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

実行時間: 01:00

**増分**

週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

一定間隔で複数回実行  
開始時刻: 07:00 終了時刻: 21:00 実行間隔: 60 分ごと

一回のみ実行: 01:00

新規トリガーを追加 (ベース) 新規トリガーを追加 (増分)

イベントバックアップ:  
 システムのシャットダウン/再起動 ベースと増分

オプション:  
 スキップされたスケジュールタスクを自動的に実行する  
 ベース・増分のバックアップが完了した場合、優先して実行する

OK キャンセル

マルチスケジュール設定例:

[新規トリガーを追加] をクリックすると、スケジュール設定を追加することができます。週単位のスケジュール設定に加え、例えば1月から12月まで、「第2金曜日」あるいは「第4金曜日」といった指定が可能です。

指定曜日

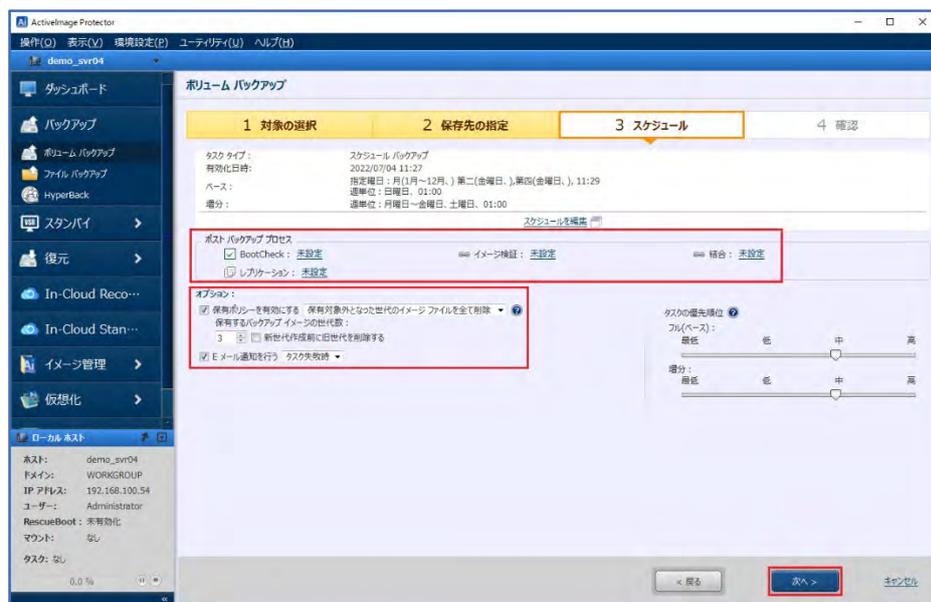
月: 1 2 3 4 5 6 7 8 9 10 11 12

	日	月	火	水	木	金	土
第一:							
第二:							
第三:							
第四:							
第五:							
最終:							

実行時間: 01:00

新規トリガーを追加 (ベース)

9. [スケジュール] タブでは、[保有ポリシーの設定]、[Eメール通知] を設定してから、[次へ] をクリックします。「ポストバックアッププロセス」の設定は、次項 (P.22) を参照してください。

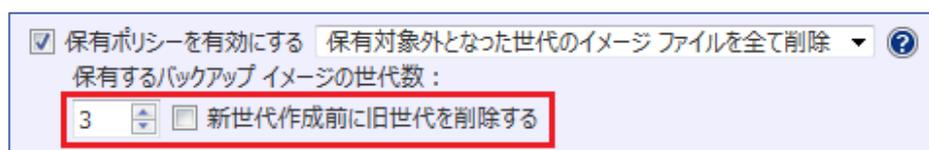


### (1) 保有ポリシーの設定

バックアップ保存先に残すバックアップの世代数を設定します。

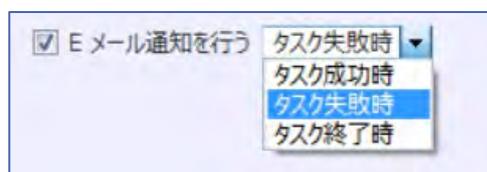
ここでの例として、[保有ポリシーを有効にする] のチェックボックスにチェックを入れます。[保有するバックアップの世代数:] をデフォルト設定の「3」にします。この設定で、バックアップの保存先に3世代分のバックアップが残ります。

※ ActiveImage Protector は、ベースバックアップとそれに紐づく増分バックアップを1世代として管理しています。



### (2) Eメール通知の設定

バックアップタスクの成功/失敗/終了時に、Eメール通知を行えます。[Eメール通知を行う] のチェックボックスにチェックを入れます。[タスク失敗時] を選択すると、バックアップタスクがエラーなどで失敗した場合のみEメールで通知します。Eメール通知を行うには、あらかじめ[環境設定]の[Eメール通知設定]で送信設定をする必要があります。

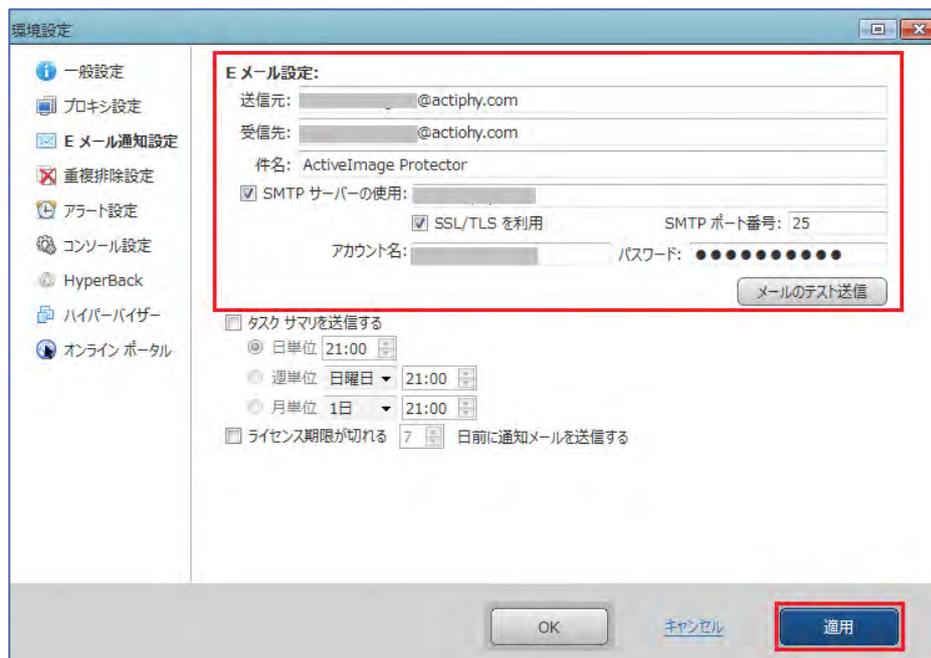


## バックアップの設定と実行

### (3) E メール通知の環境設定

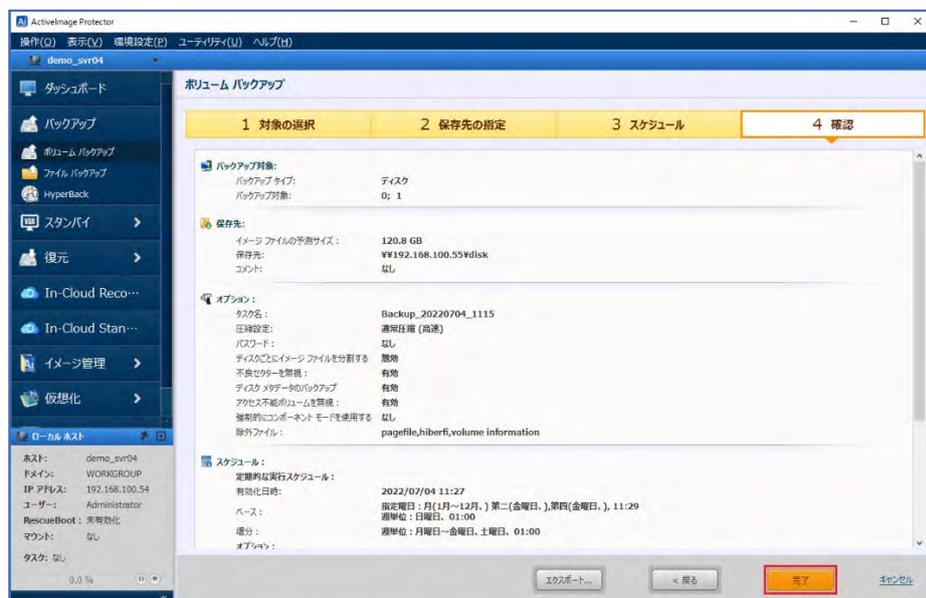
[環境設定] → [E メール通知設定] をクリックして、E メール通知の環境設定を起動します。

すべてのEメール通知設定が完了したら、[メールのテスト送信] を実行して正常動作を確認します。テストメールの送信が確認されたら、[適用] をクリックします。



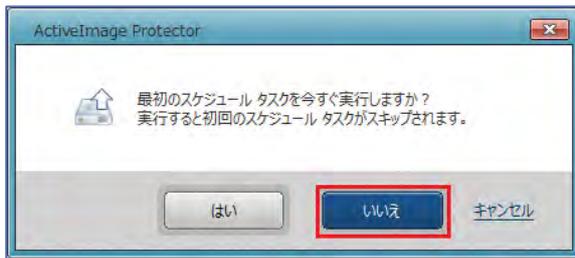
### 10. バックアップの設定内容が表示されます。

内容を確認してから [完了] をクリックします。

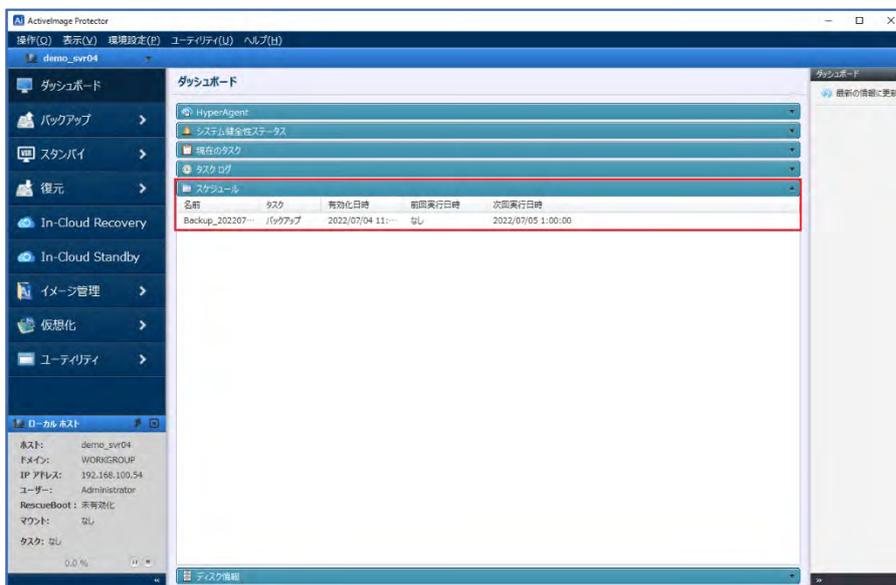


## バックアップの設定と実行

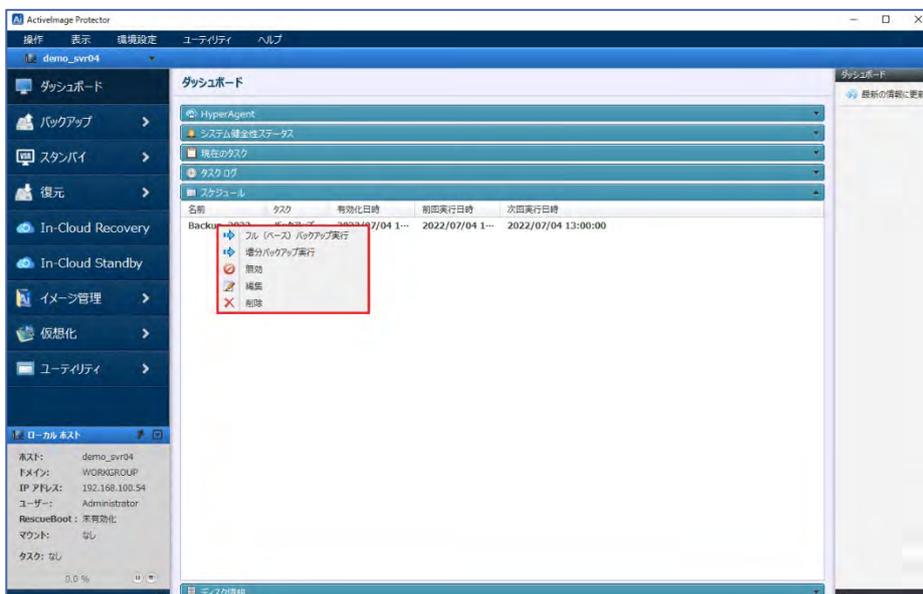
11. [いいえ] をクリックして、ダッシュボードに戻ります。[はい] をクリックすると最初のスケジュール タスクが実行されます。



12. 作成済みのスケジュールは、[ダッシュボード] → [スケジュール] で確認できます。指定した時刻になると、スケジュールバックアップが実行されます。



13. [スケジュール名] を右クリックすると、直ちにフルバックアップや増分バックアップの実行、スケジュールの編集などを行うことができます。



14. [保存先隔離オプション]、[オプション]、[高度な設定]、[ポストバックアッププロセス] は、必要に応じて設定します。ここでは、設定例について説明します。

(1) [保存先隔離オプション] の設定

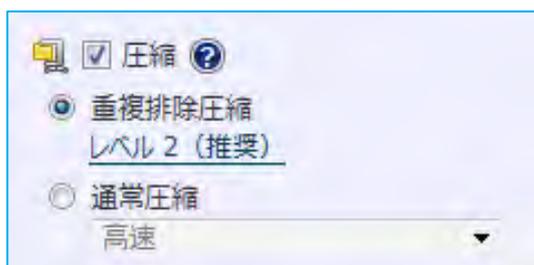
保存先隔離オプションは、バックアップ作業の終了後に、ディスクのオフライン化やネットワークの遮断を行う機能です。ランサムウェアなどのウイルス感染があった場合でも、攻撃からバックアップ保存先やバックアップファイルを保護します。保存先隔離オプションには、4つのオプションが用意されています。



- バックアップ後にドライブレターを削除する：  
バックアップ後にローカルハードディスクからドライブ文字の割り当てを解除します。
- バックアップ後に保存先 HDD をオフラインにする：  
保存先のローカルハードディスクをオフラインにします。
- バックアップ後に保存先リムーバブル USB HDD を取り外す：  
USB ハードディスクなどの取り外し可能なハードディスクをイジェクトします。
- バックアップ後に指定したネットワークを無効にする：  
バックアップ後にバックアップ先のネットワークを遮断します。

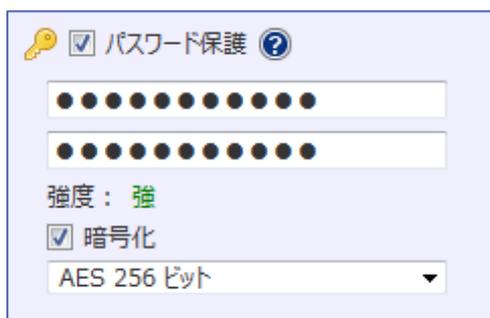
(2) [オプション] の設定

- 圧縮レベルの設定：  
標準設定の通常圧縮と重複排除圧縮の2種類の圧縮方式をサポートします。圧縮率は、データの種類により異なりますが、通常圧縮で70%、重複排除圧縮では50%程度を目安としてください。画面の右の[オプション:] から指定します。重複排除圧縮を選択すると、その下の[レベル2 (推奨)] と重複排除処理の一時作業領域の[一時ファイルフォルダーを変更] の設定が可能になります。



- 暗号化の設定：

バックアップファイルのパスワード保護と暗号化をサポートしています。まず、[パスワード保護] のチェックボックスにチェックを入れ、パスワードを入力します。次に、暗号化レベルの「RCS」、「AES128 ビット」、「AES256 ビット」から選択して設定します。バックアップファイルの外部サイト保管やサイバー攻撃からバックアップファイルを安全に保護します。

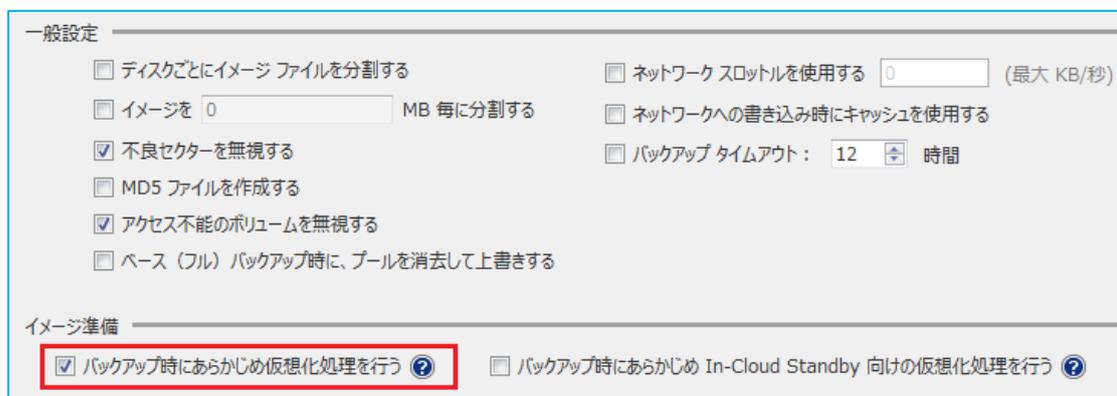


(3) [高度な設定] の設定

オプション中の [高度な設定] では、バックアップファイルの分割、ネットワーク共有フォルダーに保存する際の帯域制御やキャッシュ使用、バックアップファイルの仮想化処理、バックアップ処理と連動したユーザー作成のスキプトの実行などの設定が可能です。ここでは、[バックアップファイルの仮想化処理] と [スクリプト] について解説します。

- バックアップファイルの仮想化処理：

エージェントの「仮想化」機能を使わずに、仮想マシンに直接復元する場合は [バックアップ時にあらかじめ仮想化処理を行う] のオプションを有効にしてください。あらかじめ、エージェントの「仮想化」機能と同じ処理 (VMware vSphere / Microsoft Hyper-V のドライバー追加、レジストリ変更など) を行った状態でバックアップを作成します。例えば、バックアップ元より小さなサイズの仮想ディスクで構成された仮想マシンに、ボリューム単位での縮小復元やディスクのボリュームレイアウトの変更など、柔軟な復元を行うことができます。



## バックアップの設定と実行

- スクリプトの設定：

指定したスクリプトをスナップショット実行前、実行後、およびバックアップ作成後に実行することができます。使用例として、Microsoft ボリューム・シャドウコピー・サービス (Volume Shadow Copy Service) に対応していないデータベース・アプリケーションの場合は、バックアップデータの整合性を保つために、バックアップ開始前にサービスを停止する必要がありますが、スナップショット実行前後に、サービス停止/起動のスクリプトを設定することができます。サービスの停止時間は、スナップショットを取得する約1分~2分となります。

The screenshot shows a configuration window for backup scripts. It has three rows for different stages: 'スナップショット実行前に実行するスクリプト' (Script to run before snapshot), 'スナップショット実行後に実行するスクリプト' (Script to run after snapshot), and 'イメージファイル作成後に実行するスクリプト' (Script to run after image file creation). Each row has a text input field for the script path (e.g., 'C:\temp\DB\_shutdown.ps1.txt'), a '...' button, a 'タイムアウト' (Timeout) field set to '30 分' (30 minutes), and an '実行設定' (Execution setting) dropdown menu set to 'ベースと増分' (Base and incremental). A checkbox at the bottom is labeled 'バックアップタスクの実行エラー時でも指定したスクリプトを全て実行する' (Execute all specified scripts even when backup task fails).

#### (4) ポストバックアッププロセスの設定

[ポストバックアッププロセス] では、[BootCheck]、[イメージ検証]、[結合]、[レプリケーション] の設定を行います。

- BootCheck の設定：

バックアップファイルが、起動可能か仮想マシンを使い確認します。

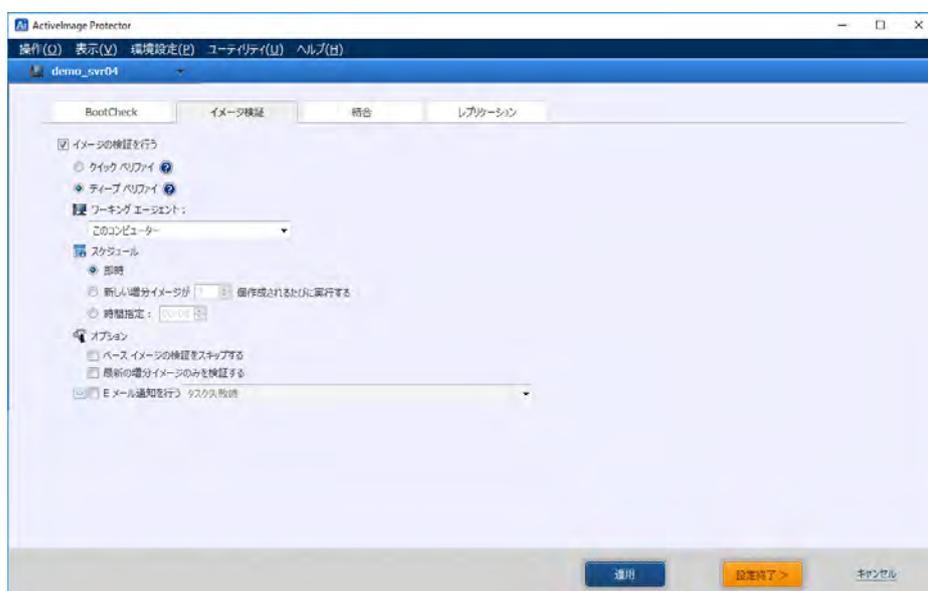
[BootCheck を行う] のチェックボックスにチェックを入れると、BootCheck が有効になります。実行するスケジュール、メール通知などを設定します。

The screenshot shows the 'ActiveImage Protector' software interface. The 'BootCheck' tab is selected. The 'BootCheck を行う' (Perform BootCheck) checkbox is checked. Under 'ワーニング エージェント' (Warning Agent), 'このコンピュータ' (This computer) is selected. Under 'スケジュール' (Schedule), '即時' (Immediately) is selected. Under '設定' (Settings), '失敗した場合、ひとつ前のイメージで再試行する' (Retry with previous image on failure) is checked, and the 'タイムアウト' (Timeout) is set to '600 秒' (600 seconds). Under 'オプション' (Options), 'Eメール通知を行う' (Send email notification) is checked, with 'タスク失敗時' (Task failure) selected for the notification trigger. Buttons for '適用' (Apply), '設定完了' (Finish), and 'キャンセル' (Cancel) are at the bottom.

## バックアップの設定と実行

- ・ イメージ検証の設定：

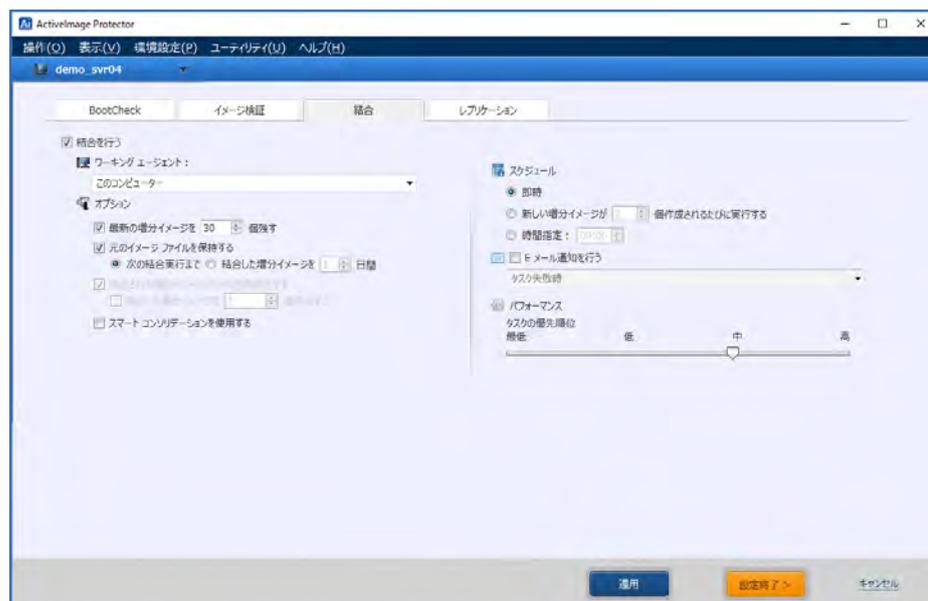
バックアップファイルの検証を行います。[イメージの検証を行う]のチェックボックスにチェックを入れると、イメージ検証が有効になります。ここで、実行するスケジュールを設定します。



- ・ 結合の設定：

増分バックアップなどで、バックアップファイルが多数になった場合に、結合（コンソリデーション）してバックアップファイルを削減します。バックアップファイルの管理を容易にするための機能です。

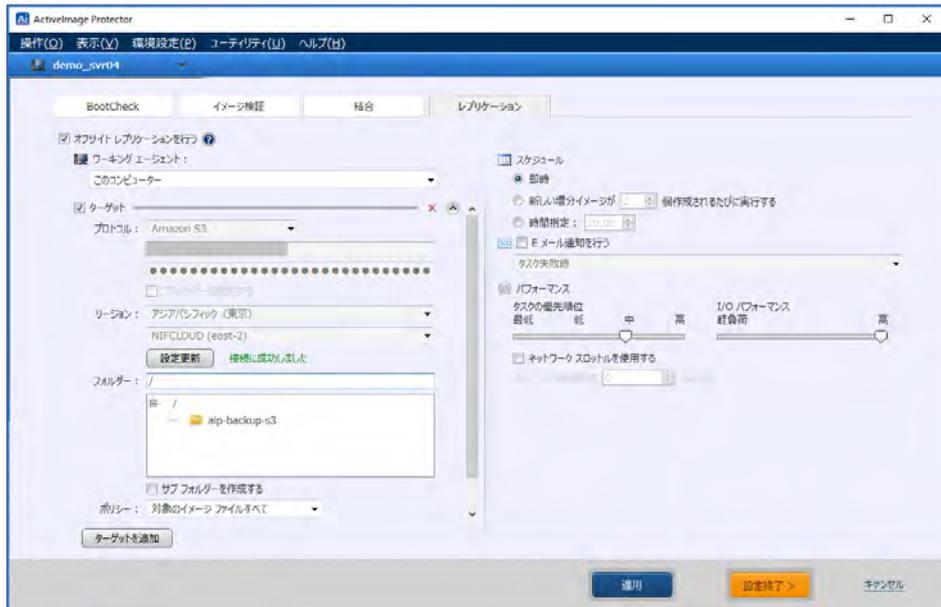
[結合を行う]のチェックボックスにチェックを入れると有効になります。コンソリデーションを行うファイル数、実行するスケジュール、メール通知、パフォーマンスなどを設定します。



## バックアップの設定と実行

- レプリケーションの設定：

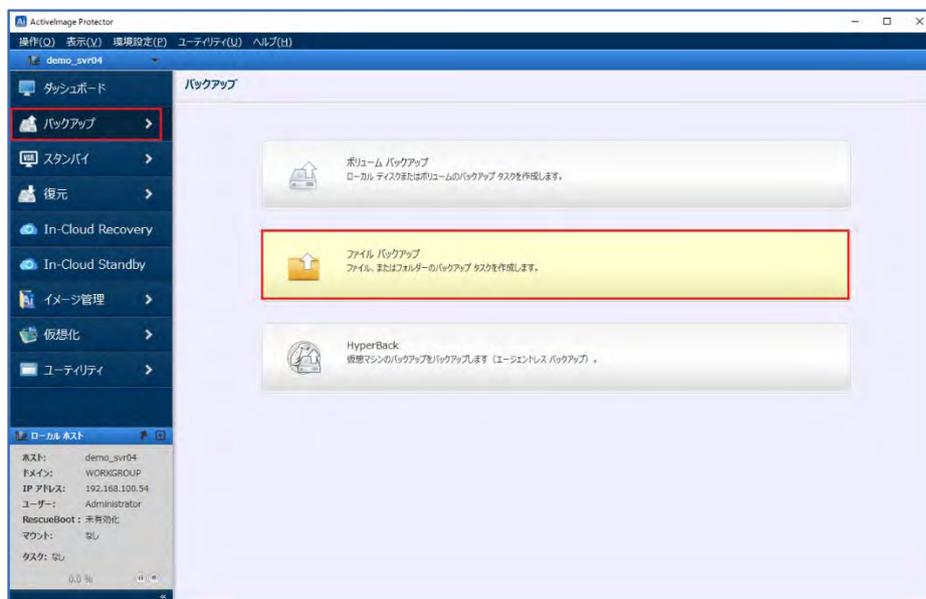
クラウドストレージなどを含め、任意の場所にレプリケーションを作成します。災害対策の基本の1つとして、バックアップデータを遠隔地に保存するという考え方があります。ActiveImage Protector では、ローカルストレージ / 共有フォルダー / WebDAV / FTP / Amazon S3 / Azure Storage / OneDrive / Google Drive / Dropbox / Wasabi / Neutrix Cloud の保存先が利用可能です。



### 4-3. ファイル バックアップ：スケジュール

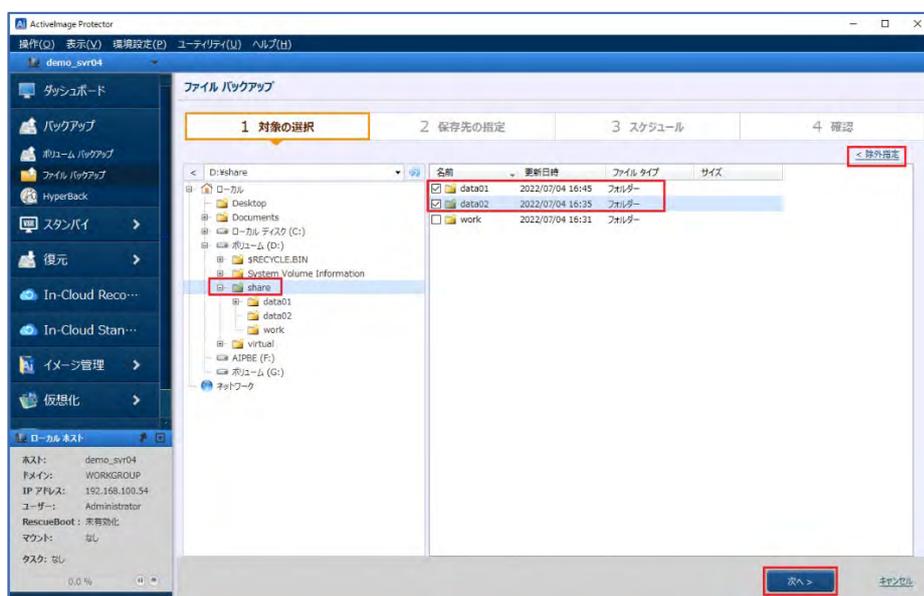
定期的にファイル/フォルダー単位のスケジュール バックアップの設定手順について説明します。

1. ActiVImage Protector を起動します。  
Windows スタートメニューから [ActiPhy] → [ActiVImage Protector] をクリックします。
2. [バックアップ] → [ファイル バックアップ] をクリックします。



3. バックアップ対象を選択します。

ここでの例として、Dドライブの「share」フォルダー内の「data01」と「data02」のフォルダーをバックアップ元として説明します。Dドライブの「share」フォルダーを選択して、その中の「data01」と「data02」のフォルダーのチェックボックスにチェックを入れます。右上の「<除外設定を」をクリックすると、除外したいファイルを指定することができます。除外指定は、ファイルのパス（例：C:\test\EULA.txt）、拡張子（例：EULA.txt）、ワイルドカード「\*」（例：\*.txt、EULA.\*）などで指定します。設定が完了したら、「次へ」をクリックします。

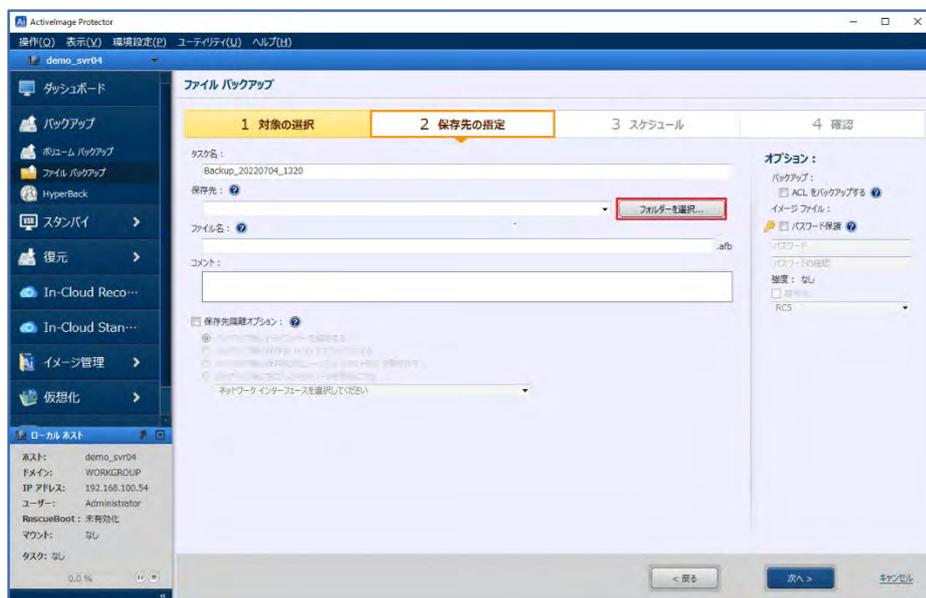


## バックアップの設定と実行

### 4. バックアップの保存先を指定します。

ここでの例として、ネットワーク共有フォルダー「¥¥192.168.100.55¥disk1」を保存先として説明します。

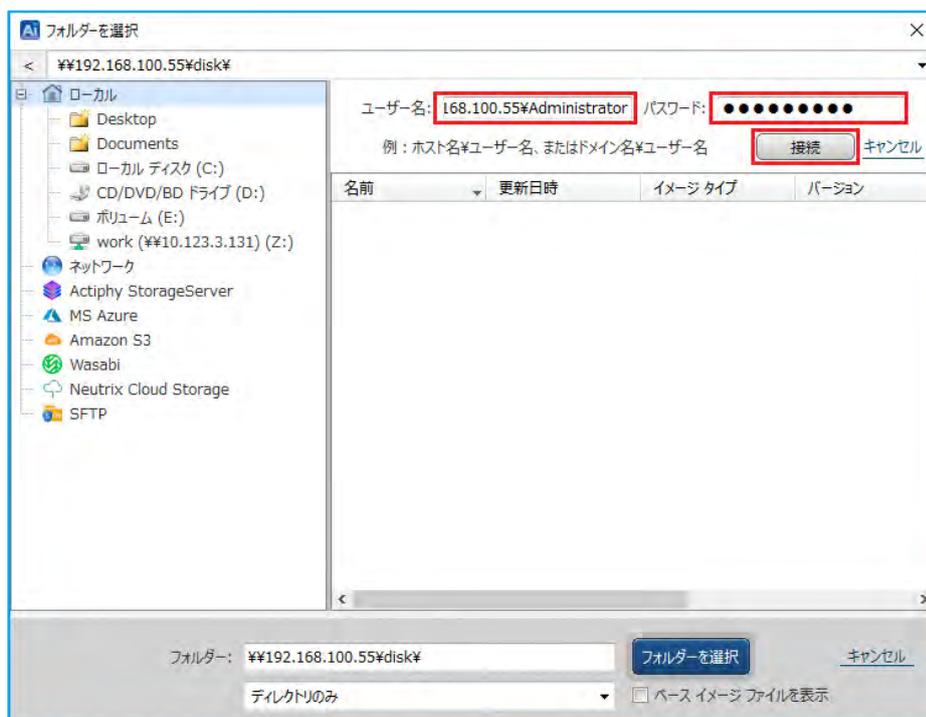
[フォルダーを選択] をクリックします。テキストボックスの右にある [▼] をクリックすると、これまでのバックアッププロセスやバックアップで使用した保存先が表示されますので、ここから選択もできます。



### 5. 保存先の共有フォルダーを指定します。

下記の場所に保存先の直接パス「¥¥192.168.100.55¥disk1」を入力し、Enter キーを押します。次に、保存先に対する認証情報を入力します。

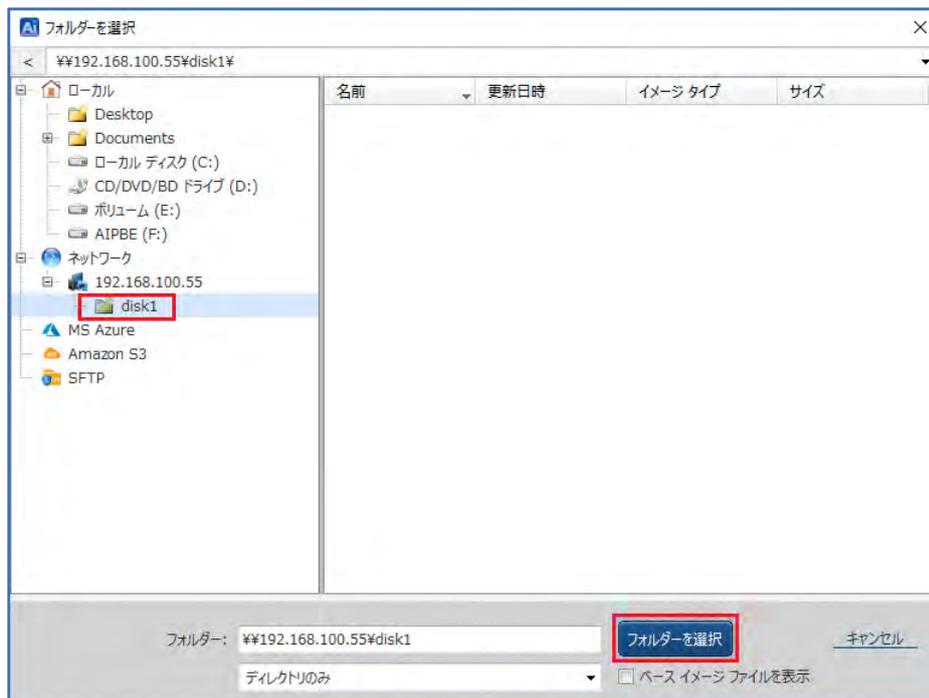
ここでの例として、[ユーザー名:] に「192.168.100.55¥Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。



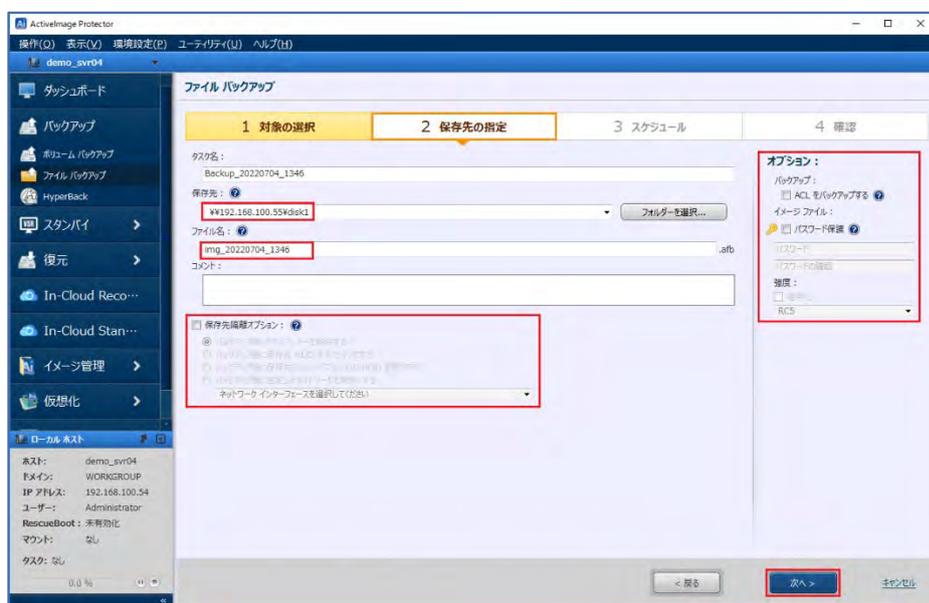
## バックアップの設定と実行

### 6. 保存先の共有フォルダーを登録します。

保存先の共有フォルダーを指定してしてから [フォルダーを選択] をクリックします。



### 7. 保存先の共有フォルダーが登録されていることを確認後に、 [次へ] をクリックします。「ファイル名」には、任意のファイル名を設定することができます。「保存先隔離オプション」、「オプション」は必要に応じて設定します。



(1) [保存先隔離オプション] の設定

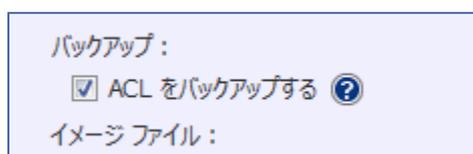
保存先隔離オプションは、バックアップ作業の終了後に、ディスクのオフライン化やネットワークの遮断を行う機能です。ランサムウェアなどのウイルス感染があった場合でも、攻撃からバックアップ保存先やバックアップファイルを保護します。保存先隔離オプションには、4つのオプションが用意されています。



- ・ バックアップ後にドライブレターを削除する：  
バックアップ後にローカルハードディスクからドライブ文字の割り当てを解除します。
- ・ バックアップ後に保存先 HDD をオフラインにする：  
保存先のローカルハードディスクをオフラインにします。
- ・ バックアップ後に保存先リムーバブル USB HDD を取り外す：  
USB ハードディスクなどの取り外し可能なハードディスクをイジェクトします。
- ・ バックアップ後に指定したネットワークを無効にする：  
バックアップ後にバックアップ先のネットワークを遮断します。

(2) [オプション] の設定

- ・ ACL のバックアップ設定：  
[ACL をバックアップする] を有効にすると、バックアップ対象のファイルのアクセス制御リスト (ACL) がバックアップされます。復元時にはバックアップされた ACL を復元することができます。



- ・ 暗号化の設定：  
バックアップファイルのパスワード保護と AES256 ビットの暗号化をサポートしています。まず、[パスワード保護] のチェックボックスにチェックを入れ、パスワードを入力します。次に、暗号化レベルの RCS、AES 128 ビット、AES 256 ビットから選択して設定します。バックアップファイルの外部サイト保管やサイバー攻撃からバックアップファイルを安全に保護します。

## バックアップの設定と実行

A dialog box for password protection settings. It features a key icon and a checked checkbox labeled 'パスワード保護' (Password Protection). Below this are two password input fields, each containing ten black dots. The strength is indicated as '強度: 強' (Strength: Strong). There is a checked checkbox for '暗号化' (Encryption) and a dropdown menu set to 'AES 256 ビット' (AES 256 bits).

### 8. バックアップのスケジュール設定を行います。

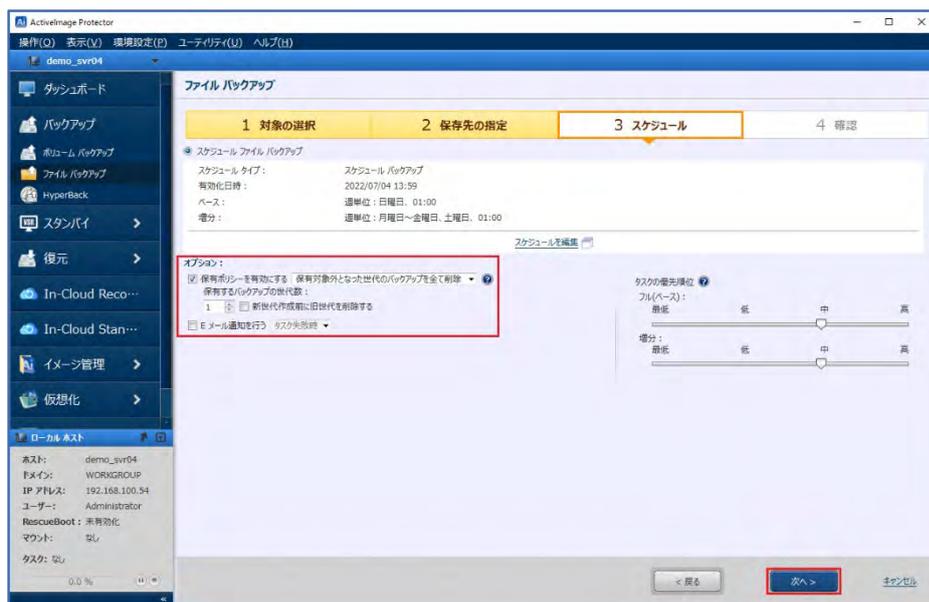
ここでの例として、下記の設定で週単位のバックアップスケジュールを作成します。

- ・ ベースバックアップ：週単位
- ・ 増分バックアップ：週単位
- ・ ベースバックアップ：日曜日の午前1時
- ・ 増分バックアップ：月曜日から土曜日までの午前1時

タスク タイプに [スケジュールバックアップ] を選択して、すべての項目を設定したら、[OK] をクリックします。

The 'スケジュールの設定' (Schedule Settings) dialog box for a backup task named 'Backup\_20220704\_1346'. The effective period is from 2022/07/04 13:59 to 2023/07/04 13:59, with '期限なし' (No limit) checked. The task type is 'スケジュールバックアップ' (Schedule Backup). The 'ベース' (Base) section is set to '週単位' (Weekly) with '日曜日' (Sunday) selected. The '増分' (Incremental) section is also set to '週単位' (Weekly) with '日曜日' (Sunday) through '土曜日' (Saturday) selected. The execution time for the base backup is '01:00'. The '一回のみ実行' (Run once) option is selected with a time of '01:00'. The 'オプション' (Options) section includes 'スキップされたスケジュール タスクを自動的に実行する' (Automatically execute skipped schedule tasks) checked. The 'OK' button is highlighted with a red box.

9. [スケジュール] タブでは、保有ポリシーの設定、Eメール通知の設定を必要に応じて設定してから、[次へ] をクリックします。

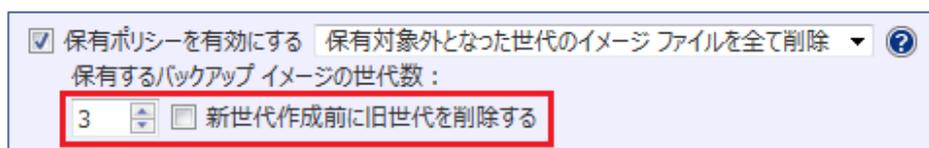


### (1) 保有ポリシーの設定

バックアップ保存先に残すバックアップの世代数を設定します。

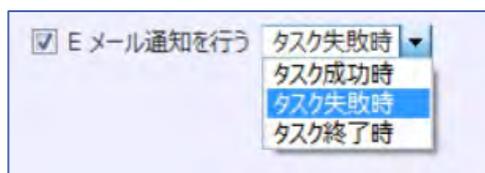
ここでの例では、[保有ポリシーを有効にする] のチェックボックスにチェックを入れ、[保有するバックアップの世代数:] をデフォルト設定の「3」に設定します。この設定で、バックアップの保存先に3世代分のバックアップが残ります。

※ ActiImage Protector は、ベースバックアップとそれに紐づく増分バックアップを1世代として管理します。



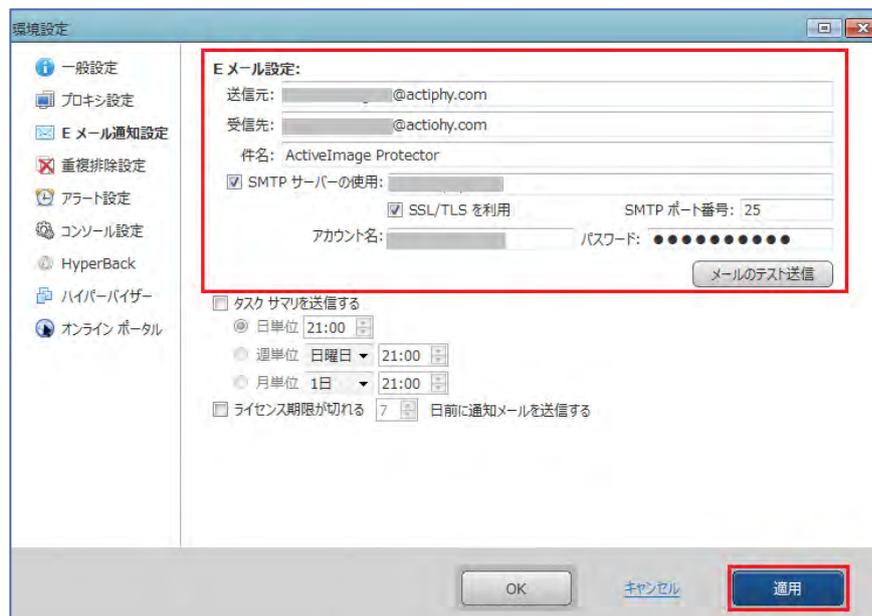
### (2) Eメール通知の設定

バックアップタスクの成功/失敗/終了時に、Eメール通知を行えます。[Eメール通知を行う] のチェックボックスにチェックを入れます。[タスク失敗時] を選択すると、バックアップタスクがエラーなどで失敗した場合のみEメールで通知します。Eメール通知を行うには、あらかじめ[環境設定] → [Eメール通知設定] で送信設定をする必要があります。



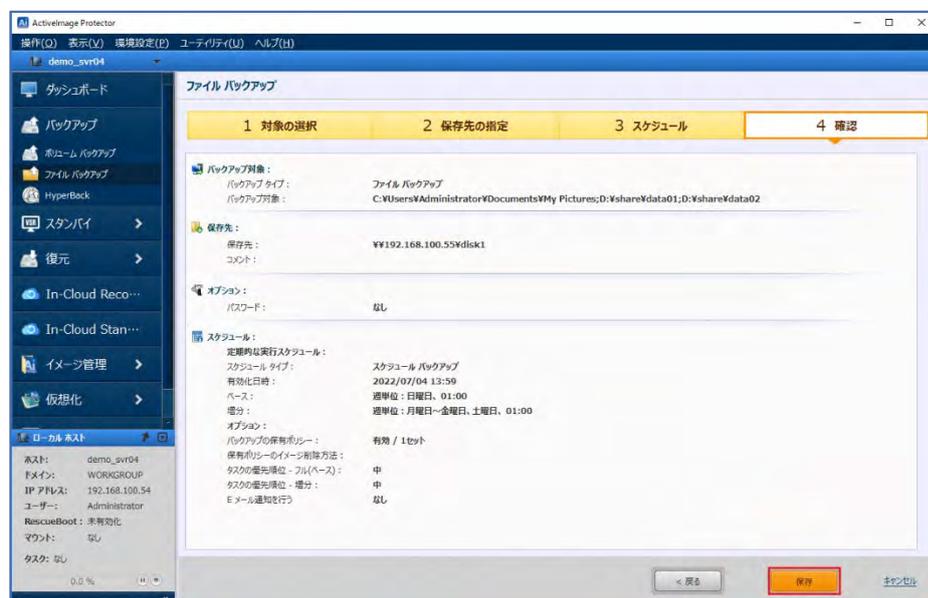
(3) E メール通知の環境設定

[環境設定] → [E メール通知設定] をクリックして、E メール通知の環境設定を起動します。すべての E メール通知設定が完了したら、[メールのテスト送信] を実行して正常動作を確認します。テストメールの送信が確認されたら、[適用] をクリックします。



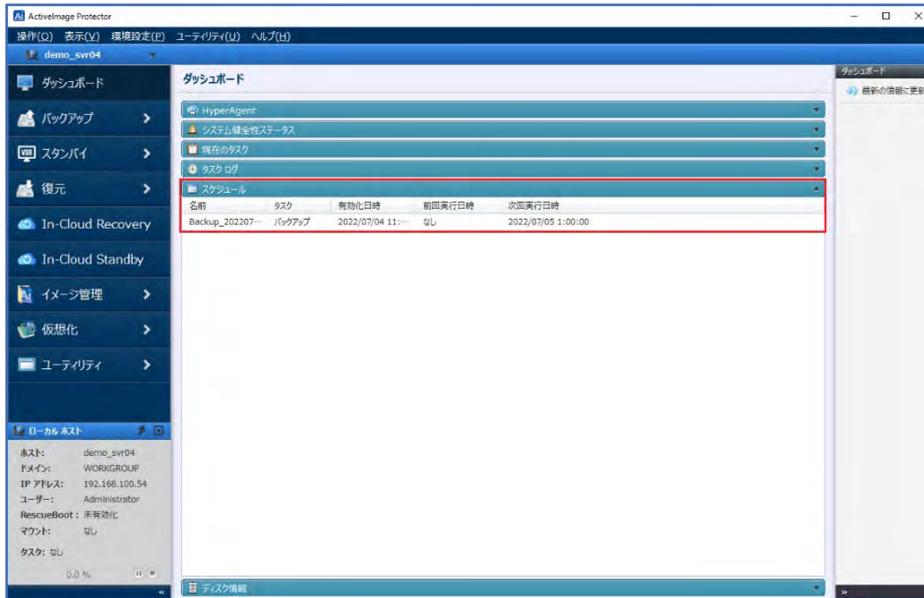
10. バックアップの内容が表示されます。

内容を確認してから [保存] をクリックすると、ダッシュボードに戻ります。

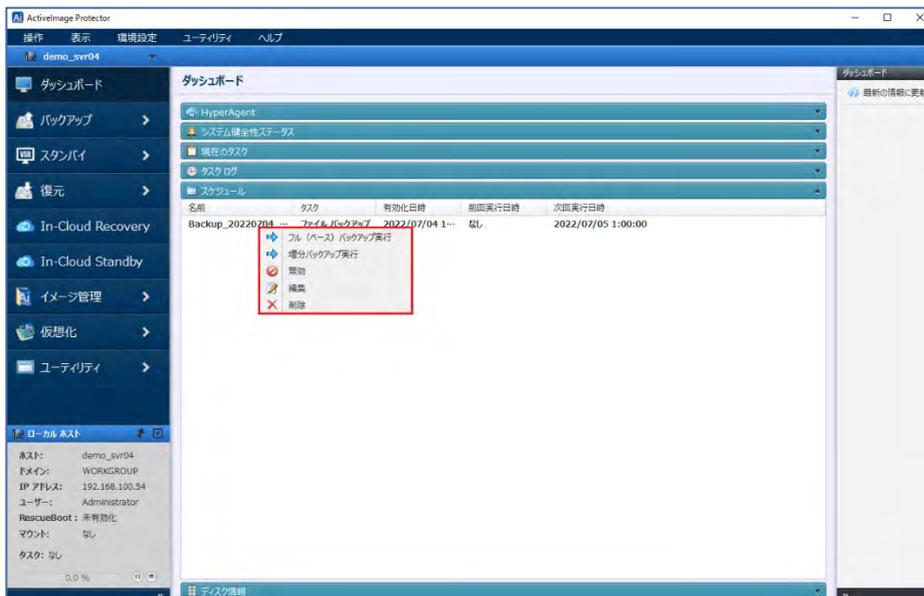


## バックアップの設定と実行

11. 作成済みのスケジュールは [ダッシュボード] → [スケジュール] で確認できます。指定した時刻になると、スケジュールバックアップが実行されます。



12. [スケジュール名] を右クリックすると、直ちにフルバックアップや増分バックアップの実行、スケジュールの編集などを行うことができます。



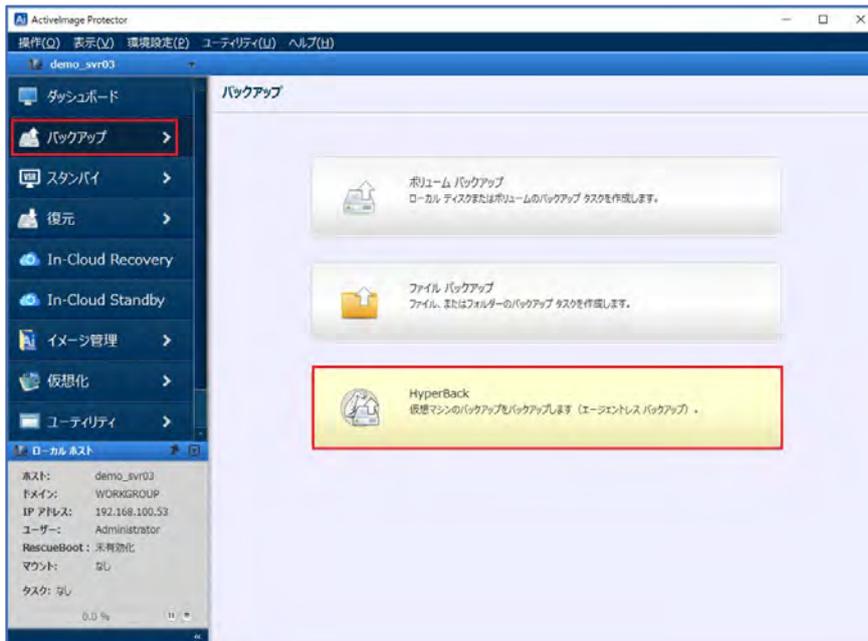
#### 4-4. エージェントレス バックアップ (HyperBack)

ハイパーバイザー (Microsoft Hyper-V、または VMware vSphere (ESXi)) 上の仮想マシンに、エージェントをインストールすることなくバックアップする、エージェントレス バックアップの設定手順について説明します。

1. ActiImage Protector を起動します。

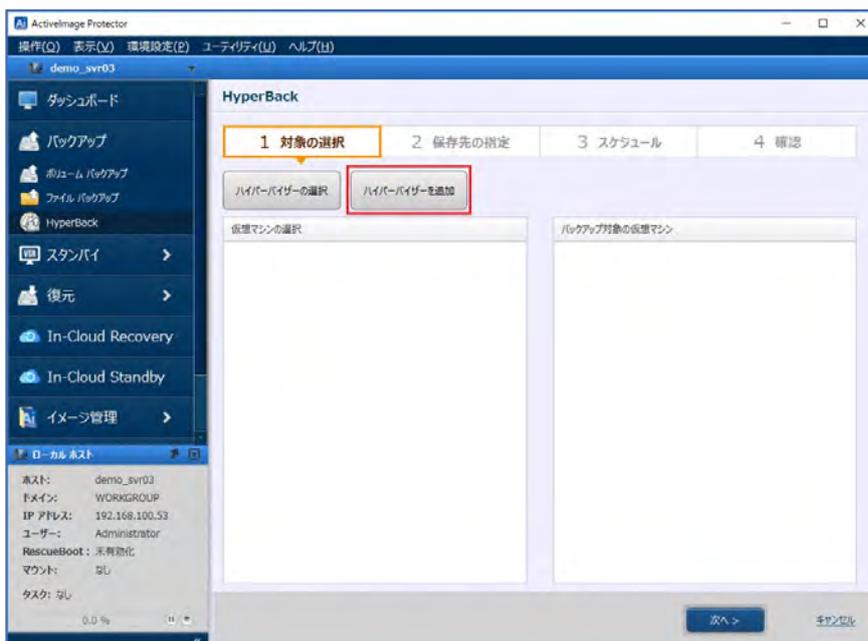
Windows スタートメニューから [Actipty] → [ActiImage Protector] をクリックします。

2. [バックアップ] → [HyperBack] をクリックします。



3. 最初に、バックアップ対象の仮想マシンが構成されているハイパーバイザーを登録します。

[ハイパーバイザーを追加] をクリックします。



4. [ハイパーバイザーを追加...] をクリックします。

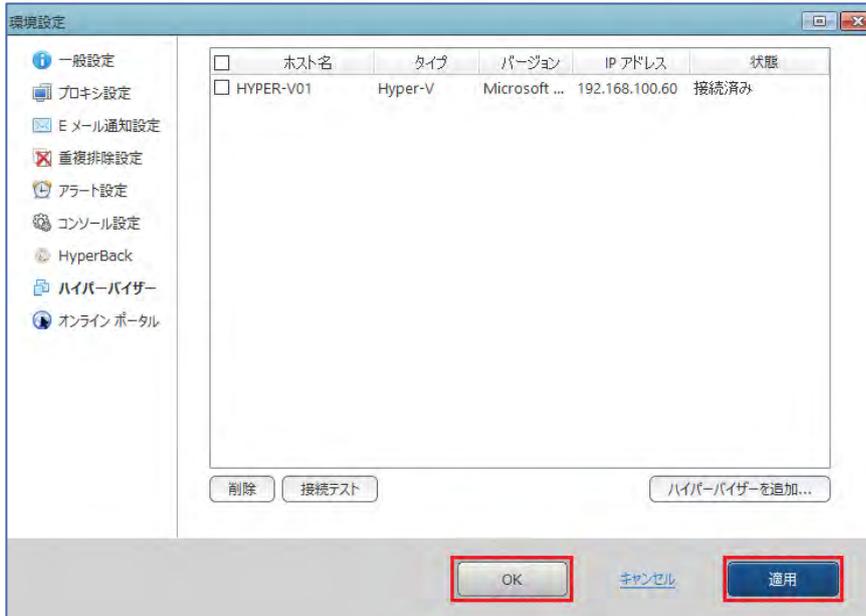


5. ハイパーバイザーを選択して、認証情報を入力します。  
 ここでの例として、[ハイパーバイザータイプ:] に「Microsoft Hyper-V」を選択し、[ホスト名、または IP アドレス:] に Hyper-V ホストの IP アドレス「192.168.100.60」、[ユーザー名:] に「Administrator」、[パスワード:] に設定されているパスワードを入力してから、[OK] をクリックします。

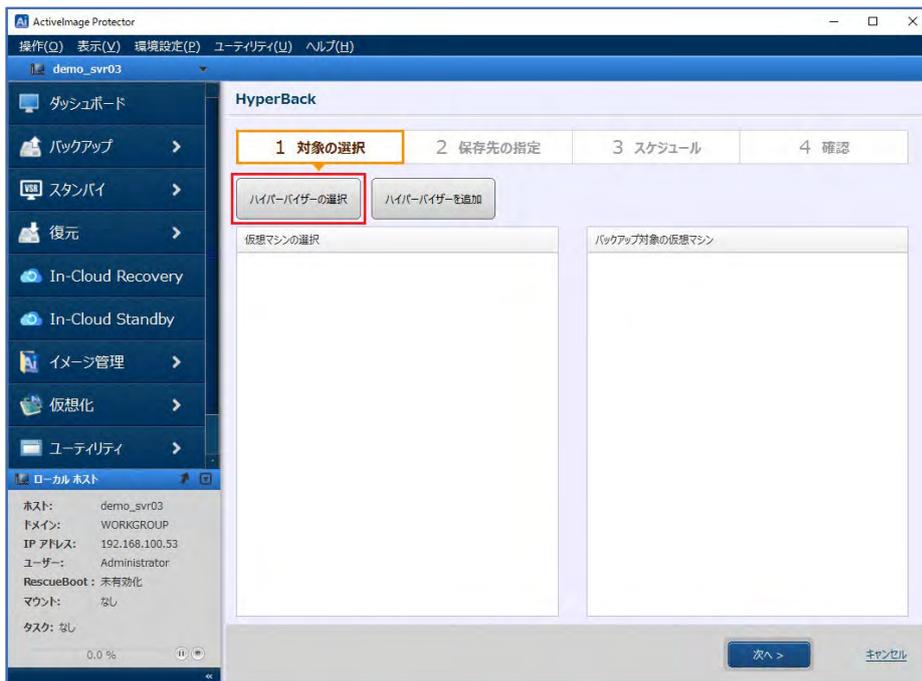


## バックアップの設定と実行

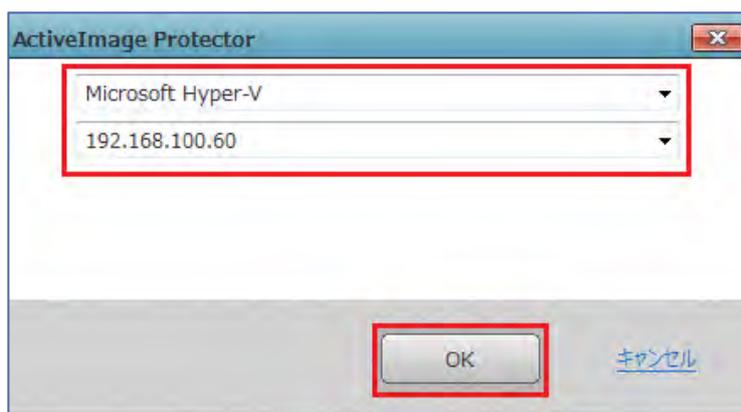
6. ハイパーバイザーの登録を確認し、[適用] をクリックしてから、[OK] をクリックすると [HyperBack] の設定画面に戻ります。ハイパーバイザーの登録は完了です。



7. 登録したハイパーバイザーを選択します。[ハイパーバイザーの選択] をクリックします。

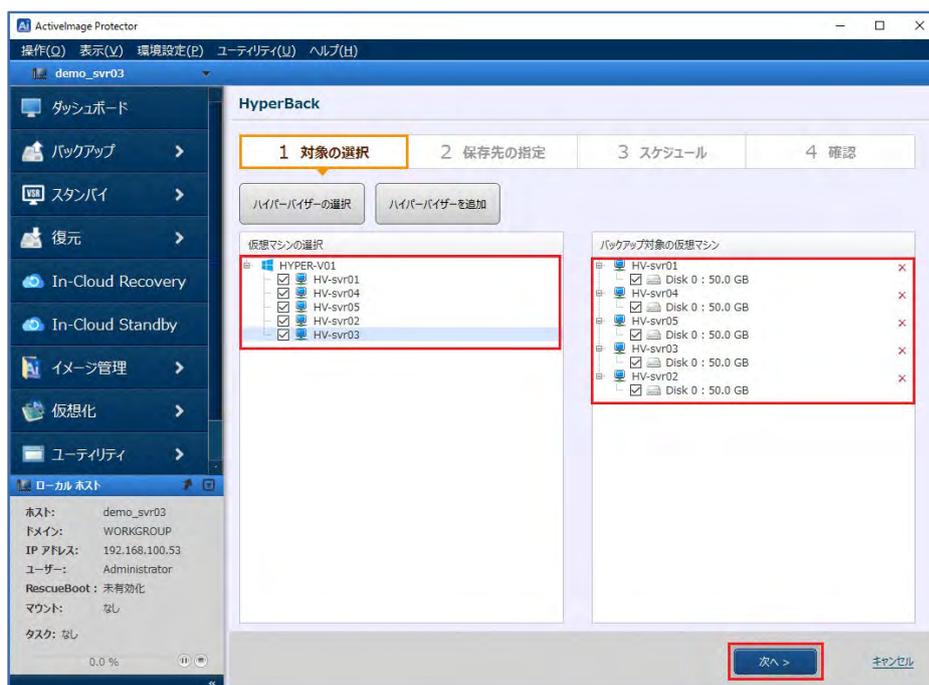


8. 登録したハイパーバイザーを選択してから、[OK] をクリックします。



9. バックアップ対象の仮想マシンを選択します。

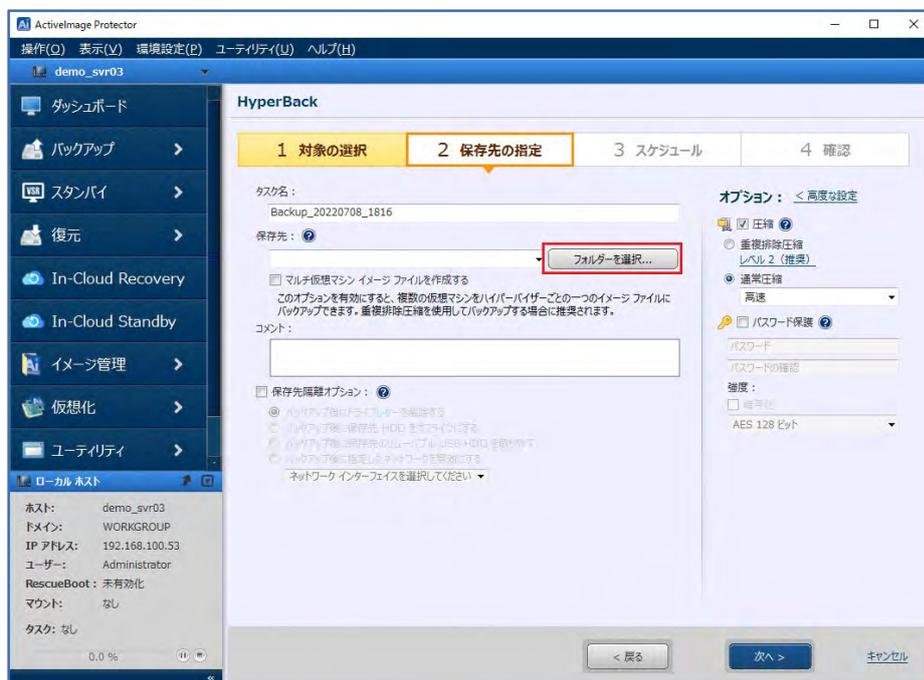
バックアップ対象の仮想マシンのチェックボックスにチェックを入れると、右側の「バックアップ対象の仮想マシン」のリストに追加されますので、確認後に、[次へ] をクリックします。複数の仮想マシンのバックアップの並行実行の数は、デフォルトでは「5」となっています。HyperBack オプションの設定は、次項 (P.42) を参照してください。



## バックアップの設定と実行

### 10. バックアップの保存先を指定します。

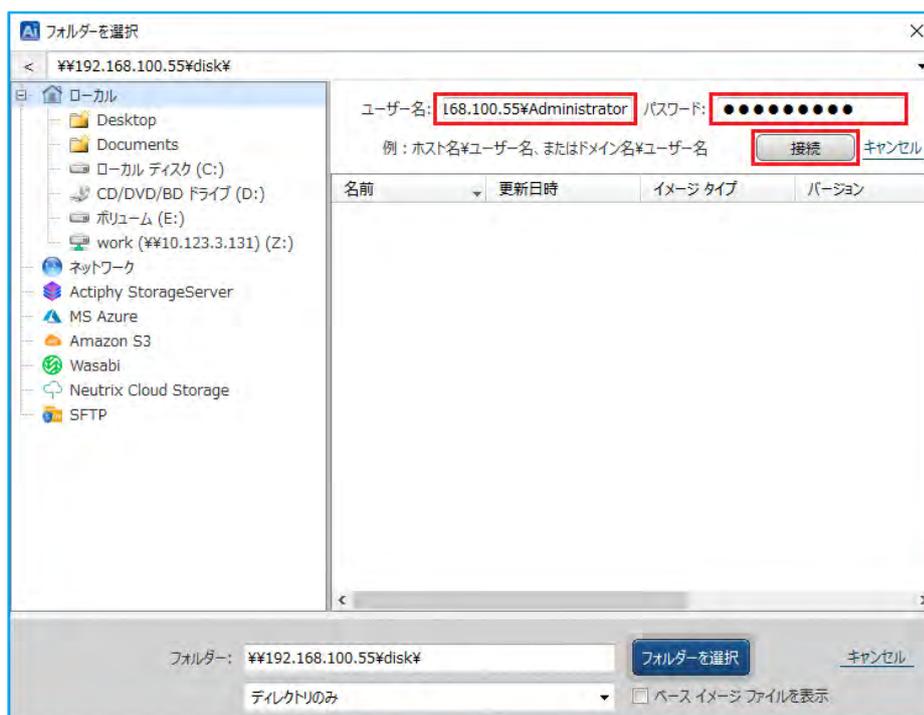
ここでの例として、ネットワーク共有フォルダーの「¥¥192.168.100.55¥disk」を保存先として説明します。  
[フォルダーを選択] をクリックします。



### 11. 保存先の共有フォルダーを指定します。

下記の場所に保存先の直接パス「¥¥192.168.100.55¥disk」を入力し、Enter キーを押します。次に、保存先に対する認証情報を入力します。

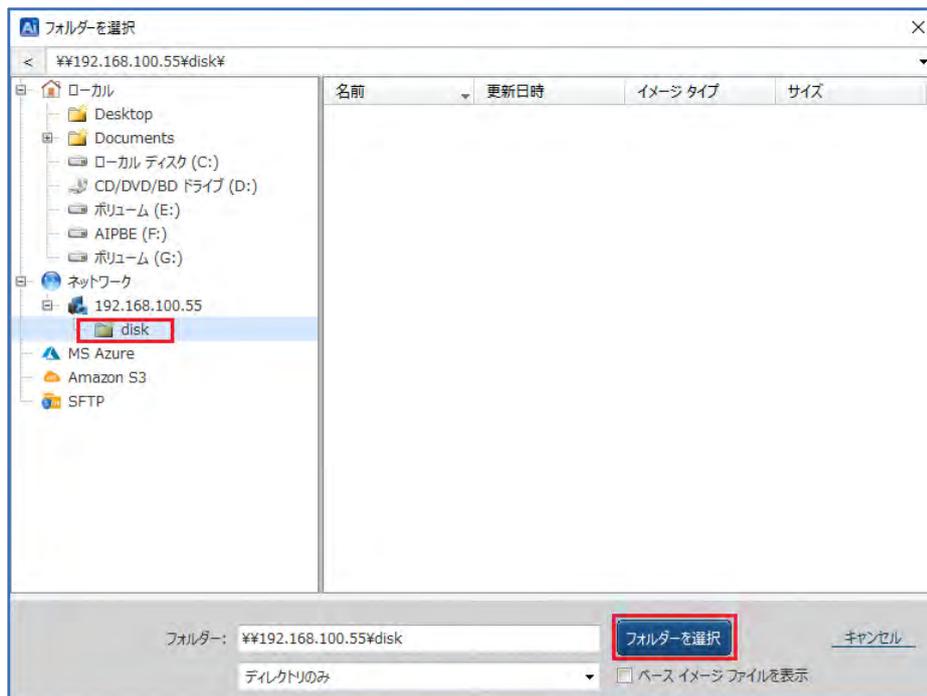
ここでの例として、[ユーザー名:] に「192.168.100.55¥Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。



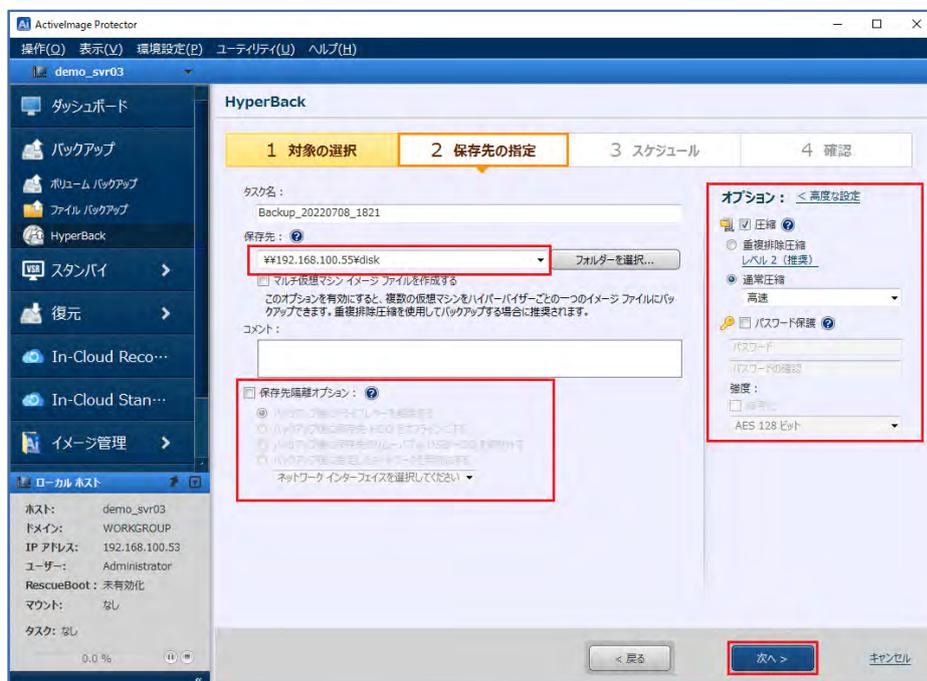
## バックアップの設定と実行

12. 保存先の共有フォルダーを登録します。

保存先の共有フォルダーを指定してしてから、[フォルダーを選択] をクリックします。



13. 保存先の共有フォルダーが登録されていることを確認後に、[次へ] をクリックします。「保存先隔離オプション」、「オプション」の設定は、次項(P.43)を参照してください。



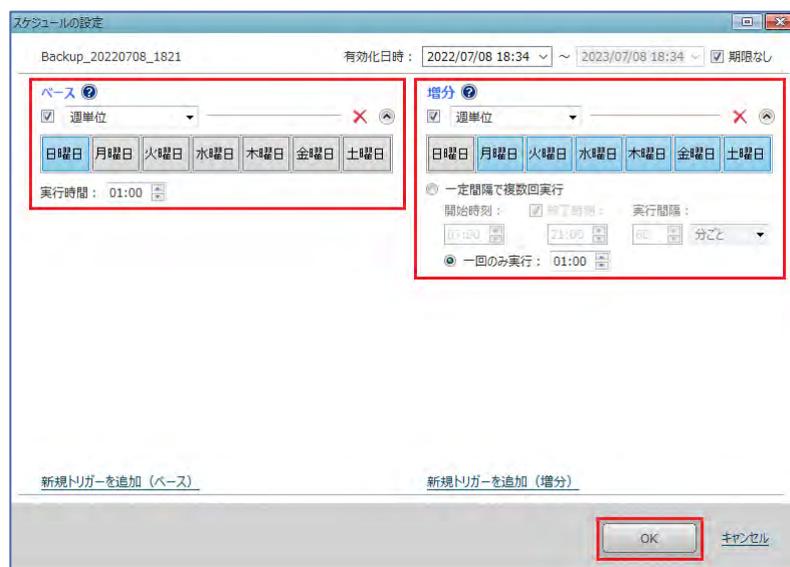
## バックアップの設定と実行

### 14. バックアップのスケジュール設定を行います。

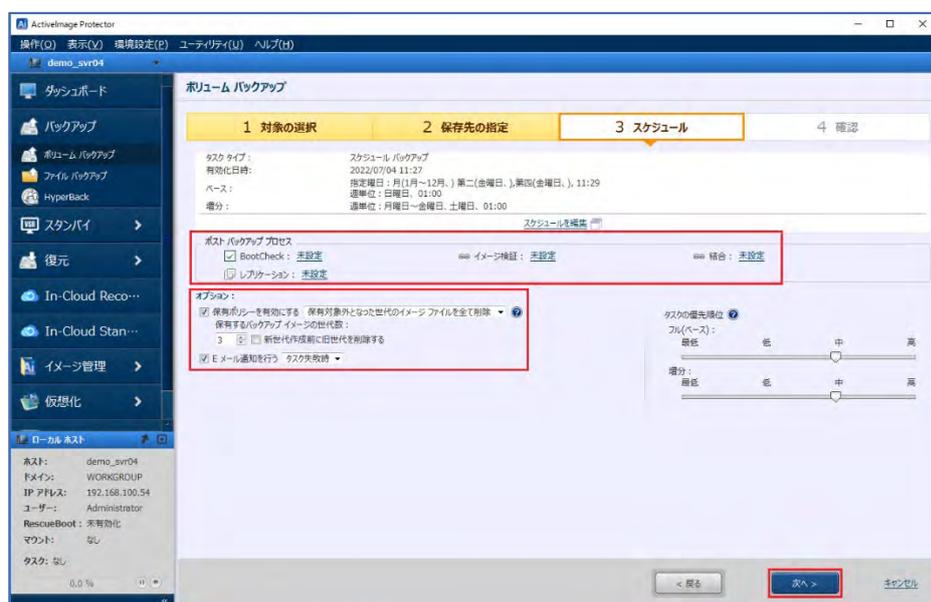
ここでの例として、下記の設定で週単位のバックアップスケジュールを作成します。

- ・ ベースバックアップ：週単位
- ・ 増分バックアップ：週単位
- ・ ベースバックアップ：日曜日の午前1時
- ・ 増分バックアップ：月曜日から土曜日までの午前1時

タスク タイプに [スケジュールバックアップ] を選択して、すべての項目を設定したら、[OK] をクリックします。



### 15. [スケジュール] タブでは、[保有ポリシーの設定]、[Eメール通知] を設定してから、[次へ] をクリックします。「ポストバックアッププロセス」の設定は、次項 (P.45) を参照してください。

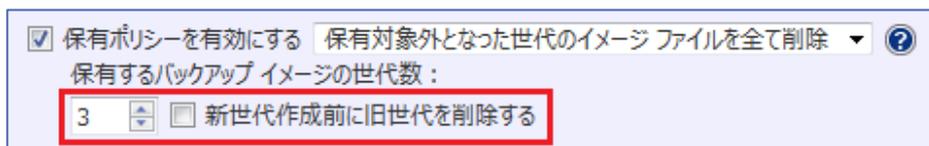


(1) 保有ポリシーの設定

バックアップ保存先に残すバックアップの世代数を設定します。

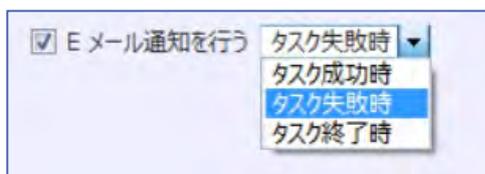
ここでの例として、[保有ポリシーを有効にする]のチェックボックスにチェックを入れます。[保有するバックアップの世代数:]をデフォルト設定の「3」にします。この設定で、バックアップの保存先に3世代分のバックアップが残ります。

※ ActiveImage Protector は、ベースバックアップとそれに紐づく増分バックアップを1世代として管理しています。



(2) Eメール通知の設定

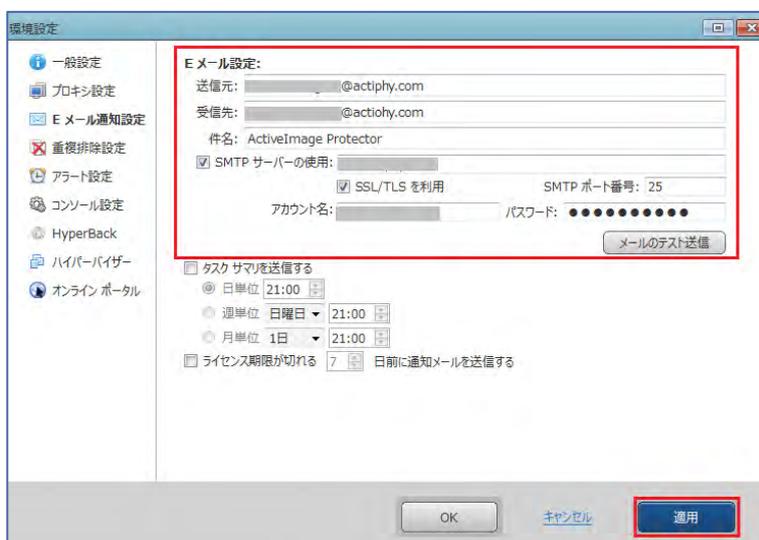
バックアップタスクの成功/失敗/終了時に、Eメール通知を行えます。[Eメール通知を行う]のチェックボックスにチェックを入れます。[タスク失敗時]を選択すると、バックアップタスクがエラーなどで失敗した場合のみEメールで通知します。Eメール通知を行うには、あらかじめ[環境設定]の[Eメール通知設定]で送信設定をする必要があります。



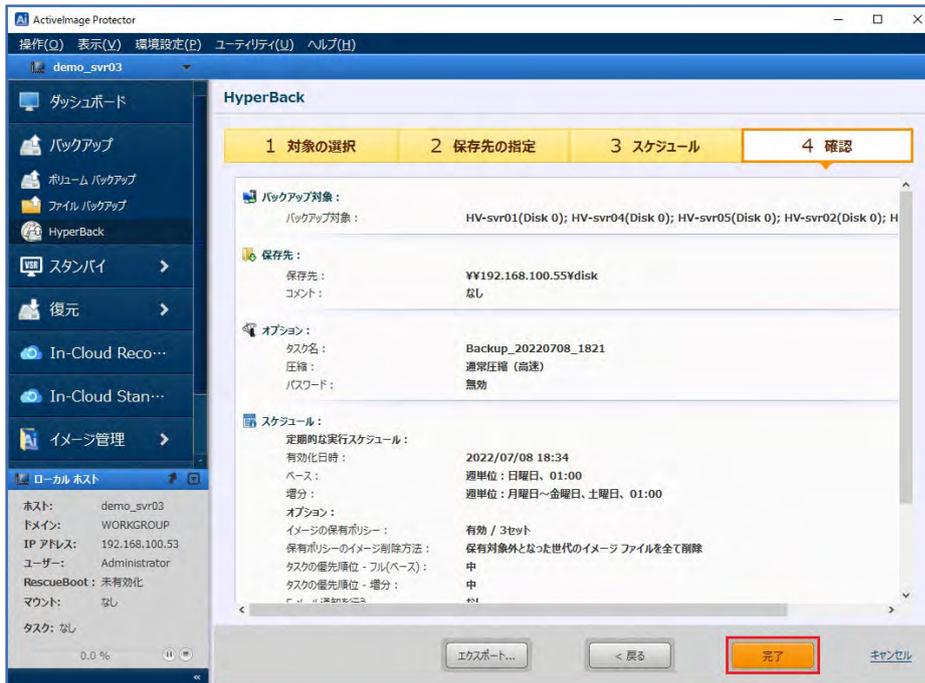
(3) Eメール通知の環境設定

[環境設定] → [Eメール通知設定] をクリックして、Eメール通知の環境設定を起動します。

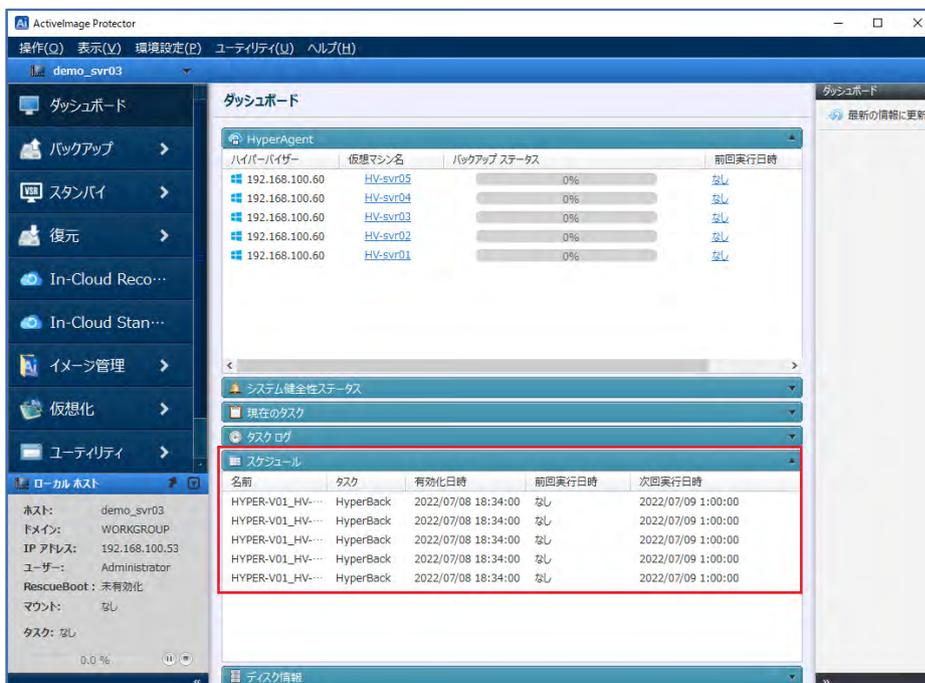
すべてのEメール通知設定が完了したら、[メールのテスト送信]を実行して正常動作を確認します。テストメールの送信が確認されたら、[適用]をクリックします。



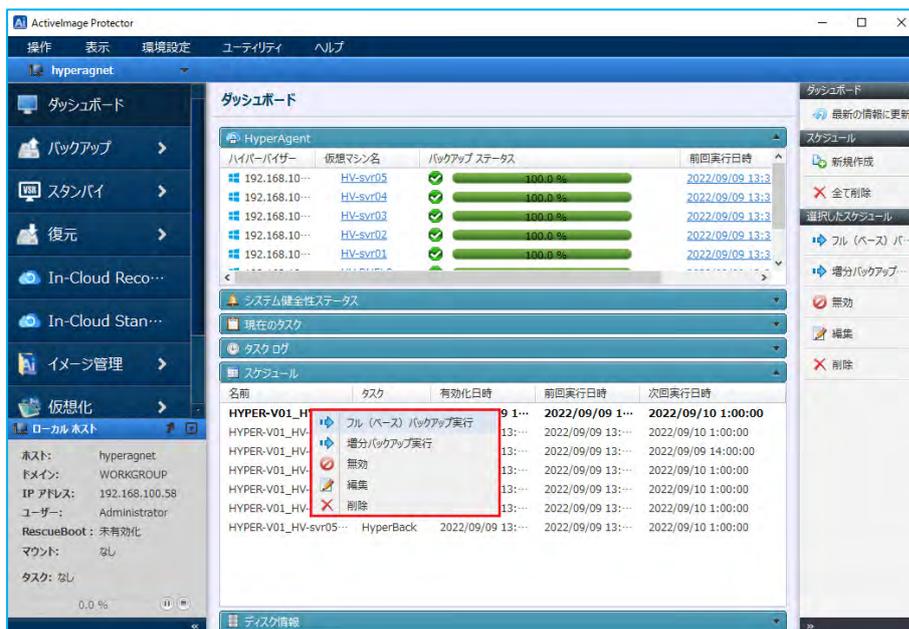
16. バックアップの内容が表示されます。  
 内容を確認してから [保存] をクリックすると、ダッシュボードに戻ります。



17. 作成済みのスケジュールは [ダッシュボード] → [スケジュール] で確認できます。仮想マシンごとに、スケジュールが作成されます。指定した時刻になると、仮想マシンごとにスケジュールバックアップが実行されます。

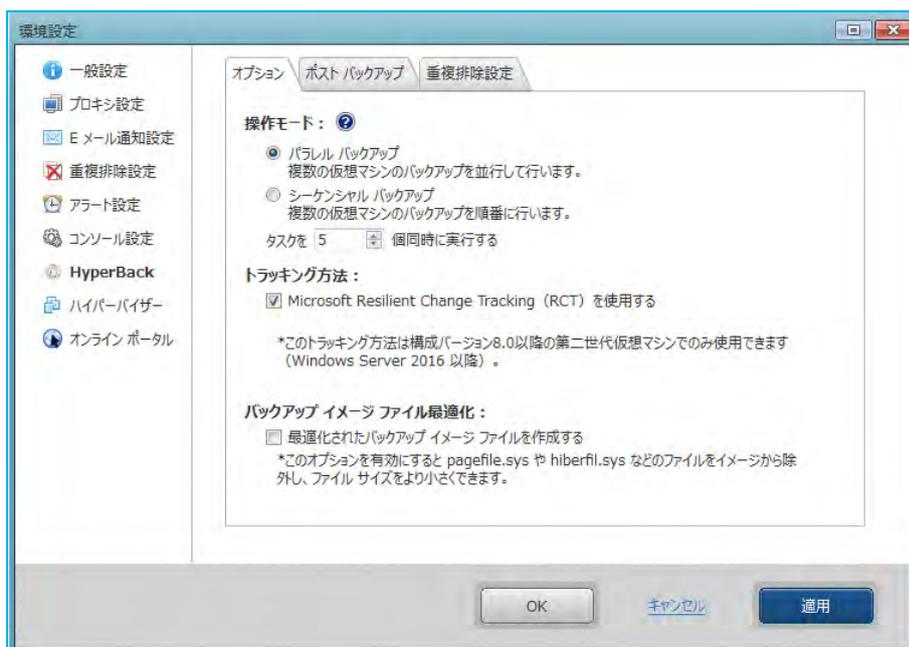


18. [スケジュール名] を右クリックすると、直ちにフルバックアップや増分バックアップの実行、スケジュールの編集などを行うことができます。



### 19. HyperBack オプションの設定

コンソールメニューから [環境設定] → [HyperBack] をクリックすると、HyperBack のオプションを設定することができます。「操作モード」は、複数の仮想マシンのバックアップを並行して行うか、順番にひとつずつ行うかの設定です。「HyperAgent」が導入されたコンピューターのマシンリソース、ネットワークリソースに余裕がない時には「シーケンシャル バックアップ」を推奨します。「トラッキング方法」は仮想マシンの増分作成の方法を指定します。Windows Server 2016 以降、第二世代仮想マシンでは Window に標準で搭載された RCT を使用します。それ以外は ActiVimage 独自の方法で増分を作成します。



## 20. [保存先隔離オプション] の設定

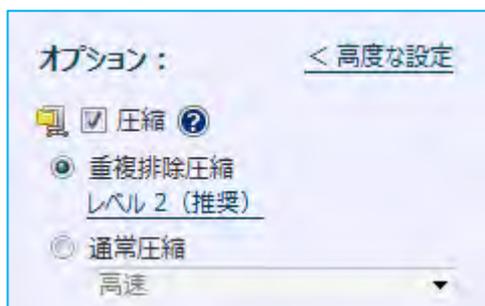
保存先隔離オプションは、バックアップ作業の終了後に、バックアップ保存先ディスクのマウントの解除やネットワークの遮断を行う機能です。ランサムウェアなどのウイルスの攻撃からバックアップ保存先やバックアップファイルを保護します。保存先隔離オプションには、以下の4つのオプションが用意されています。



## 21. [オプション] の設定

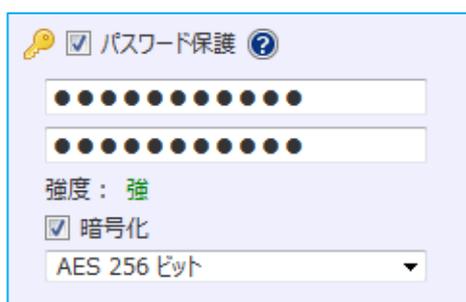
### (1) 圧縮レベルの設定

標準設定の通常圧縮と重複排除圧縮の2種類の圧縮方式をサポートします。圧縮率は、データの種類により異なりますが、通常圧縮で70%、重複排除圧縮では50%程度を目安としてください。画面の右の[オプション:] から指定します。重複排除圧縮を選択すると、その下の[レベル2 (推奨)] と重複排除処理の一時作業領域の[一時ファイルフォルダーを変更] の設定が可能になります。



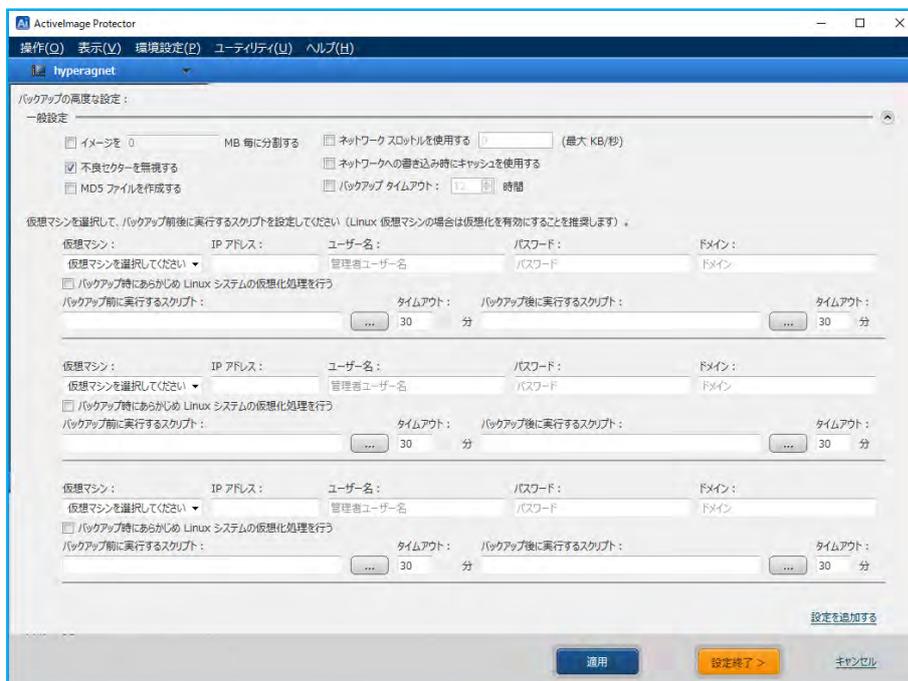
### (2) 暗号化の設定

バックアップファイルのパスワード保護と暗号化をサポートしています。[パスワード保護] にチェックを入れ、パスワードを入力します。次に、暗号化レベルの「RCS」、「AES128ビット」、「AES256ビット」から選択して設定します。バックアップファイルの外部サイト保管やサイバー攻撃からバックアップファイルを安全に保護します。



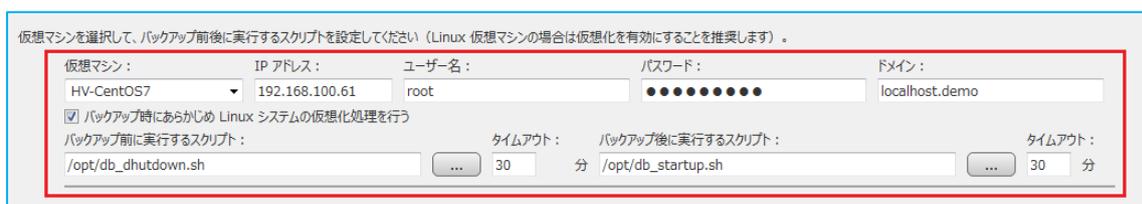
## 22. [高度な設定] の設定

オプション中の [高度な設定] では、バックアップファイルの分割、ネットワーク共有フォルダーに保存する際の帯域制御やキャッシュ使用、バックアップファイルの仮想化処理、バックアップ処理と連動したユーザー作成のスキプトの実行などの設定が可能です。ここでは、[スクリプト] について解説します。



### [スクリプトの設定:]

ユーザー作成のスクリプトなどを、バックアップ前後に自動実行することができます。例えば、VSS 非対応のデータベース・アプリケーションの場合は、バックアップデータの整合性を保つために、バックアップ開始前にサービスを停止する必要がありますが、バックアップ前後にサービス停止/起動のスクリプトを設定して自動実行することができます。



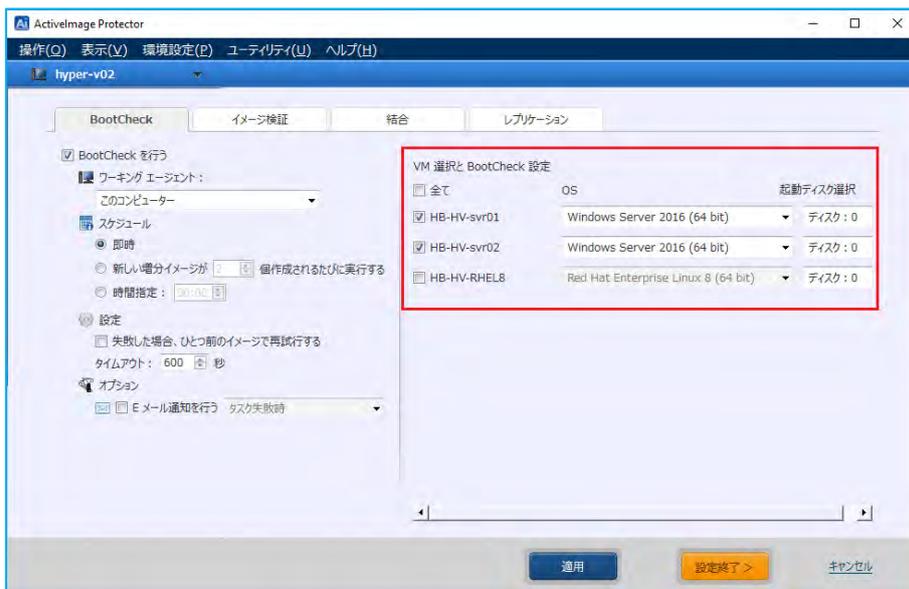
## 23. ポストバックアッププロセスの設定

[ポストバックアッププロセス] では、バックアップスケジュールと連動してバックアップファイルの [BootCheck]、[イメージ検証]、[結合]、[レプリケーション] の設定を必要に応じて行います。

### (1) BootCheck の設定

バックアップファイルが、起動可能か仮想マシンを使い確認します。[BootCheck を行う] にチェックを入れると、BootCheck が有効になります。実行するスケジュール、メール通知などを設定します。

※Linux 仮想マシンから取得したバックアップは、「BootCheck」には対応していませんので、Linux 仮想マシンにはチェックを入れないでください。



### (2) イメージ検証の設定

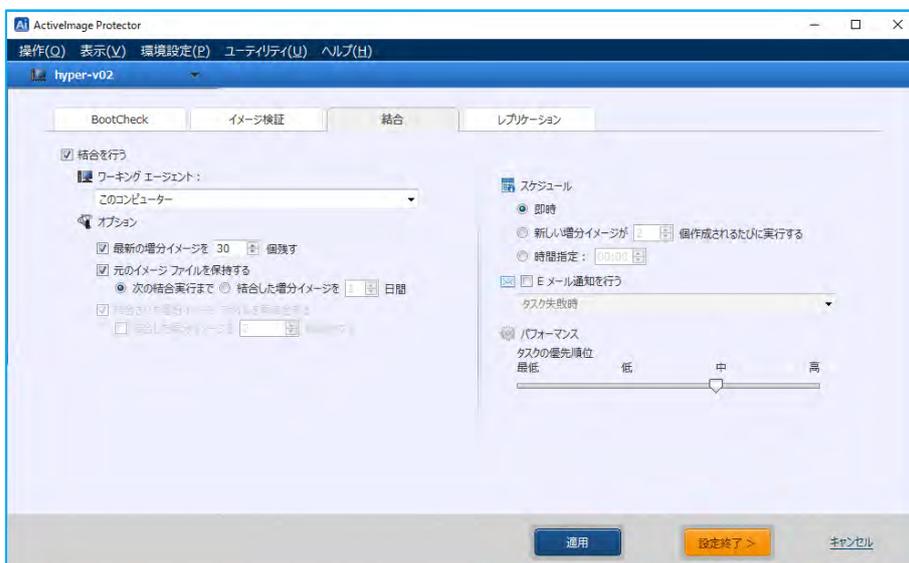
バックアップファイルの検証を行います。[イメージの検証を行う] にチェックを入れると、イメージ検証が有効になります。ここで、実行するスケジュールを設定します。



## バックアップの設定と実行

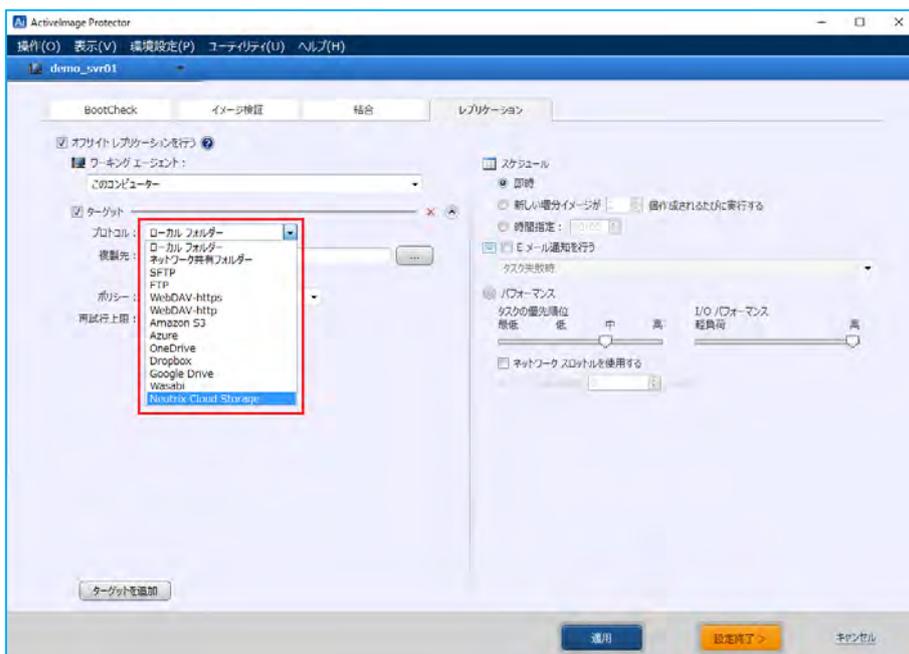
### (3) 結合の設定：

増分バックアップなどで、バックアップファイルが多数になった場合に、結合（コンソリデーション）してバックアップファイルを削減します。バックアップファイルの管理を容易にするための機能です。[結合を行う] にチェックを入れると有効になります。コンソリデーションを行うファイル数、実行するスケジュール、メール通知、パフォーマンスなどを設定します。



### (4) レプリケーションの設定

クラウドストレージなどを含め、任意の場所にレプリケーションを作成します。災害対策の基本の1つとして、バックアップデータを遠隔地に保存するという方法があります。レプリケーション先は、ローカルストレージ / 共有フォルダー / WebDAV / FTP やクラウドストレージ Amazon S3 / Azure Storage / OneDrive / Dropbox / Google Drive / Wasabi / Neutrix Cloud など幅広く対応しています。



## 5. 起動環境ビルダー

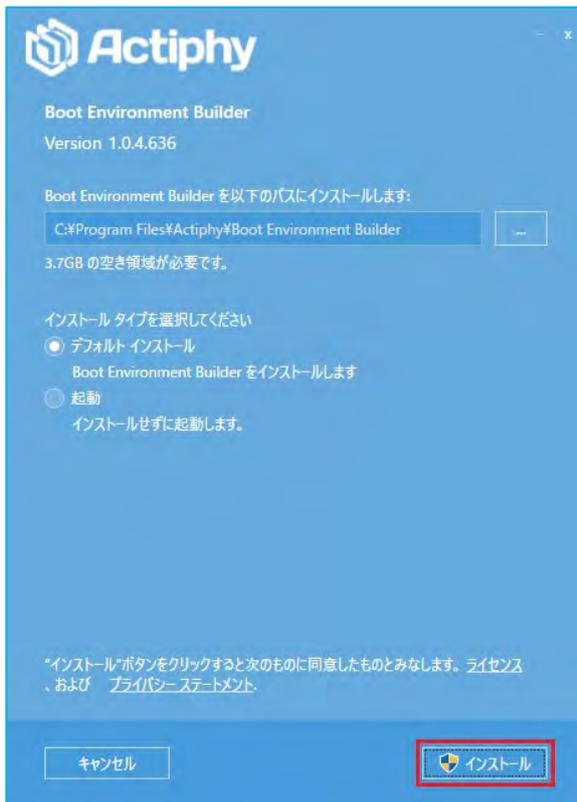
### Windows RE ベースの起動環境の作成

製品メディア自身が Linux ベースの起動環境になっていますので、基本的にはこちらを使用してください。標準の Linux ベースの起動環境から、ディスクやネットワークなどのデバイスが認識されない場合は、Windows ベース (Windows RE または Windows PE) の起動環境を作成して使用してください。

ここでの例として、Windows RE (Windows 回復環境) ベースの起動環境の作成方法について説明します。Windows RE ベースの起動環境を作成するには、起動環境作成ツール「Actiphy Boot Environment Builder」を、作業マシン (Windows 10 / Windows 11 / Windows Server 2016 以降) に導入してください。

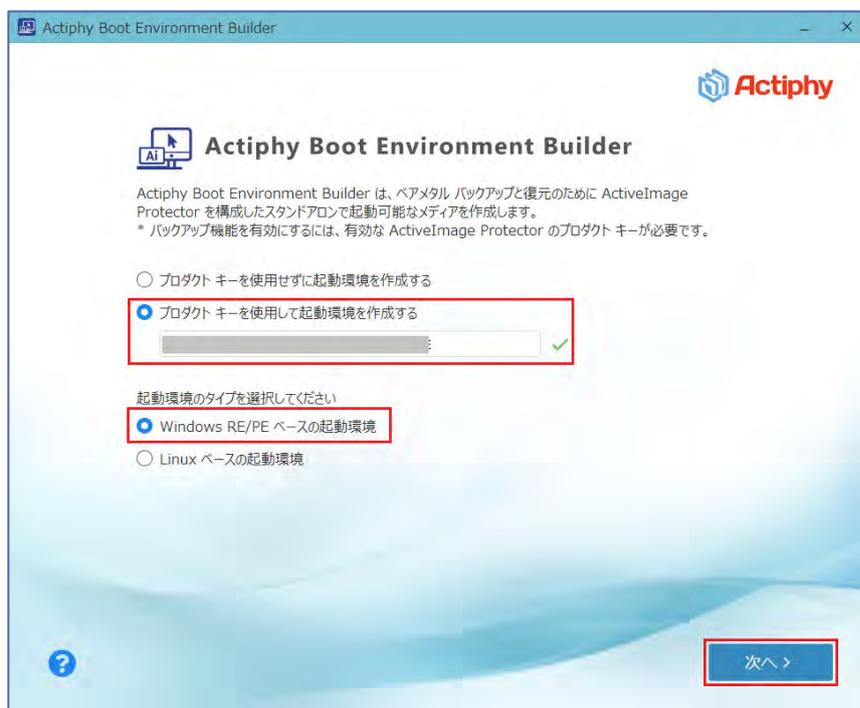
#### 1. Actiphy Boot Environment Builder をインストールします。

製品メディアから「Setup」フォルダー内の「BEBuilder.exe」を実行して、インストーラーを起動します。  
[インストール] をクリックするとインストールが開始されます。インストールが完了するとデスクトップ上に、Actiphy Boot Environment Builder のアイコンが作成されます。



2. Actiphy Boot Environment Builder を起動します。

デスクトップ上の [Actiphy Boot Environment Builder] のアイコンをクリックして起動させます。起動したら、[プロダクトキーを使用して起動環境を作成する] を選択して、プロダクトキーを入力します。次に、[Windows RE/PE] を選択して、[次へ] をクリックします。



3. 起動環境の作成媒体を指定します。

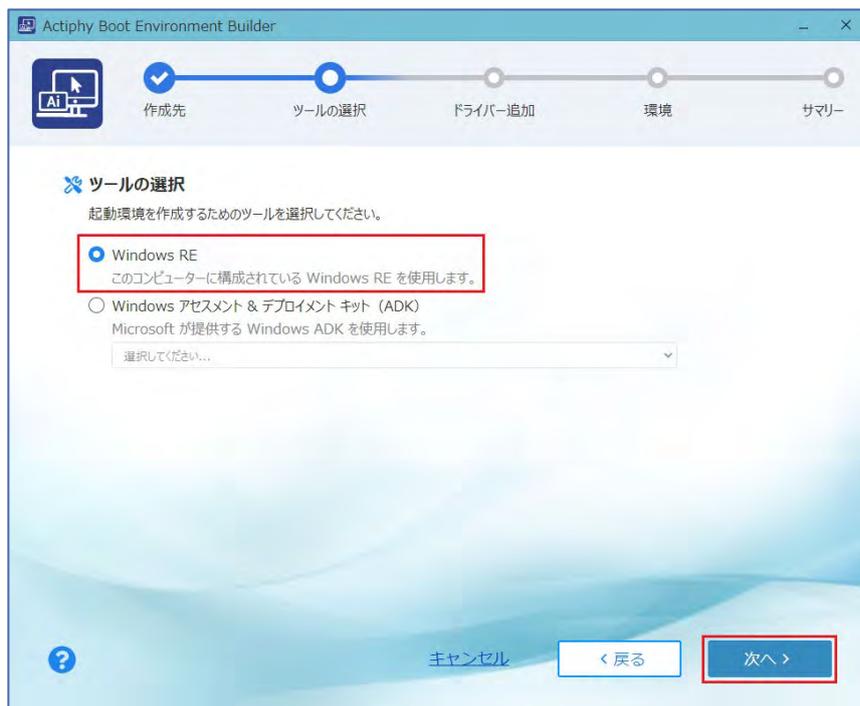
起動媒体は、DVD-R や ISO 形式、USB デバイスに作成することができます。

ここでの例として、USB メモリーに起動媒体を作成します。[USB デバイス] を選択して、作成する USB メモリーを選択してから、[次へ] をクリックしてください。



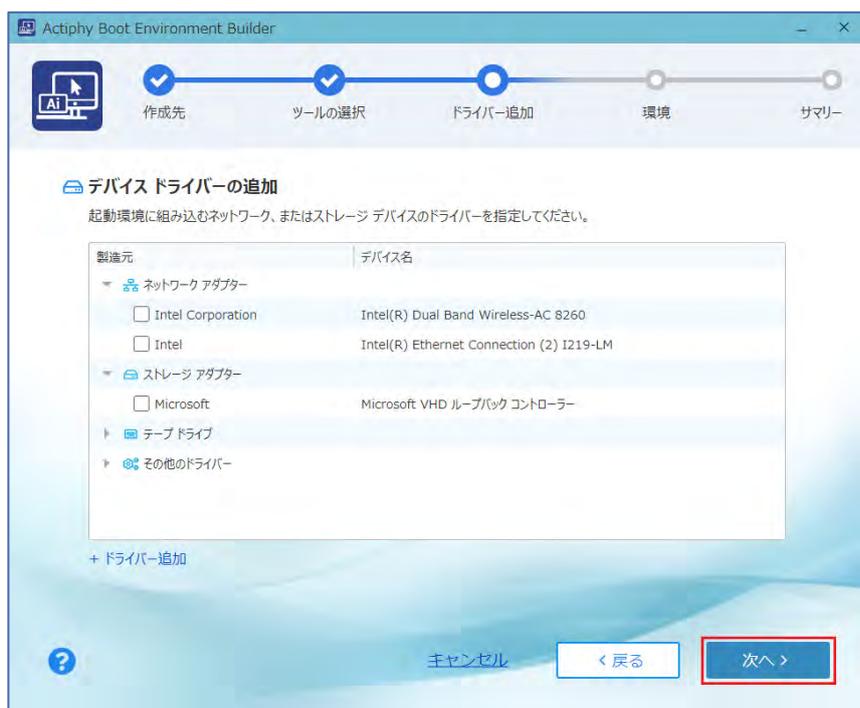
4. 起動環境のツールを指定します。

ツールの選択では、[Windows RE] を選択してから、[次へ] をクリックします。



5. 起動環境に組み込むデバイス ドライバーを選択します。

現在のシステムに存在するネットワークとストレージのドライバーが検出され表示されます。対象のドライバーのチェックボックスにチェックを入れると、作成される起動環境に組み込まれます。[ドライバー追加] をクリックすると、INF ファイルを指定して、一覧に無いドライバーを追加することもできます。対象のドライバーの追加が完了したら、[次へ] をクリックします。



## 起動環境ビルダー

6. 表示言語とキーボード タイプ、タイムゾーン、画面解像度を指定し、[次へ] をクリックします。



7. 設定内容を確認します。[戻る] をクリックすると前の設定画面に戻れます。また、ノードをクリックすることで任意の設定に戻ることができます。[起動環境の作成] をクリックすると確認メッセージが表示され、[OK] をクリックすると作成が開始されます。



8. 作成の進捗状況が表示されます。



9. 起動環境の作成が終了すると以下のメッセージが表示されます。[閉じる] をクリックして閉じてください。



## 6. リストア

### 6-1. ファイル/フォルダー単位のリストア

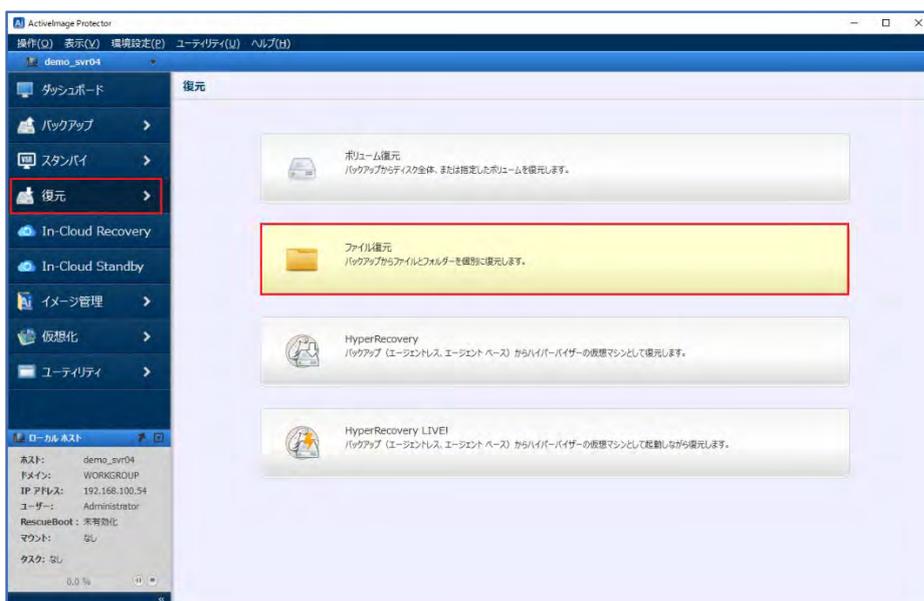
ディスク単位のバックアップからファイル/フォルダー単位のリストア手順について説明します。

ファイル/フォルダー単位のバックアップからのリストアも、基本的には同じ手順で行えます。

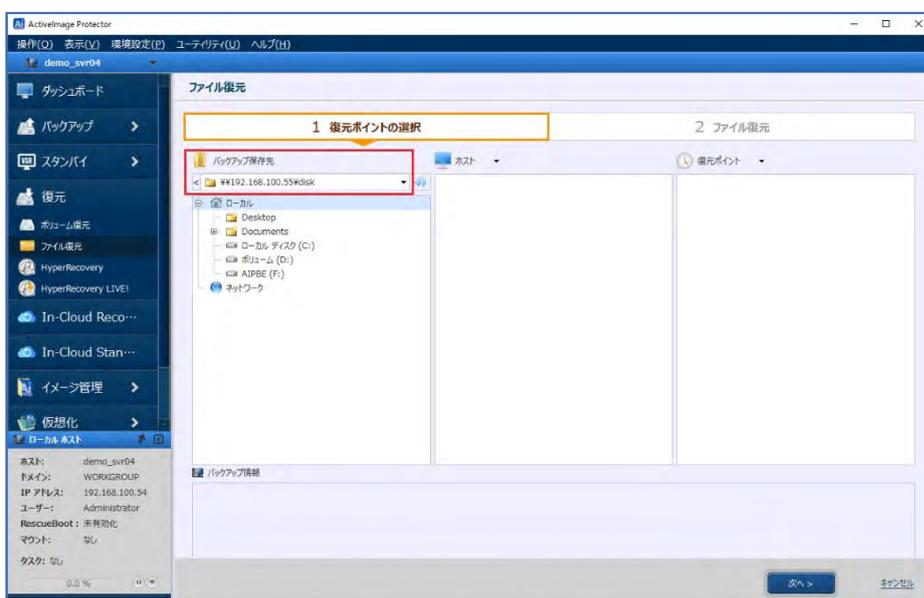
1. Activelmage Protector を起動します。

Windows スタートメニューから [Actiphy] → [Activelmage Protector] をクリックします。

2. [復元] → [ファイル復元] をクリックします。

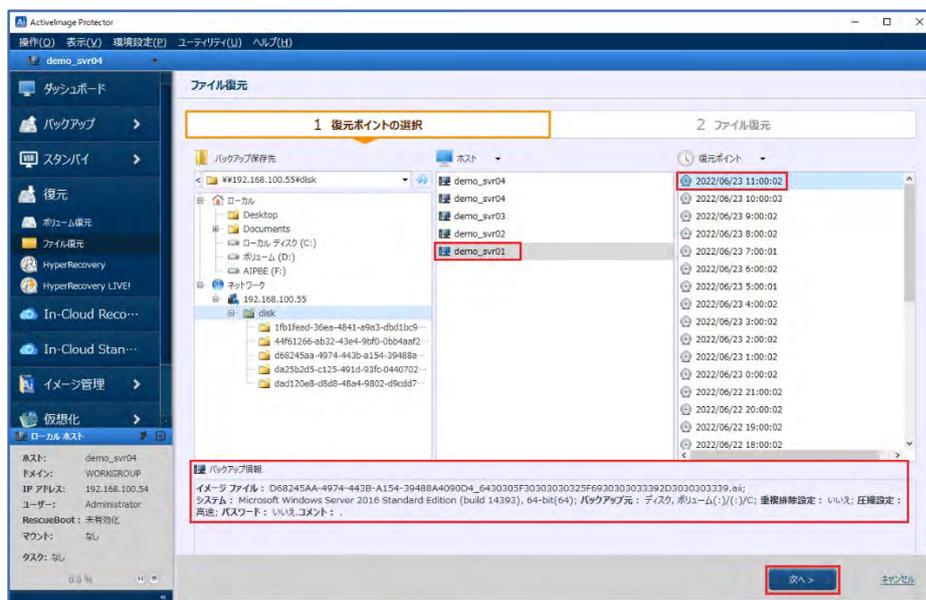


3. [バックアップ保存先] では、復元対象マシンのバックアップが保存されているフォルダーを選択します。ここでの例として、共有フォルダーのパス「¥¥192.168.100.55¥disk」を直接入力してから、Enter キーを押します。



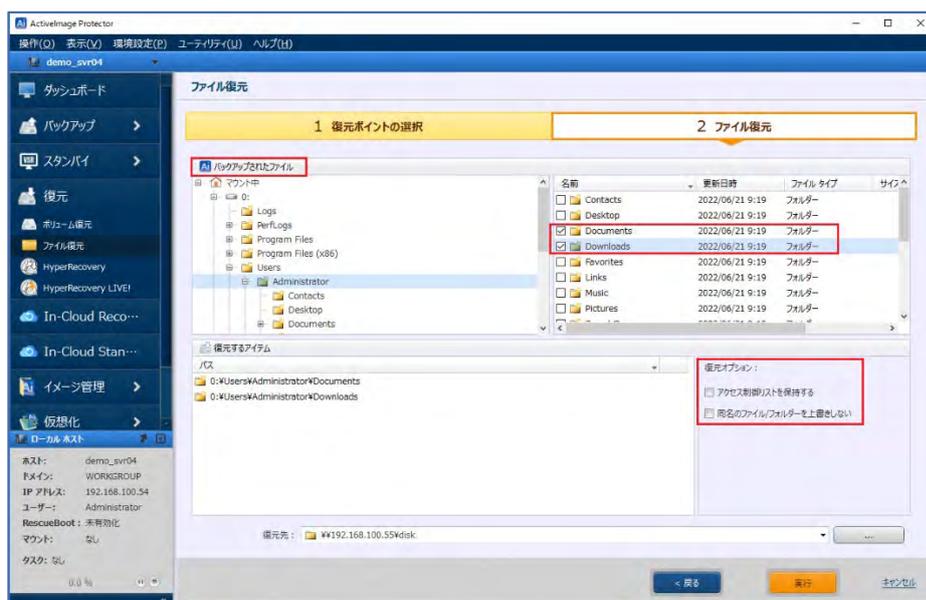
## リストア

4. 復元対象マシンを選択し、復元ポイントを指定したら [次へ] をクリックします。  
選択した復元ポイント (イメージ) の情報は [バックアップ情報] に表示されます。



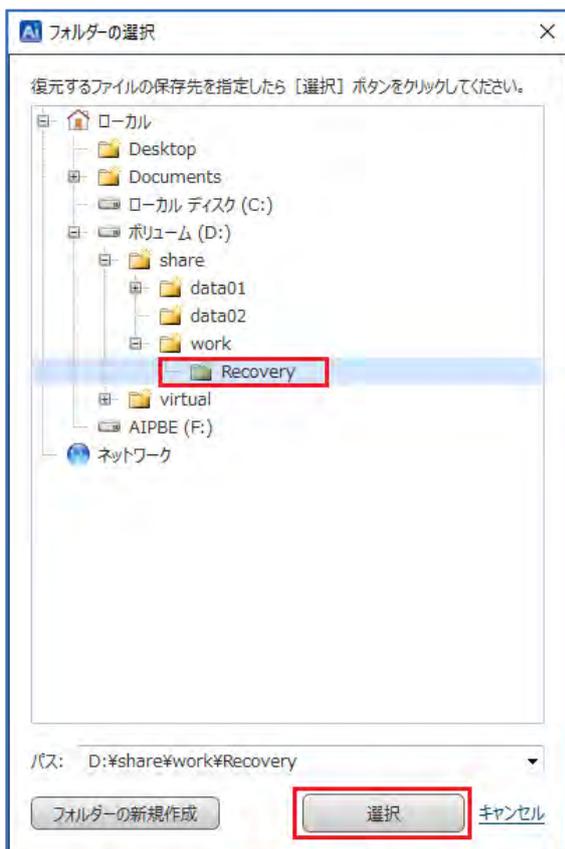
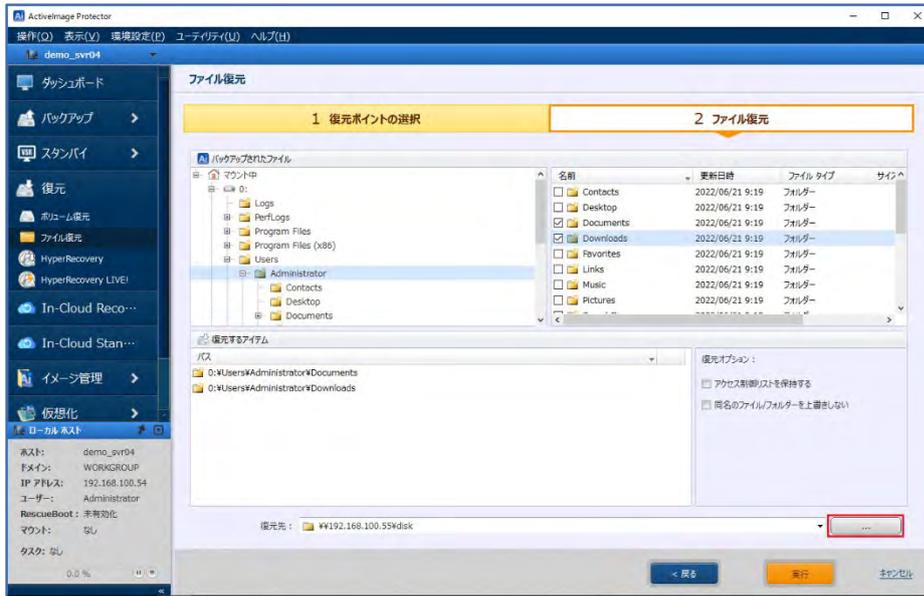
5. [バックアップされたファイル] から復元を行うアイテムのチェックボックスにチェックを入れます。  
チェックされたアイテムは [復元するアイテム] にリストされます。復元時のオプションとして以下を設定できます。

- アクセス制御リストを保持する：  
復元対象のファイルに設定されているアクセス制御リスト (ACL) を保持して復元します。
- 同名のファイル/フォルダーを上書きしない：  
保存先に同名のファイル/フォルダーがある場合、上書きせずに別名で復元します。



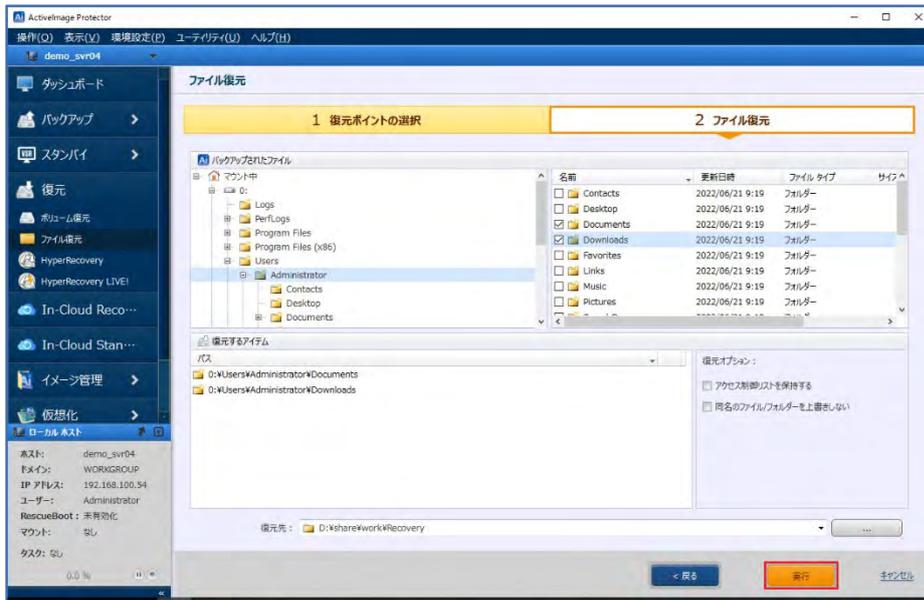
## リストア

6. 復元するアイテムの保存先を [...] (参照) から指定します。フォルダーを選択したら、[選択] をクリックします。

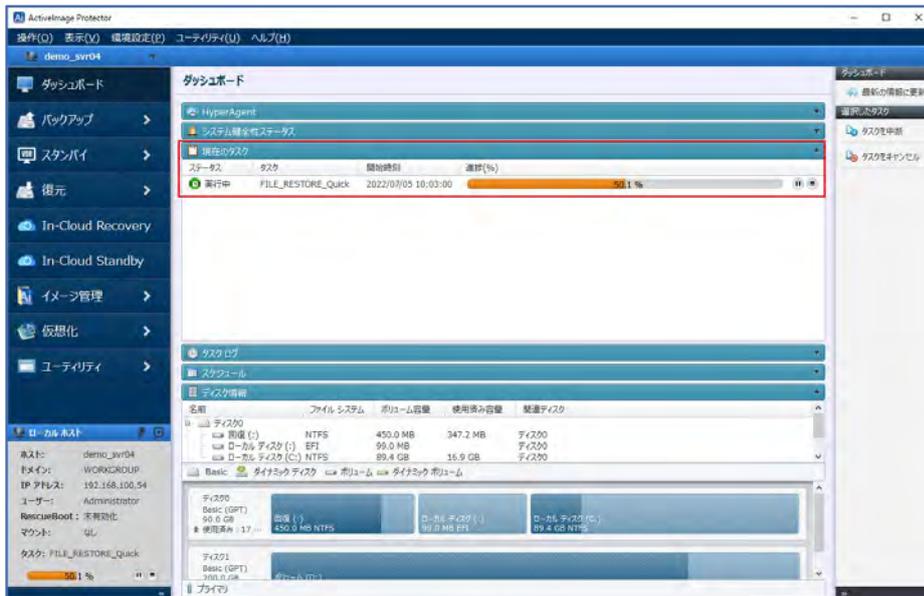


## リストア

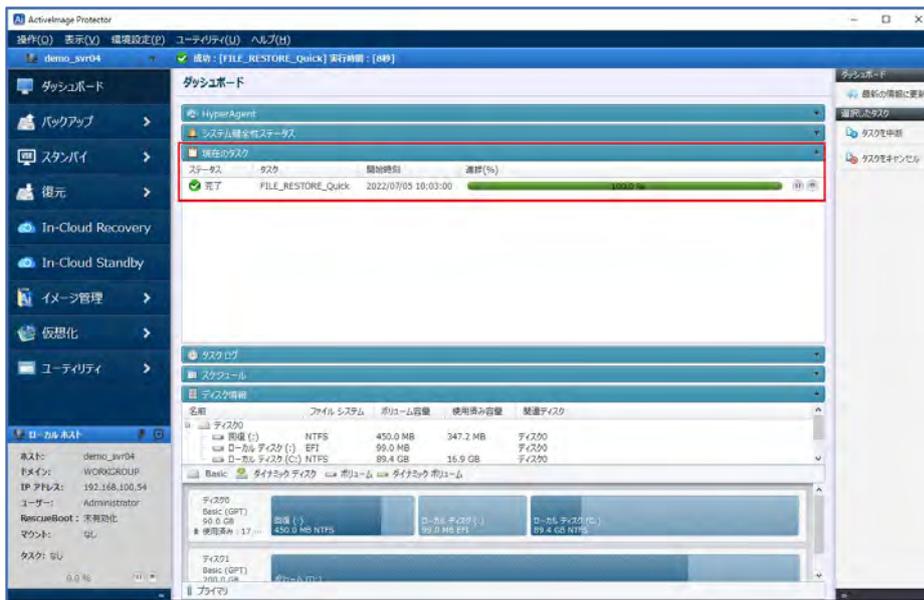
7. [実行] をクリックすると、リストアが開始されます。



8. リストア処理の進捗状況が表示されます。



9. タスクが 100%になれば、リカバリーの完了です。

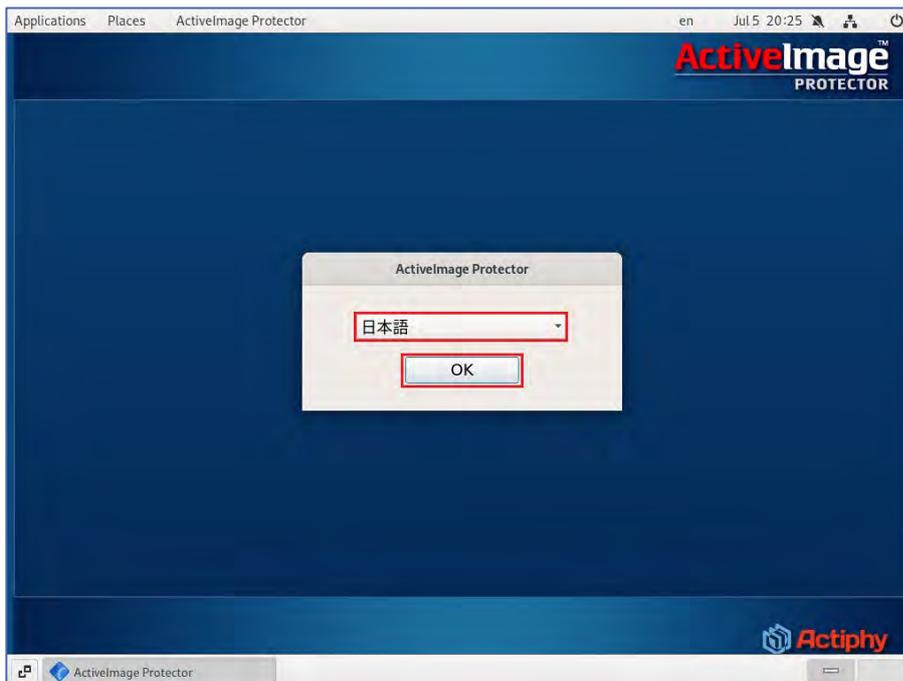


## 6-2. システムリカバリー：標準の Linux ベースの起動環境

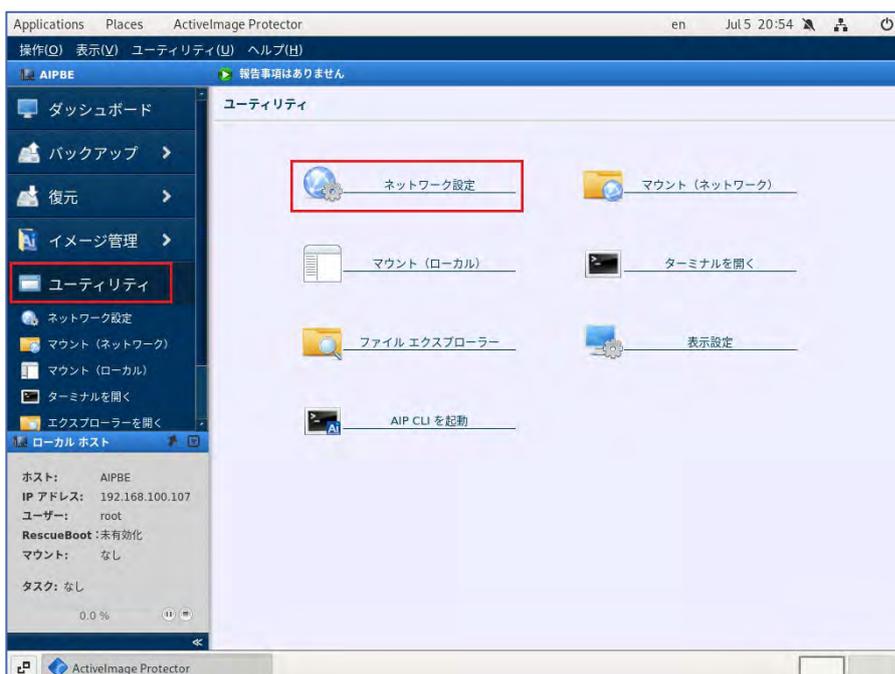
ActiveImage Protector の製品メディアを使用した、システムリカバリーの手順について説明します。

**注意：システムリカバリーを行うと、ローカルに存在するデータがすべて削除されますので、十分に注意して実行してください。**

1. 製品メディアをセットして、コンピューターをメディアから起動します。まず、表示言語に [日本語] を選択してから、[OK] をクリックします。

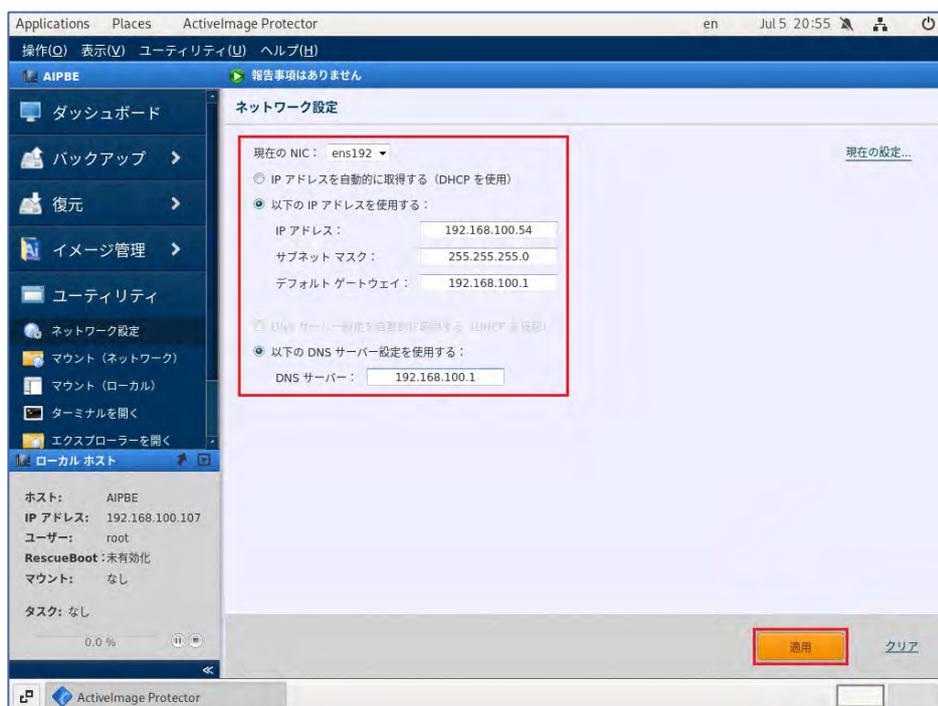


2. 保存先のネットワーク共有フォルダーにアクセスするためにネットワークの設定を行います。  
[ユーティリティ] から [ネットワーク設定] を選択します。

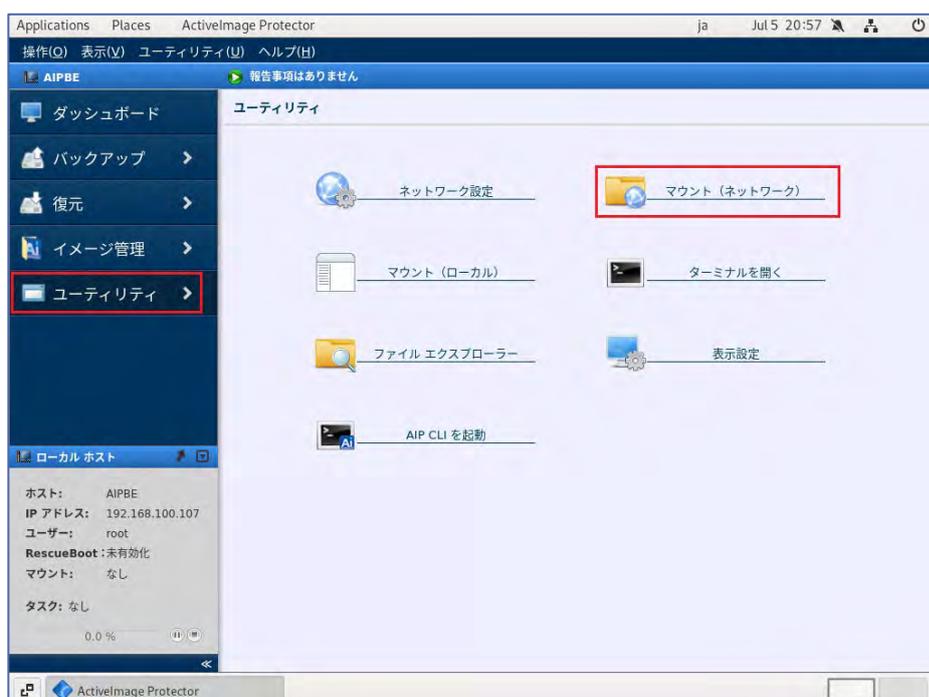


## リストア

- 保存先のネットワーク共有フォルダーにアクセスするためにネットワークの設定を行います。  
[以下の IP アドレスを使用する] を選択します。使用しているネットワークに合わせた設定を行います。  
ここでの例として、[IP アドレス:] に「192.168.100.54」、[サブネットマスク:] に「255.255.255.0」、  
[デフォルトゲートウェイ:] に「192.168.100.1」、[以下の DNS サーバー設定を使用する] を選択し、  
「192.168.100.1」を入力します。[適用] をクリックし、[OK] でネットワーク設定を終了します。

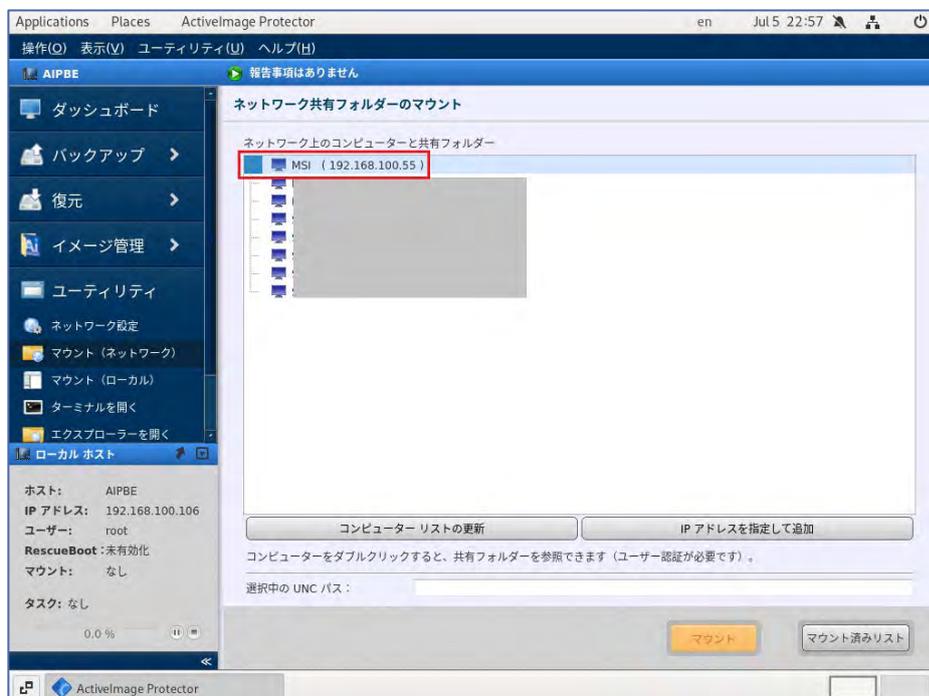


- 保存先のネットワーク共有フォルダーをマウントします。  
[ユーティリティ] から [マウント (ネットワーク)] を選択します。



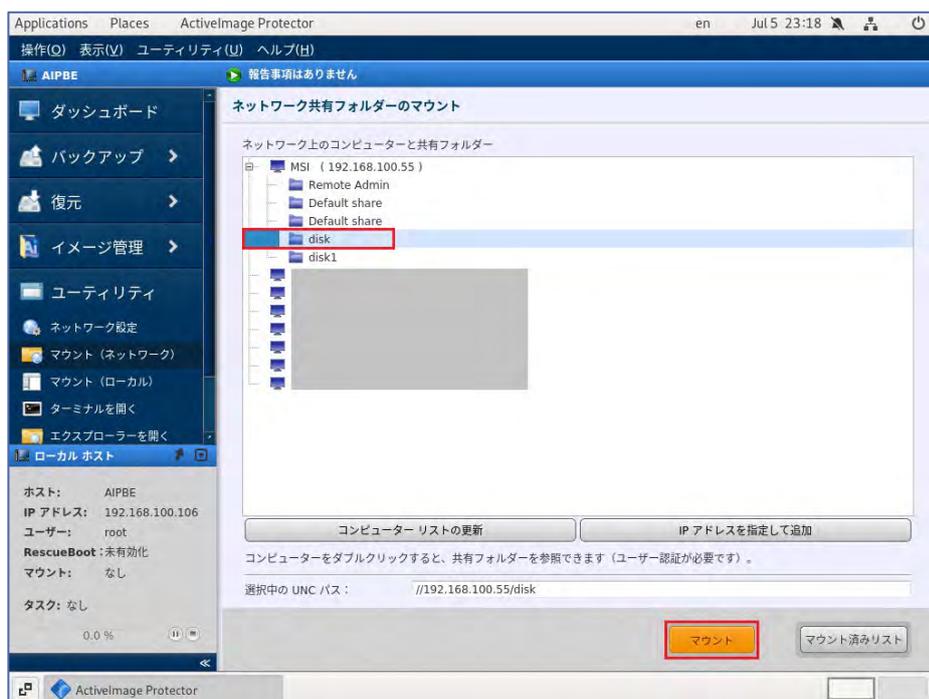
5. 共有フォルダーを参照します。

ネットワーク上のコンピューターが表示されますので、保存先の共有フォルダーが配置されているコンピューターをダブルクリックします。ユーザー認証が行われますので、[ユーザー名]と[パスワード]を入力します。



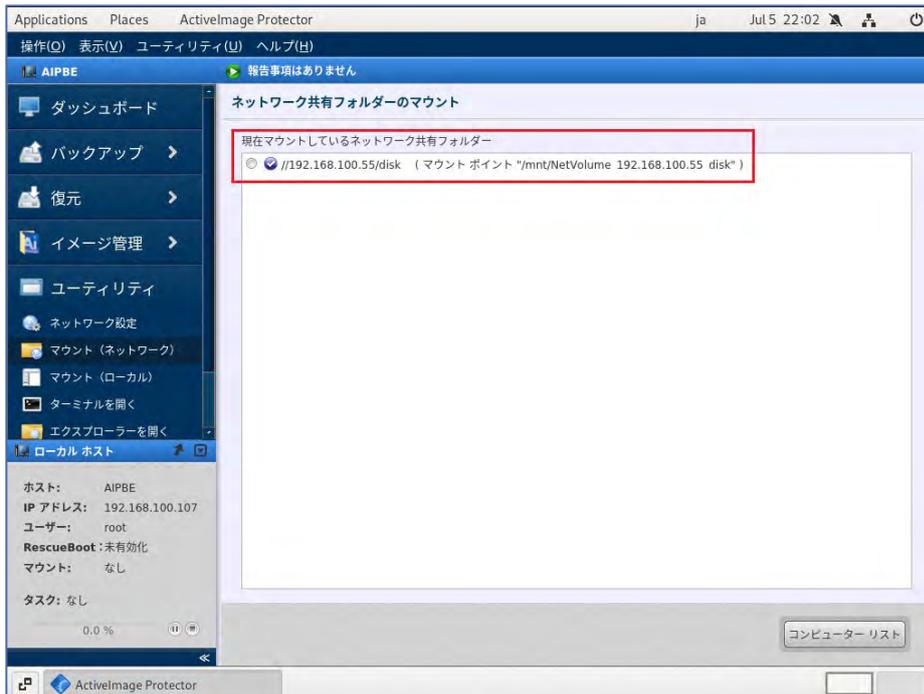
6. 保存先の共有フォルダーをマウントします。

ここでの例として、保存先のコンピューター「192.168.100.55」の共有フォルダー「disk」を選択して、[マウント]をクリックします。

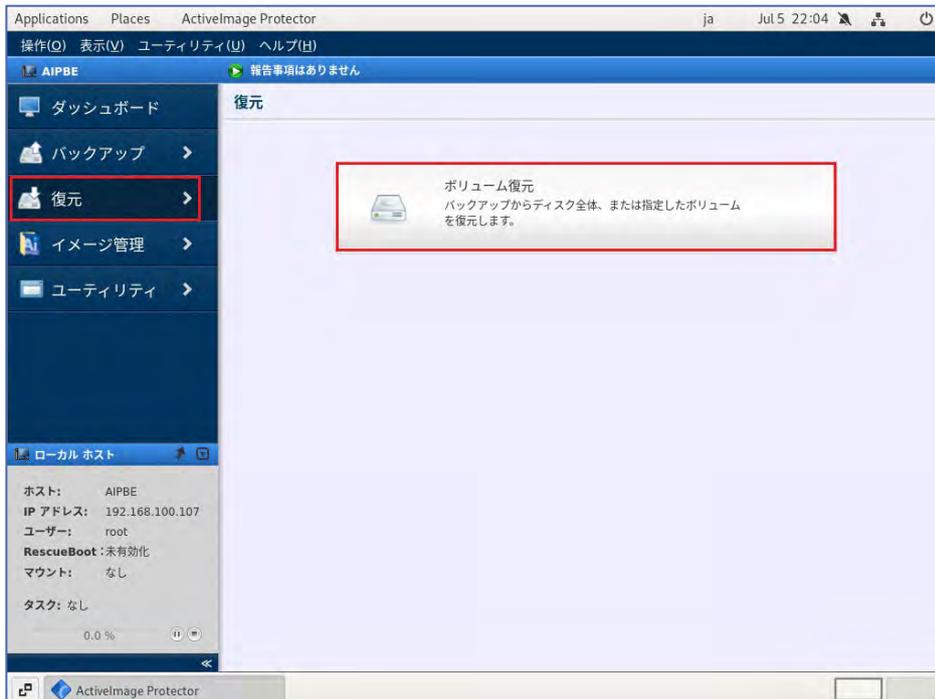


## リストア

7. マウントが完了するとマウントポイントのリスト上に表示されます。

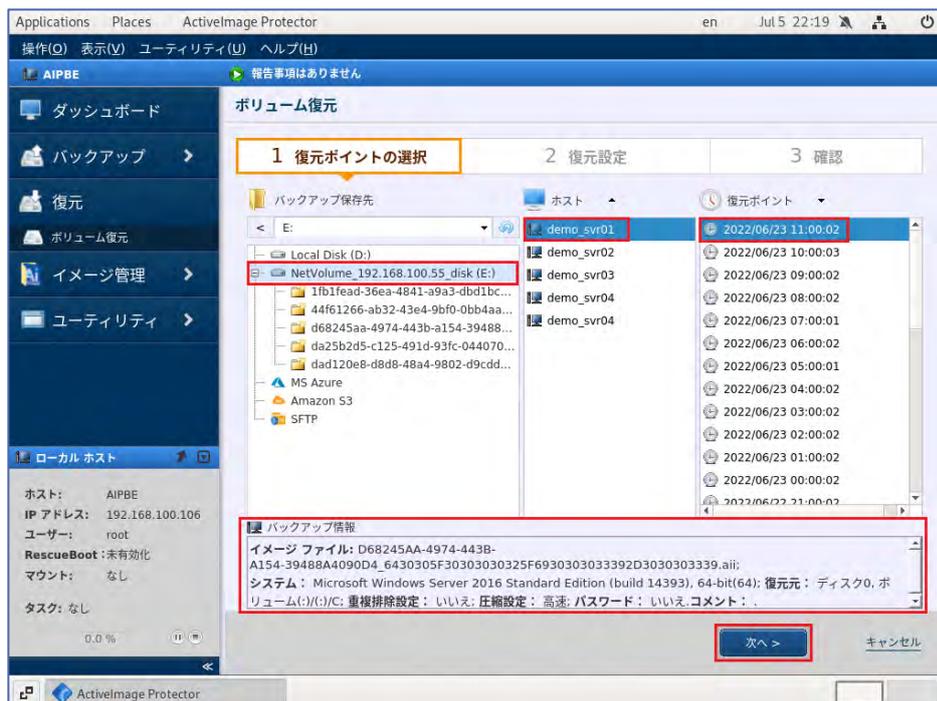


8. [復元] → [ボリューム復元] を選択します。

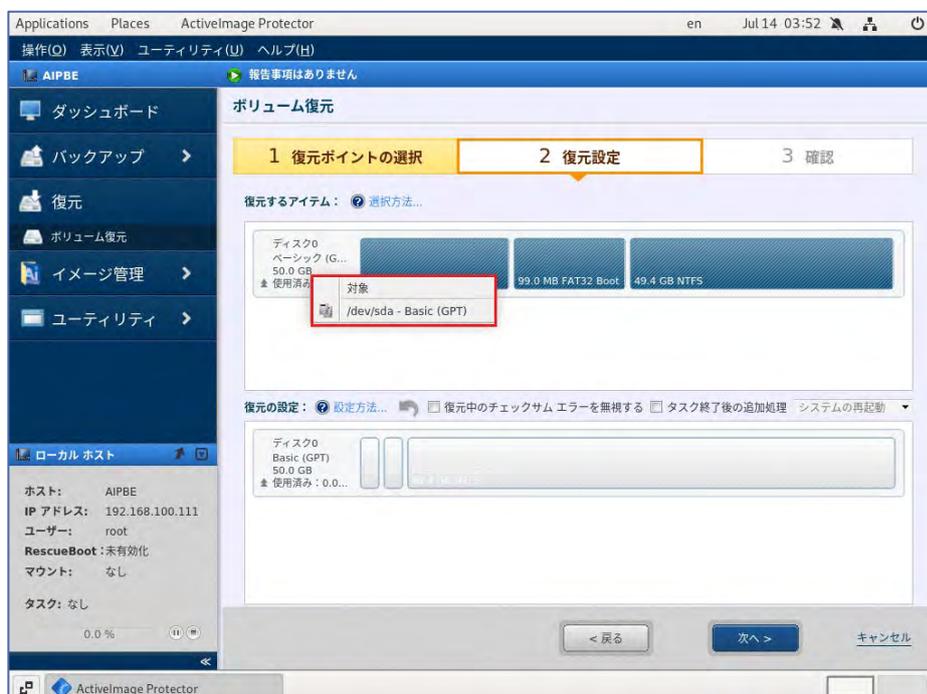


## リストア

9. マウントした保存先を選択して、バックアップ元の [ホスト] とバックアップの [復元ポイント] を指定したら [次へ] をクリックします。

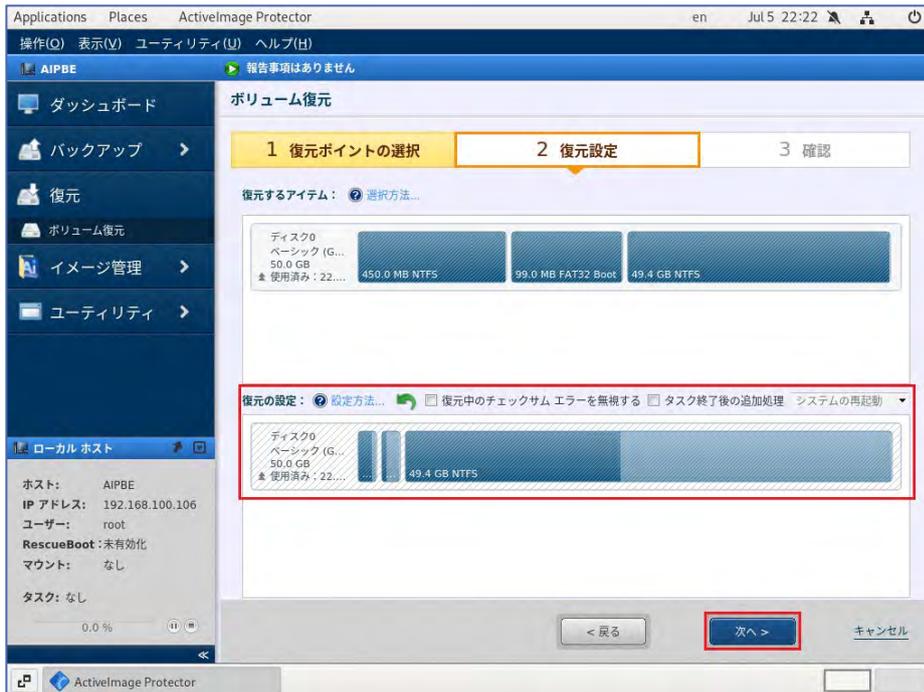


10. [復元するアイテム] からディスクマップの左部分を右クリックして、[対象] で「/dev/sda - Basic (GPT)」を選択します。または、復元先のディスクマップにドラッグ&ドロップして設定することもできます。

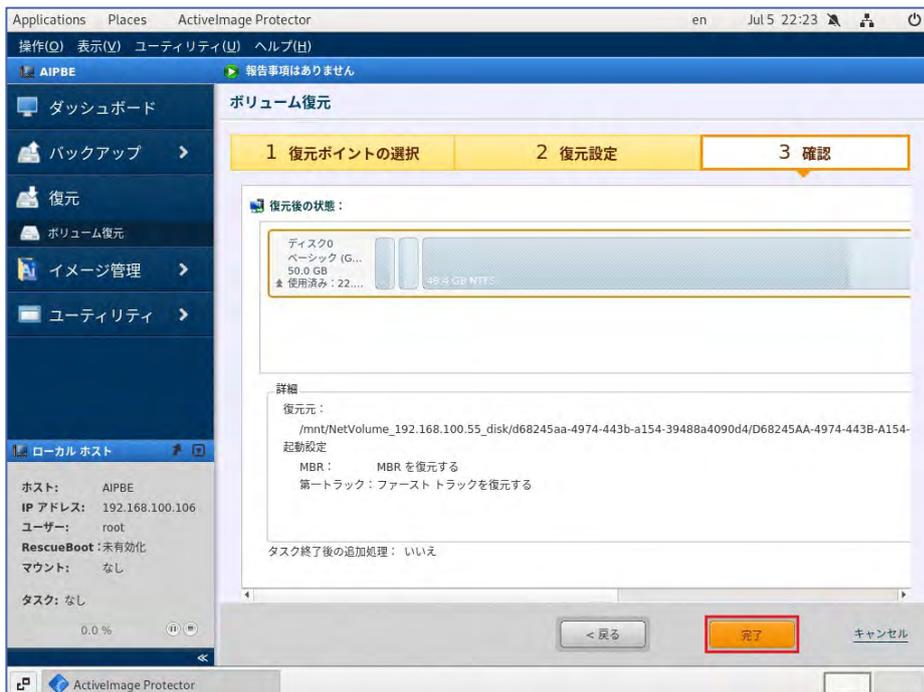


## リストア

11. [復元の設定] に復元する内容が表示されますので、確認し [次へ] をクリックします。

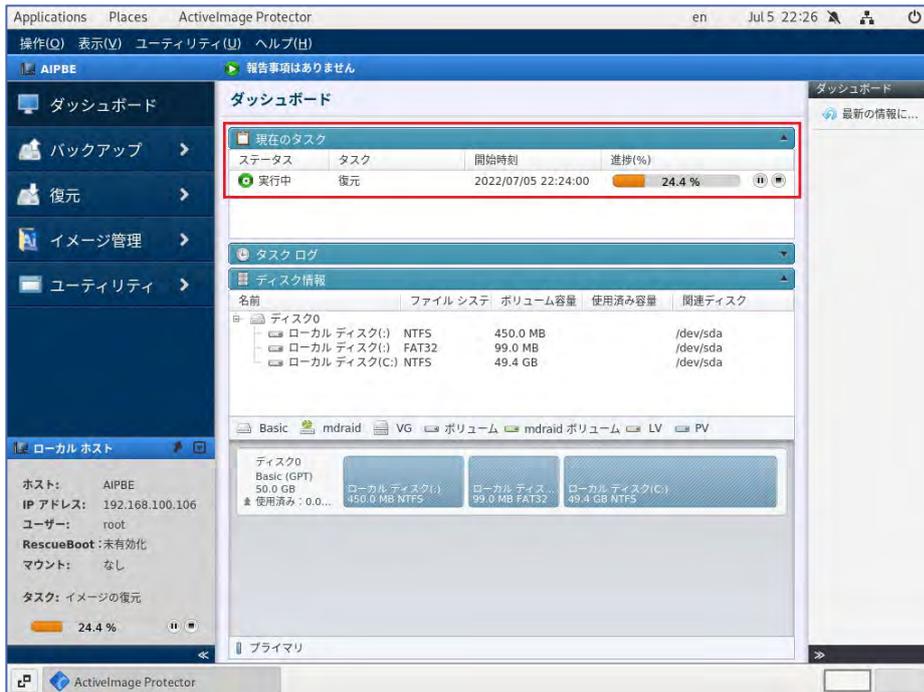


12. 確認画面になりますので、その内容を確認し、[完了] をクリックします。

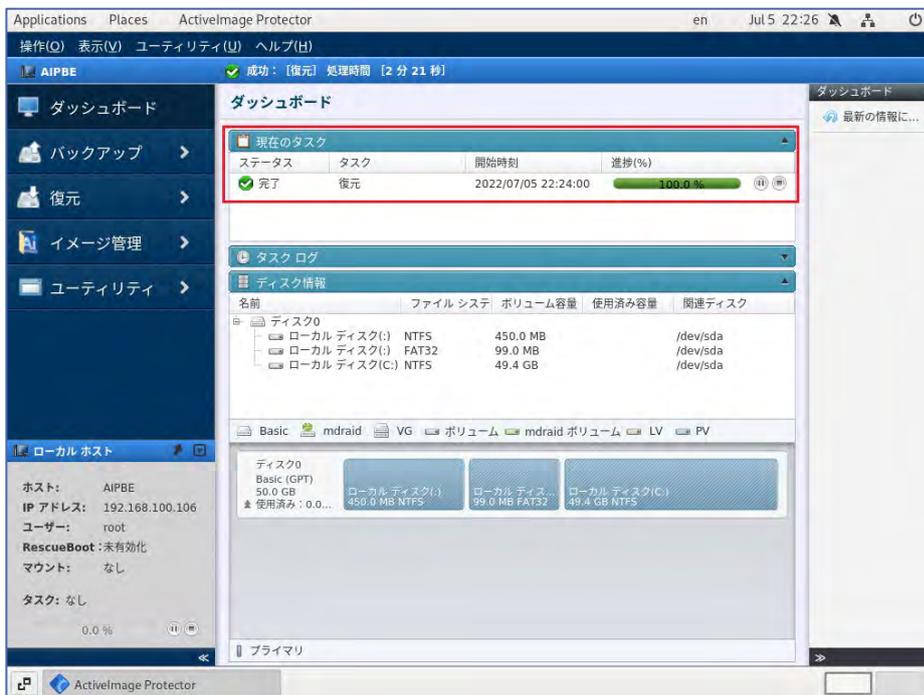


## リストア

13. リカバリーが開始されると、タスクの進捗状況が表示されます。



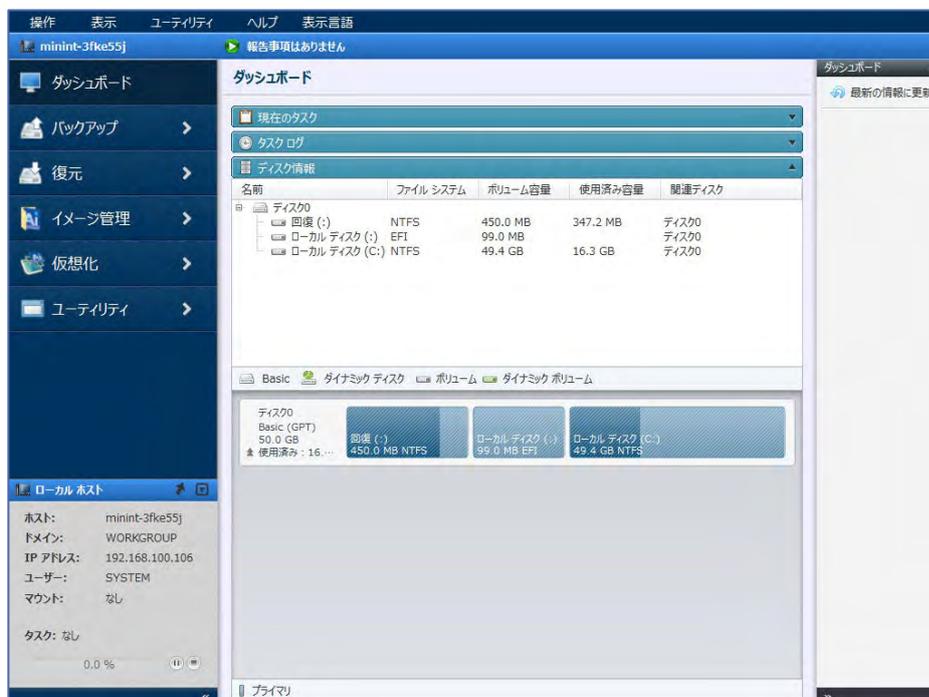
14. タスクが100%になれば、リカバリーの完了です。起動メディアを取り外し、[操作] → [終了] を選択し、シャットダウン、もしくは再起動します。リカバリーが正しくできているかを確認します。



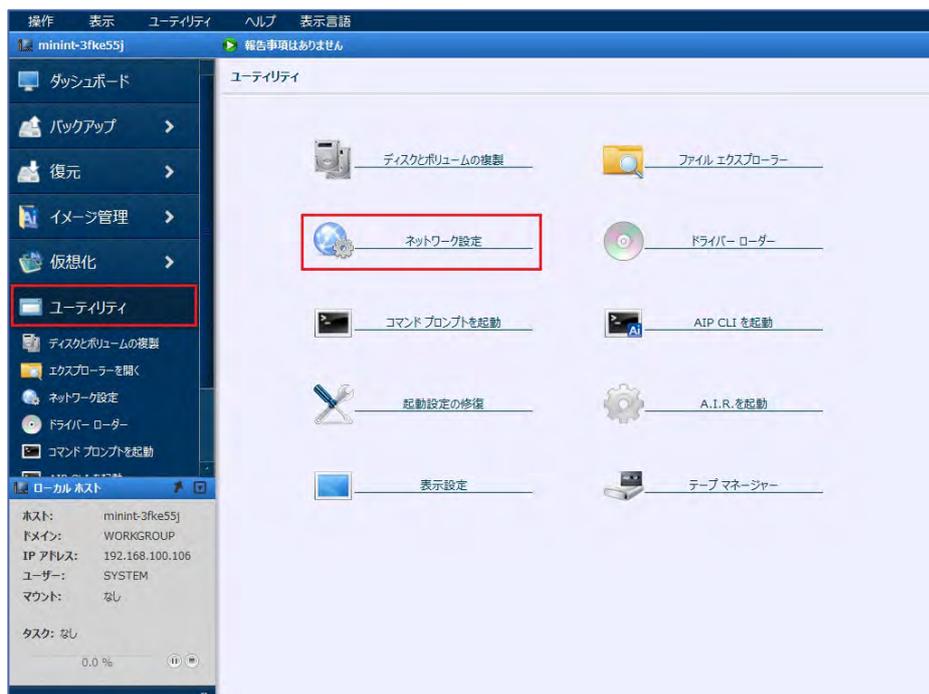
### 6-3. システムリカバリー：Windows RE ベースの起動環境

ActiveImage Protector の「起動環境ビルダー」で作成した、Windows RE ベースの起動環境を使用したシステムリカバリーの手順について説明します。

1. 作成した起動環境のメディアをセットして、コンピューターをメディアから起動します。起動環境の起動が完了するまで、しばらく待ちます。



2. 保存先のネットワーク共有フォルダーにアクセスするためにネットワークの設定を行います。  
[ユーティリティ] から [ネットワーク設定] を選択します。

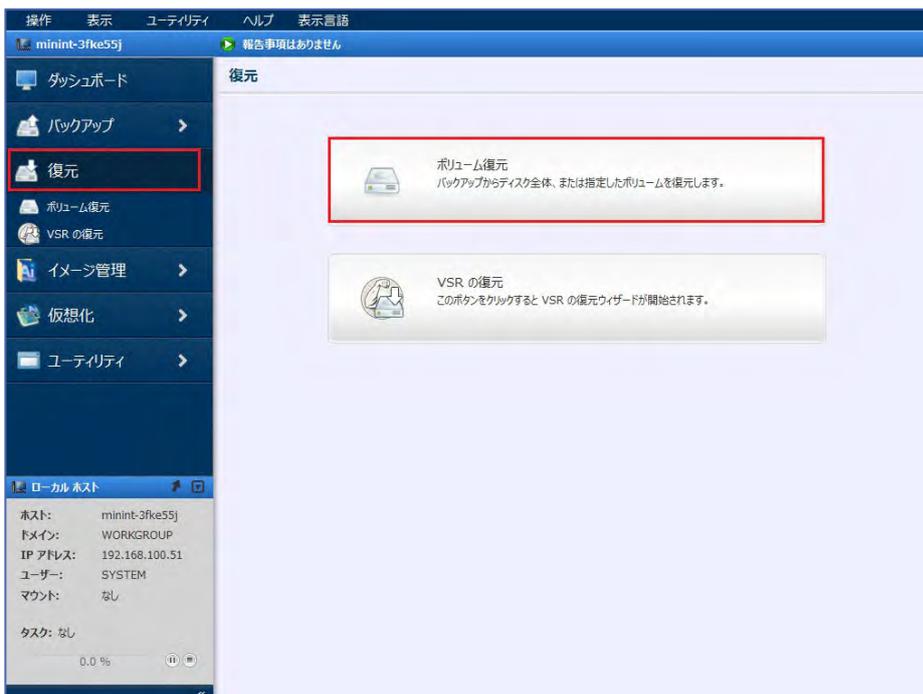


3. ネットワーク設定ダイアログになります。

ここでの例として、[以下の IP アドレスを使用する] を選択します。使用しているネットワークに合わせた設定を行います。ここでは、[IP アドレス:] に「192.168.100.51」、[サブネットマスク:] に「255.255.255.0」、[デフォルトゲートウェイ:] に「192.168.100.1」、[以下の DNS サーバー設定を使用する] を選択し、「192.168.100.1」を入力します。[適用] をクリックし、[OK] でネットワーク設定を終了します。

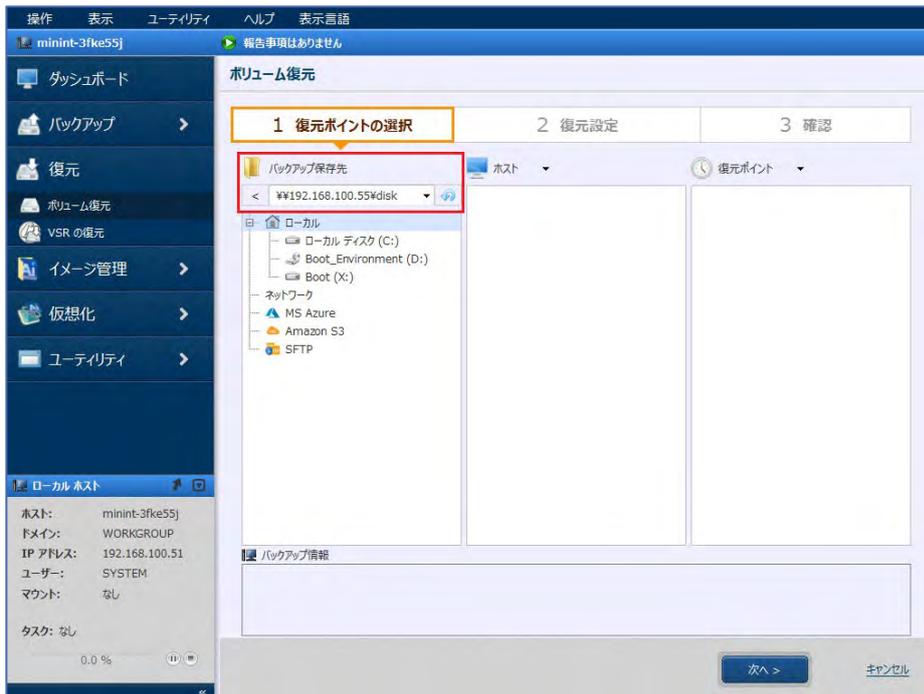


4. [復元] → [ボリューム復元] を選択します。

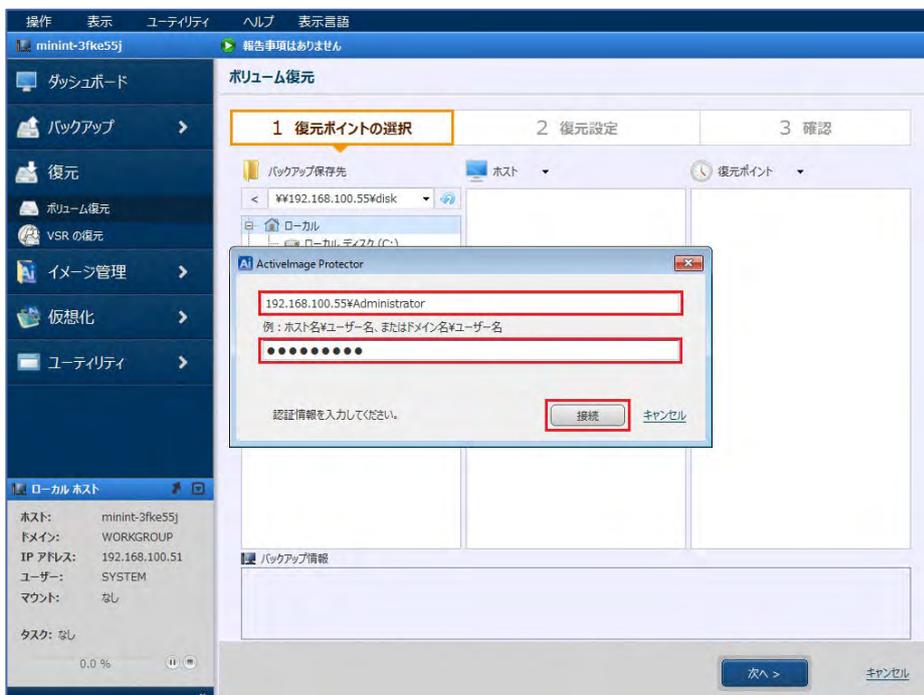


## リストア

5. ここでの例として、[バックアップの保存先] に共有フォルダー「¥¥192.168.100.55¥disk」を入力し、Enter キーを押します。

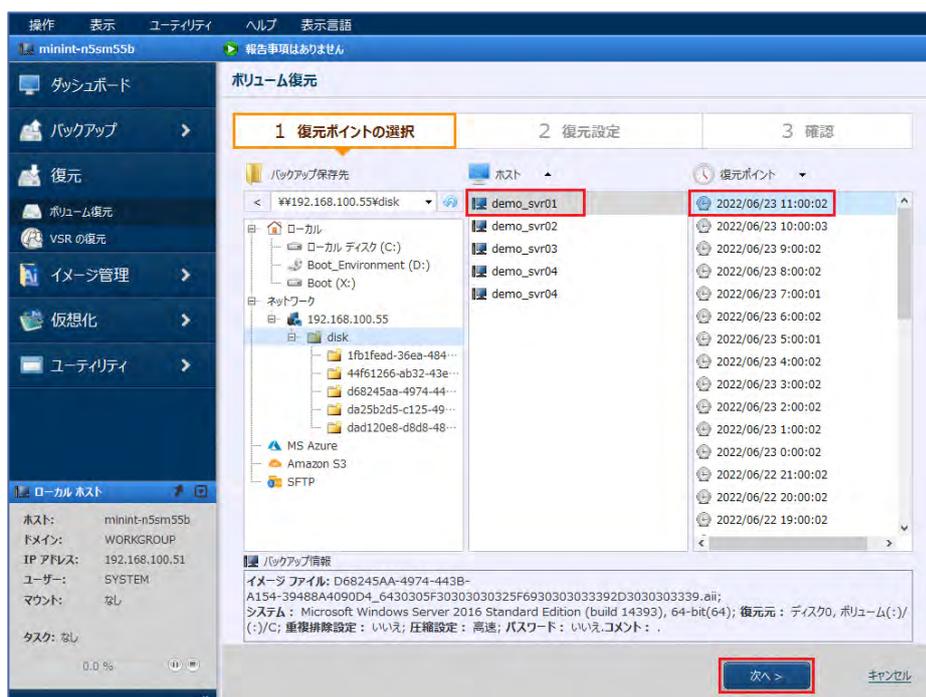


6. ユーザー認証が行われますので、ユーザー名に「192.168.100.55¥Administrator」を入力し、設定されたパスワードを入力し、[接続] をクリックします。

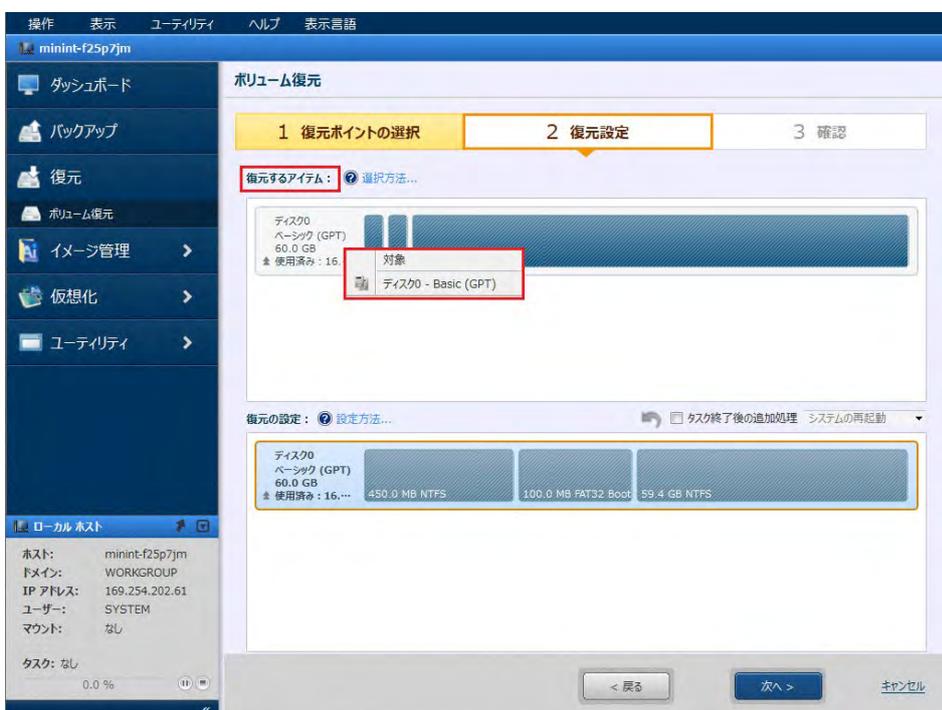


## リストア

7. バックアップ元の [ホスト] とバックアップの [復元ポイント] を指定したら、[次へ] をクリックします。

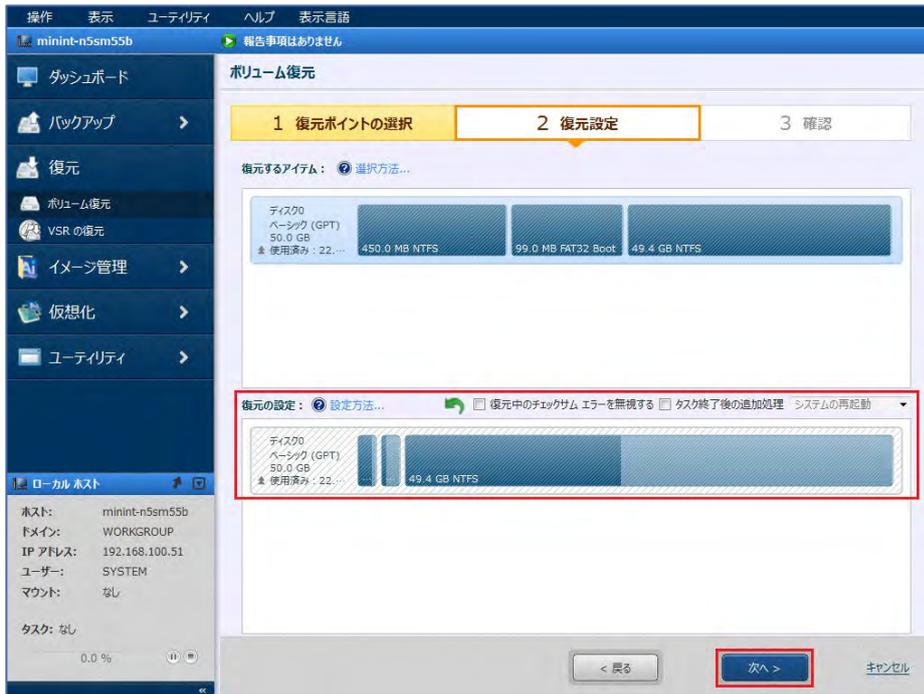


8. [復元するアイテム] からディスクマップの左部分（ベーシック（GPT）あたり）を右クリックして、[対象] で「ディスク0 - Basic（GPT）」を選択します。

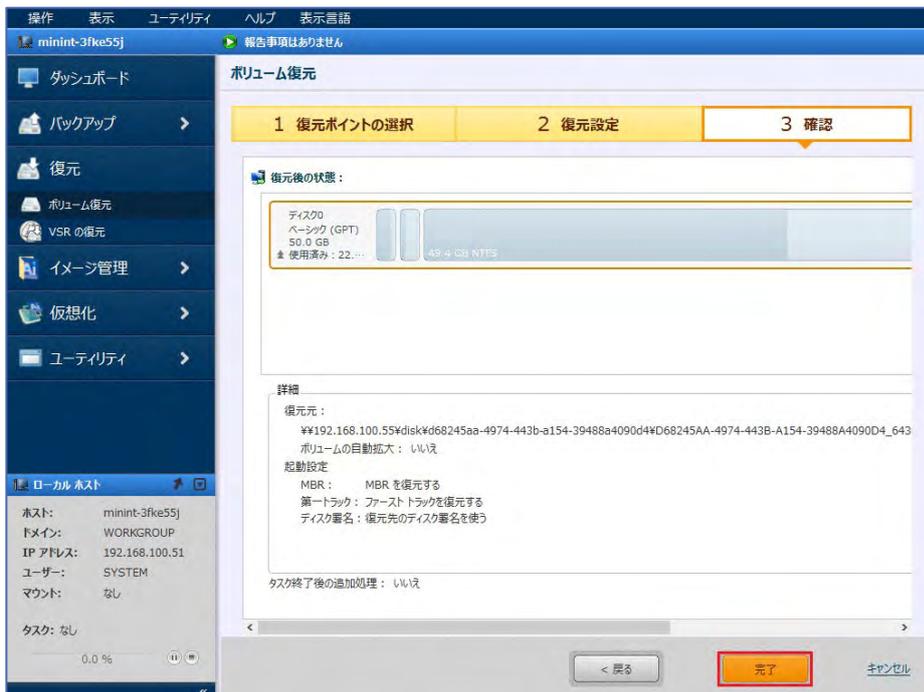


## リストア

9. [復元の設定] に復元する内容が表示されますので、確認し [次へ] をクリックします。

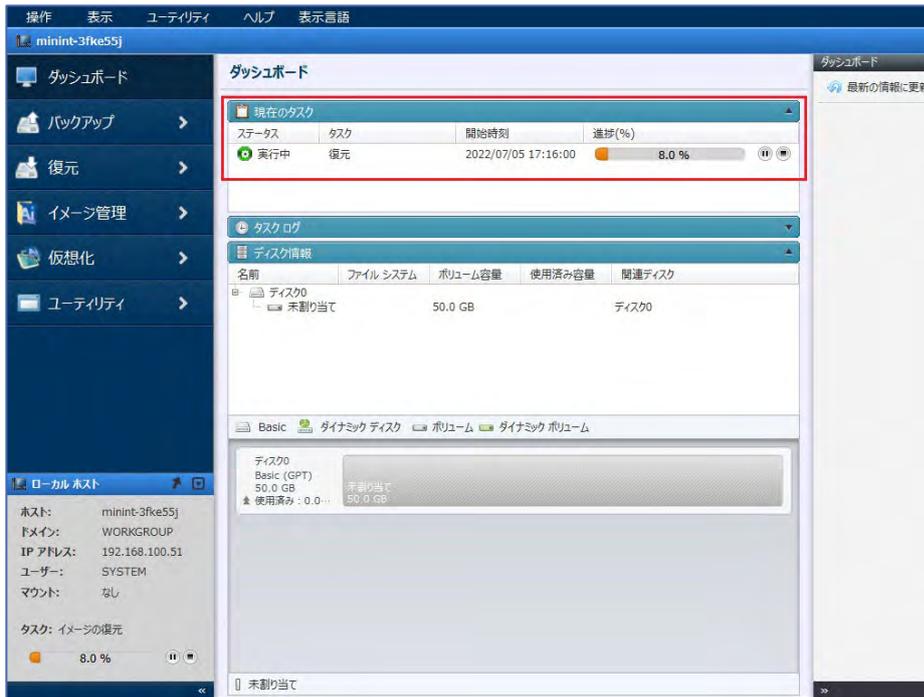


10. 確認画面になりますので、その内容を確認し、[完了] をクリックします。

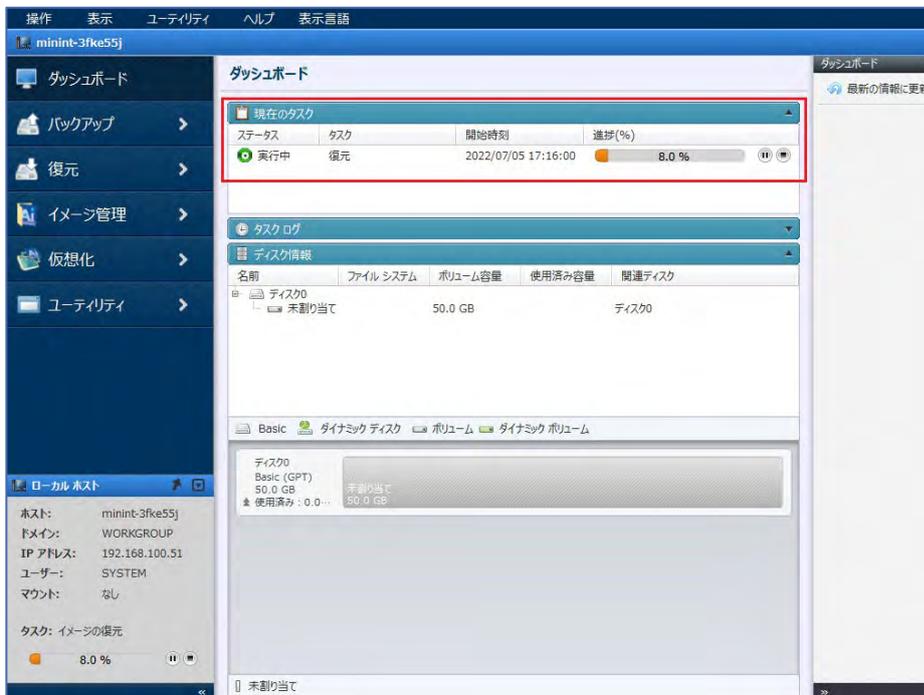


## リストア

11. リカバリーが開始されると、タスクの進捗状況が表示されます。



12. タスクが100%になれば、リカバリーの完了です。起動メディアを取り外し、[操作] → [終了] を選択し、シャットダウン、もしくは再起動します。  
リカバリーが正しくできているかを確認します



## 6-4. バックアップから新規仮想マシンを作成 (HyperRecovery)

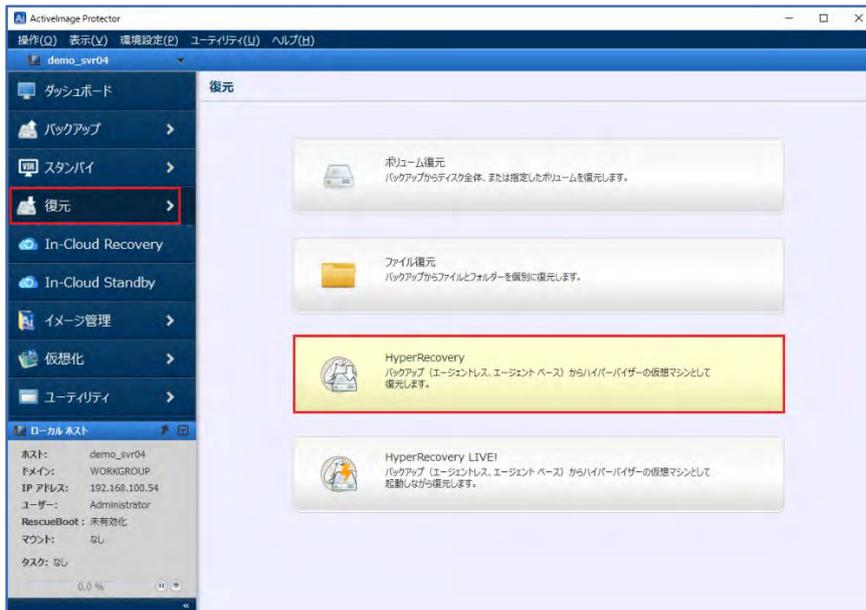
HyperRecovery は、バックアップから指定したハイパーバイザーに新規仮想マシン、または仮想ディスクを作成することができます。

ここでの例として、バックアップから新規仮想マシンを作成する手順について説明します。

1. ActiImage Protector を起動します。

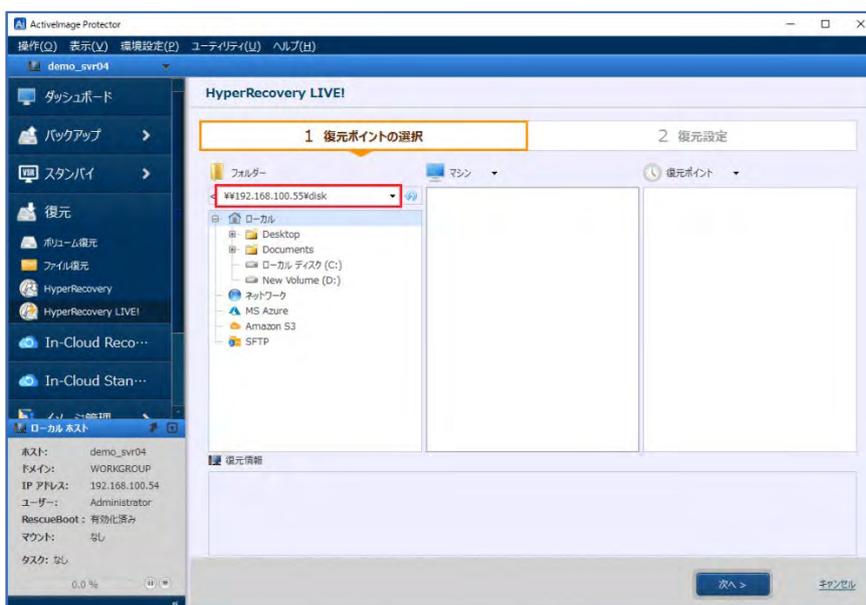
Windows スタートメニューから [Actiphly] → [ActiImage Protector] をクリックします。

2. [復元] → [HyperRecovery] をクリックします。



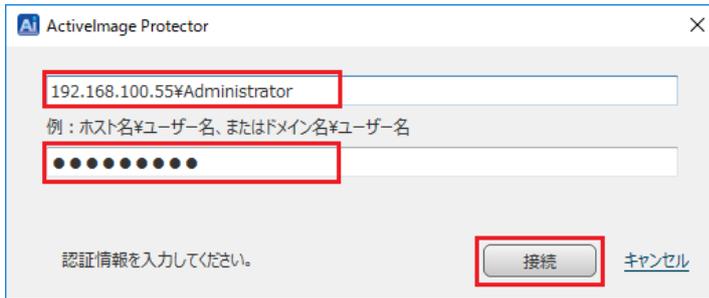
3. バックアップが保存されているフォルダーを選択します。

ここでの例として、バックアップが保存されている共有フォルダーのパス「¥¥192.168.100.55¥disk」を入力し、Enter キーを押します。

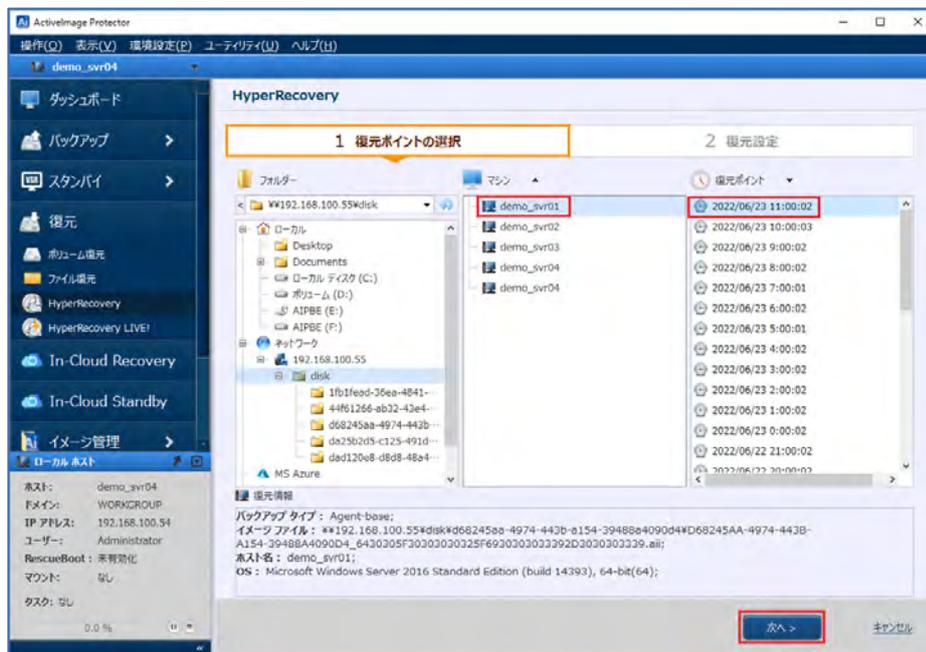


## リストア

- 共有フォルダーのユーザー認証が行われますので、[ユーザー名] に「192.168.100.55¥Administrator」と設定されたパスワードを入力し、[接続] をクリックします。

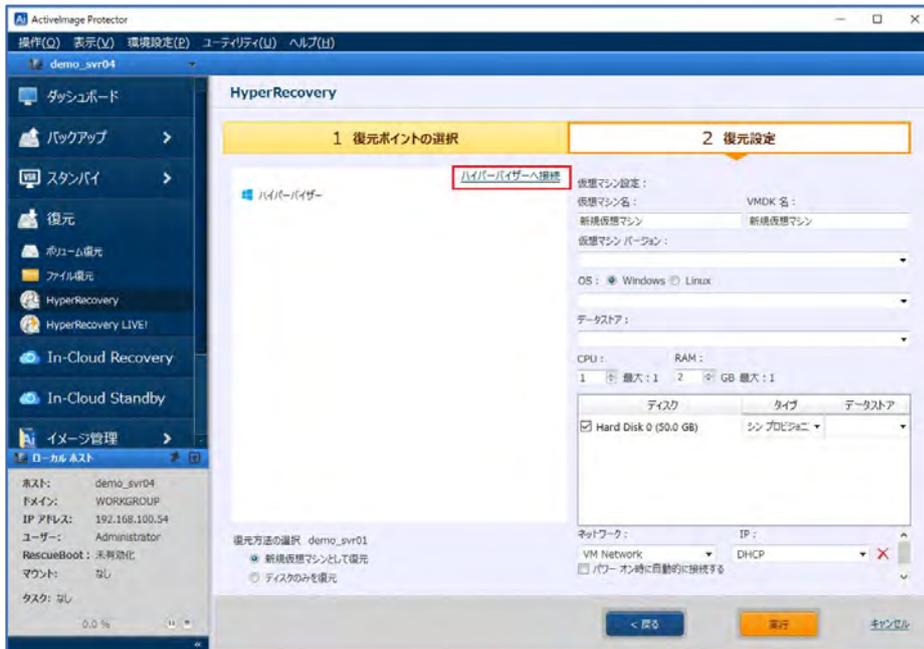


- バックアップ元の [マシン] とバックアップの [復元ポイント] を指定したら、[次へ] をクリックします。



## リストア

6. 仮想マシンを作成するハイパーバイザーを選択します。[ハイパーバイザーへ接続] をクリックします。



7. ハイパーバイザーのタイプを選択します。

ハイパーバイザーは、Microsoft Hyper-V、または VMware vSphere (ESXi) が使用できます。

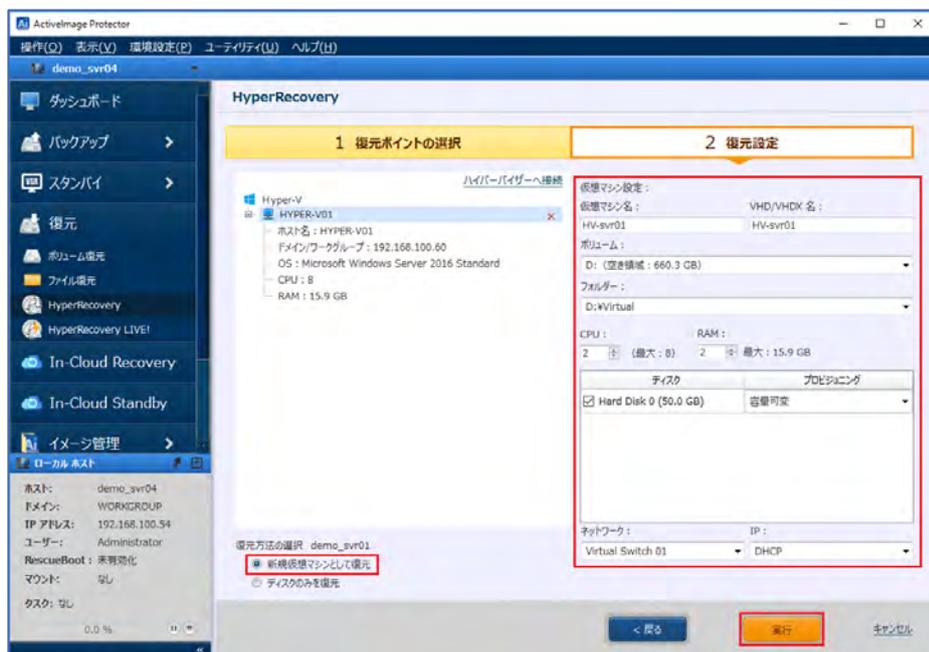
ここでの例として、[ハイパーバイザータイプ:] に「Microsoft Hyper-V」を選択し、[ホスト名、または IP アドレス:] に Hyper-V ホストの IP アドレス「192.168.100.60」、[ユーザー名:] に「Administrator」、[パスワード:] に設定されているパスワードを入力してから、[OK] をクリックします。



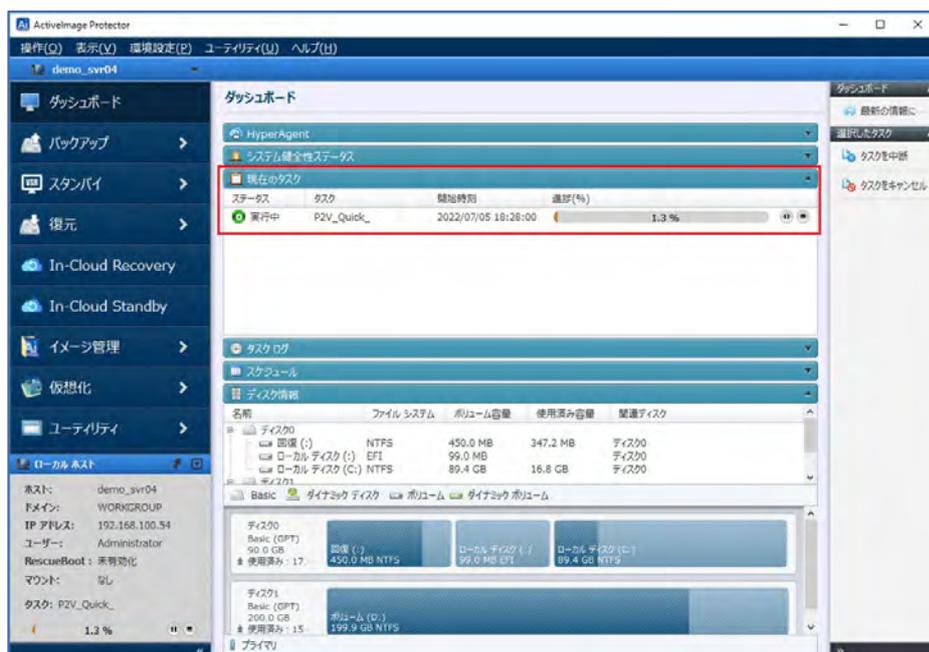
## リストア

### 8. 新規作成の仮想マシンの設定を行います。

ここでの例として、[復元方法の選択]は[新規仮想マシンとして復元]を選択します。[仮想マシンの設定]は、[仮想マシン名:]に「HV-svr01」、データストアの[ボリューム:]に「Dドライブ」、[フォルダー:]に「Virtual」、バックアップ元と同じく[CPU:]は「2」、[RAM:]は「2GB」、[ディスクのプロビジョニング:]は「容量可変」に設定します。すべての設定が完了したら、[実行]をクリックすると仮想マシンの作成が開始されます。

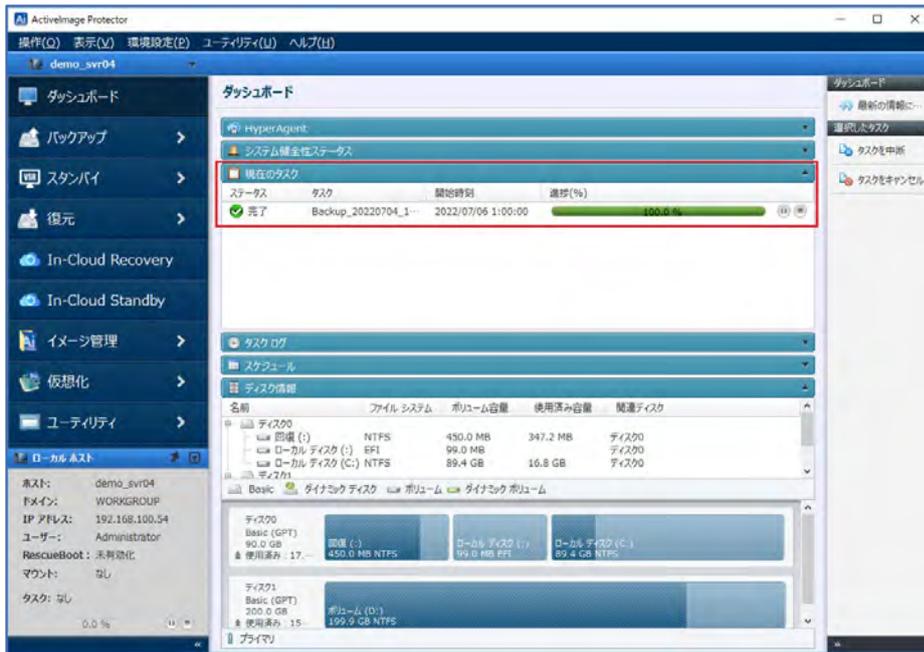


### 9. 仮想マシンの作成が開始されると、タスクの進捗状況が表示されます。



## リストア

10. タスクが 100%になれば、仮想マシンの作成は完了です。

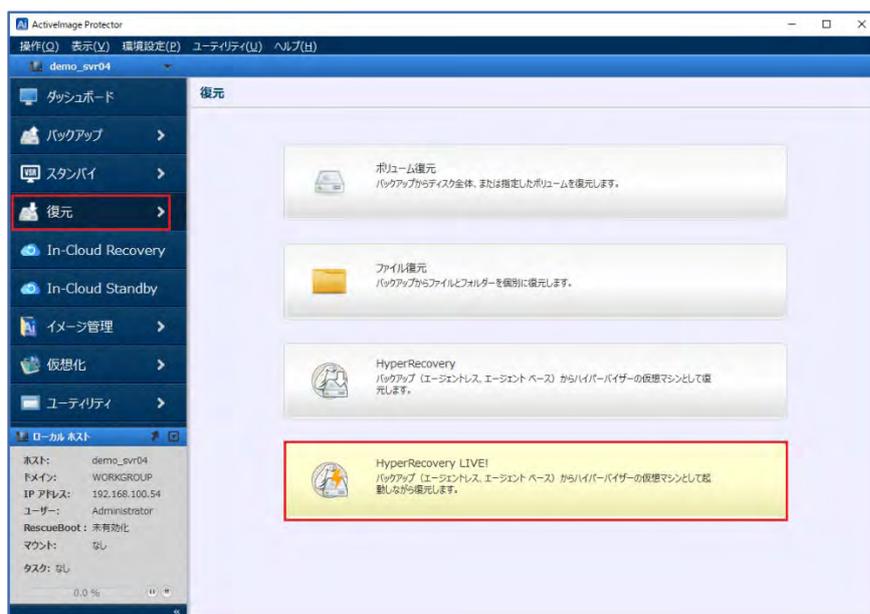


## 6-5. ゼロ タイム リカバリー (HyperRecovery LIVE!)

指定したハイパーバイザーにバックアップから直接仮想マシンとして起動し、すぐに稼働状態になります。稼働しながらバックグラウンドで、実際の復元対象の仮想ディスクへ復元を行い、完了後にはそのまま実稼働状態に移行することができます。ここでは、「HyperRecovery LIVE!」を使用した、仮想マシンへのリカバリー手順について説明します。

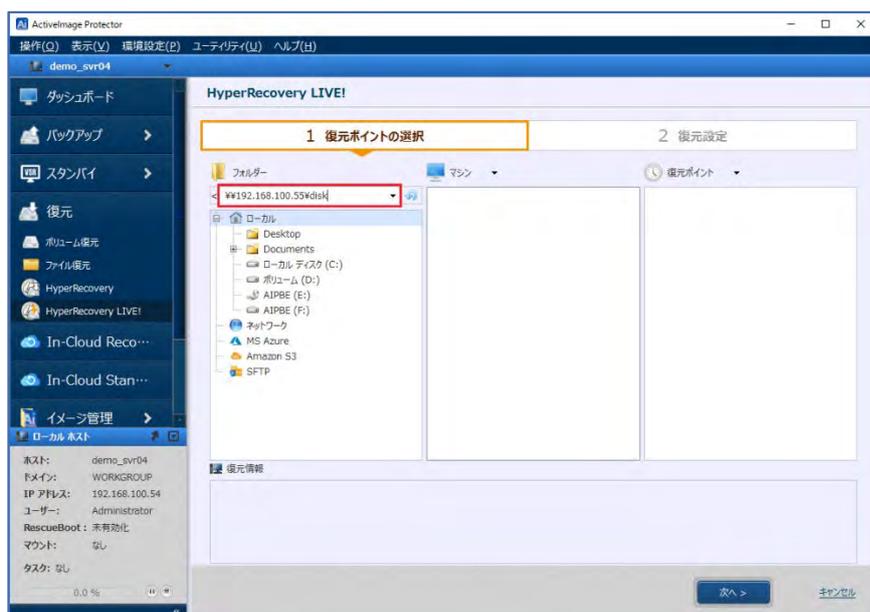
### 1. HyperRecovery LIVE!を起動します。

[復元] → [HyperRecovery LIVE!] をクリックします。



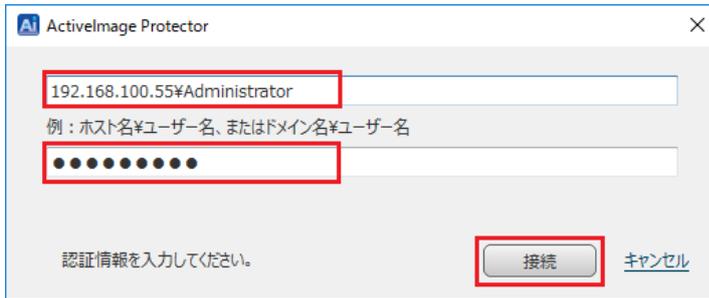
### 2. バックアップが保存されているフォルダーを選択します。

ここでの例として、バックアップが保存されている共有フォルダーのパス「¥¥192.168.100.55¥disk」を入力し、Enter キーを押します。

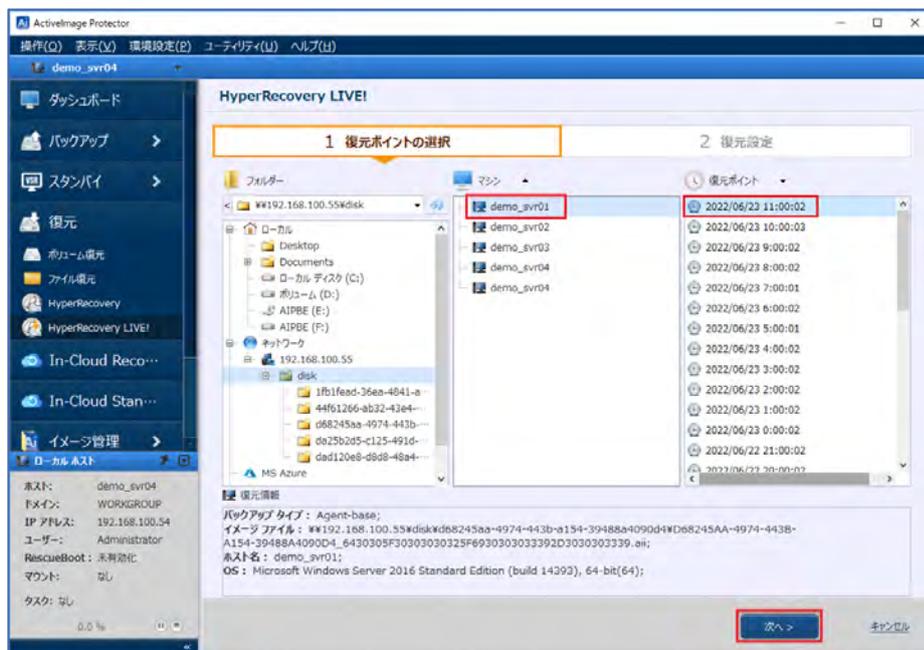


## リストア

3. ユーザー認証が行われますので、ここでの例として、[ユーザー名] に「192.168.100.55¥Administrator」を入力し、設定されたパスワードを入力して、[接続] をクリックします。

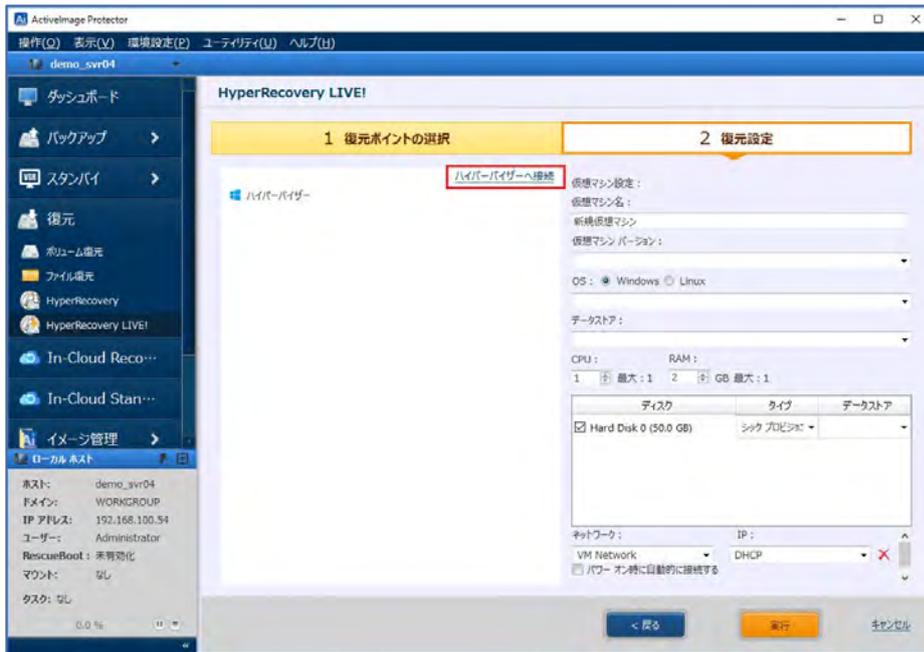


4. バックアップの復元ポイントを指定します。  
バックアップ元の [マシン] とバックアップの [復元ポイント] を指定したら、[次へ] をクリックします。



## リストア

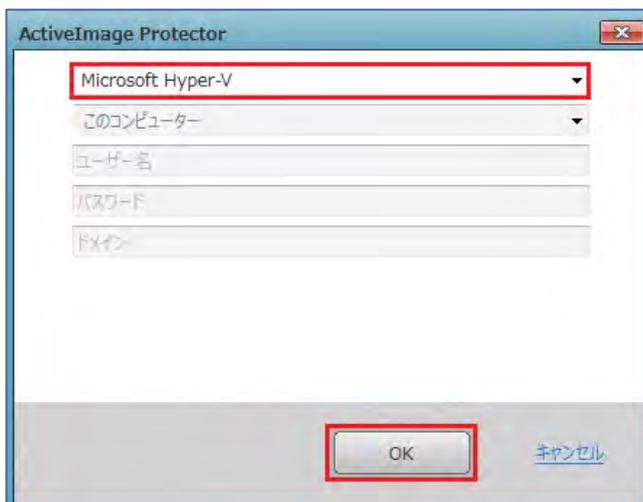
5. [ハイパーバイザーへの接続] をクリックして、復元先のハイパーバイザーを指定します。



6. ハイパーバイザーのタイプを選択します。

ハイパーバイザーは、ローカル コンピューターに構成された Microsoft Hyper-V、または VMware vSphere vCenter が使用できます。

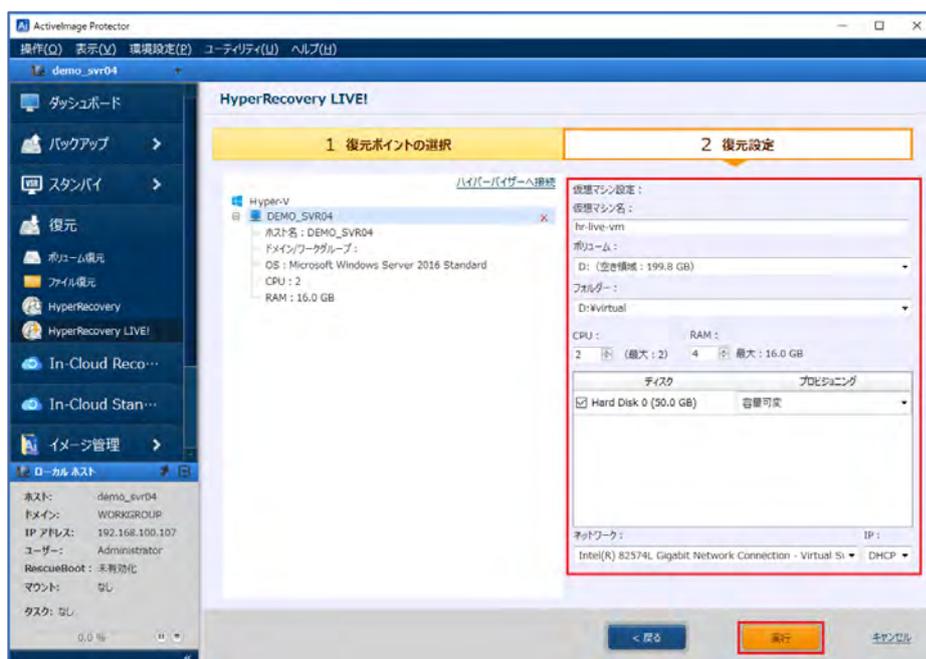
ここでの例として、ローカル コンピューターに構成された [Microsoft Hyper-V] を選択します。



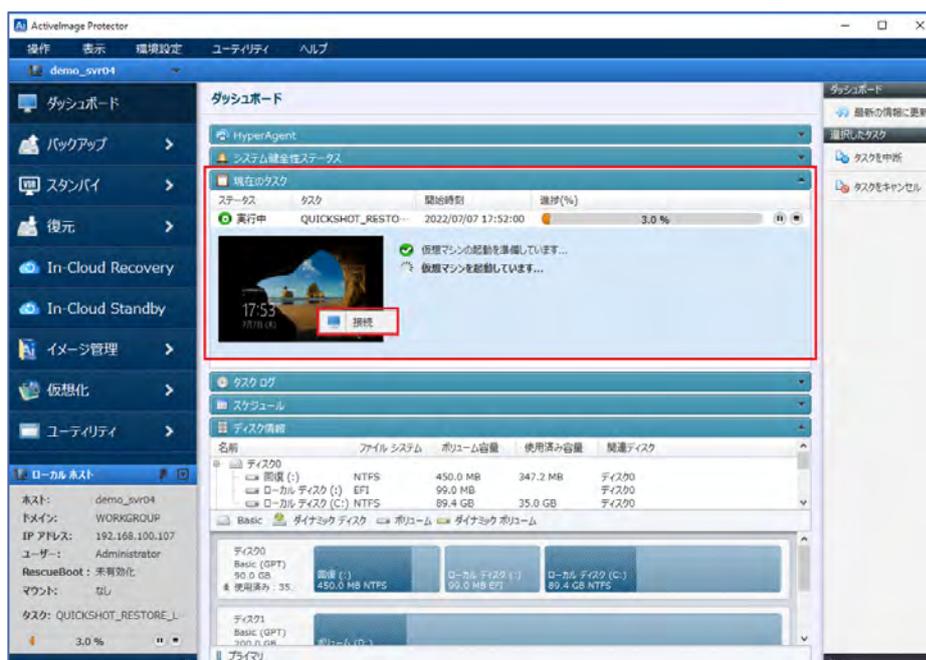
## リストア

### 7. 新規作成の仮想マシンの設定を行います。

ここでの例として、[仮想マシン名:] に「hr-live-vm」、データストアの [ボリューム:] に「D ドライブ」、[フォルダー:] に「Virtual」、バックアップ元と同じく [CPU:] は「2」、[RAM:] は「4GB」、[ディスクのプロビジョニング:] は「容量可変」に設定します。すべての設定が完了したら、[実行] をクリックします。



### 8. 復元を開始すると仮想マシンが起動し、すぐに稼働状態になります。サムネイルを右クリックして、[接続] を選択するとリモート コンソールで接続して操作を行うことができます。バックグラウンドでは、指定したハイパーバイザーにバックアップから仮想マシンとして復元します。

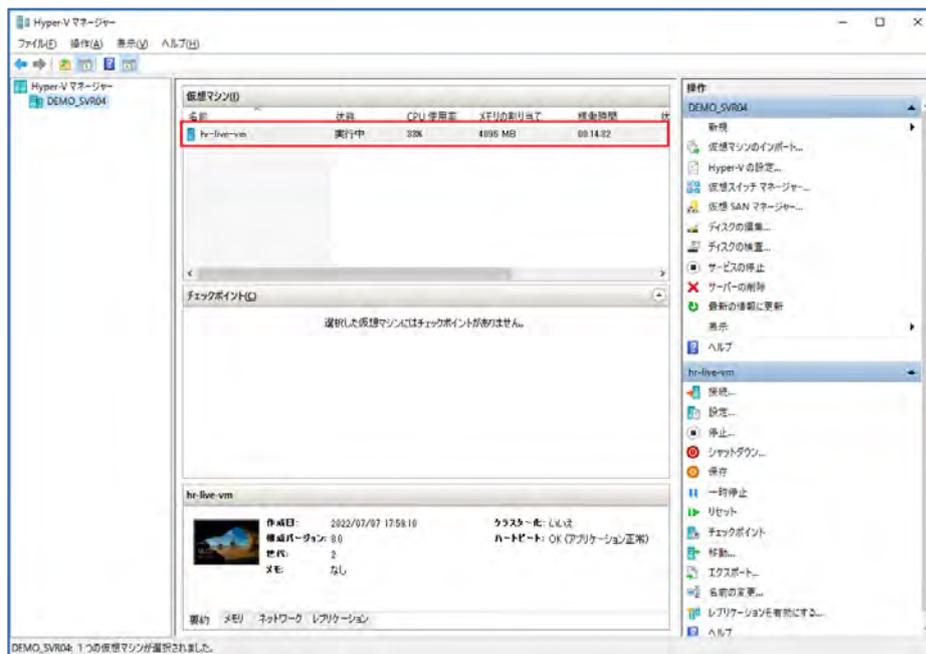


## リストア

9. バックアップ完了後には、そのまま稼働状態になります。



10. Hyper-V マネージャー上では、以下の様に仮想マシン「hr-live-vm」が作成され、稼働状態になっています。



## 6-6. クラウドリカバリー (In-Cloud Recovery)

In-Cloud Recovery は、バックアップから Amazon Web Service (AWS) 、または Microsoft Azure のクラウド上の仮想マシンに復元して、システム全体を復元して復旧することができます。復元操作は、各クラウドリージョンに配置している「Actiphy Cloud エージェント (起動環境)」を起動しておこないます。クラウドの管理コンソールやコマンドラインなどを駆使した複雑な操作を必要としません。

ここでは、バックアップからの AWS EC2 へのシステムの復旧手順について説明します。

### 1. [In-Cloud Recovery] を起動します。

左のメニューから [In-Cloud Recovery] をクリックします。

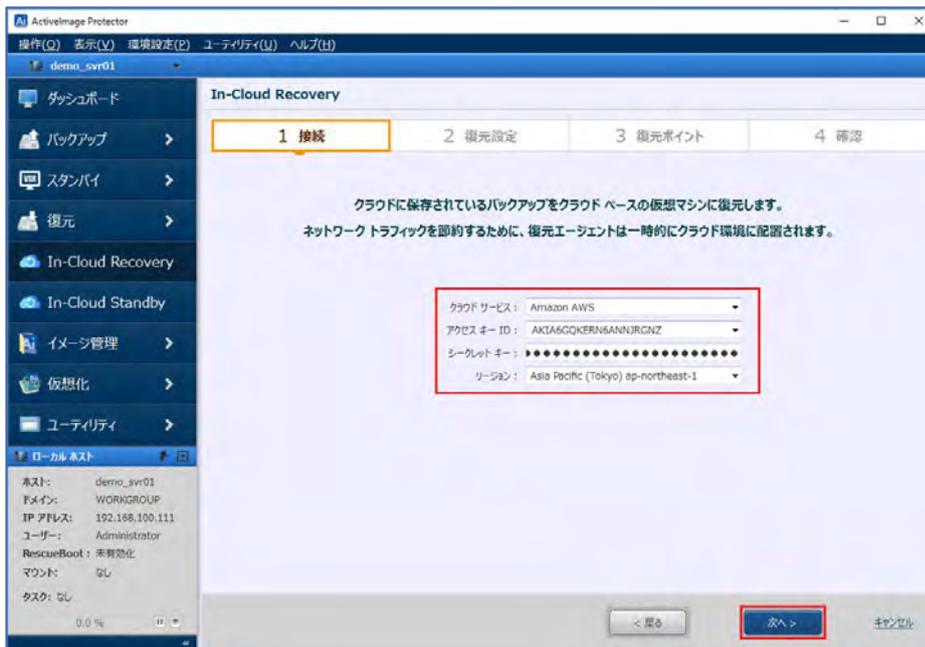
この処理の実行、および実行後の仮想マシンの運用には各クラウドプロバイダーの所定の利用料金がかかります。これに同意して、[追加費用に関して確認しました] のチェックボックスにチェックを入れ、[次へ] をクリックしてください



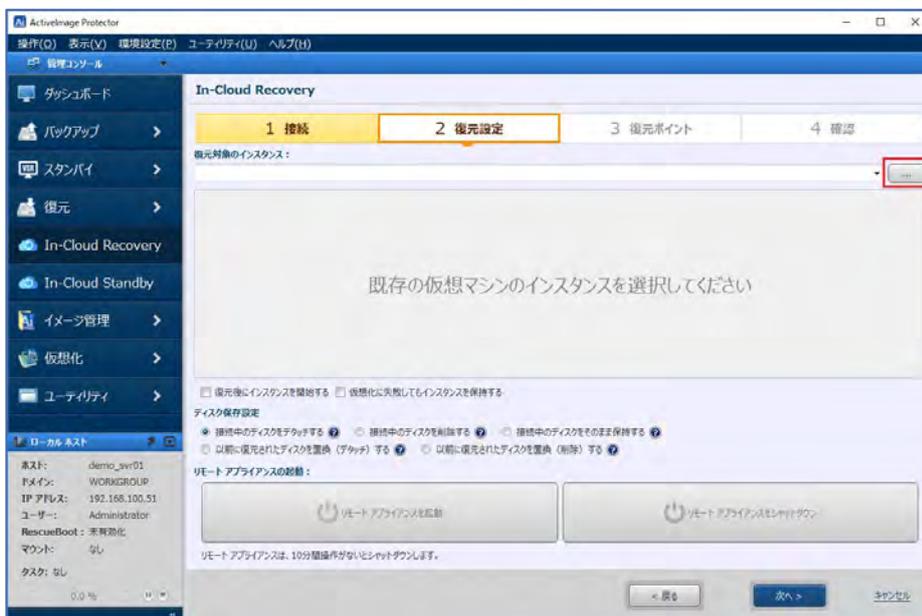
## リストア

2. 接続するクラウドサービスを選択し、必要な認証情報を入力します。

ここでの例として、クラウドサービスに [Amazon AWS] を選択して、Amazon S3 に対する AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [次へ] をクリックします。

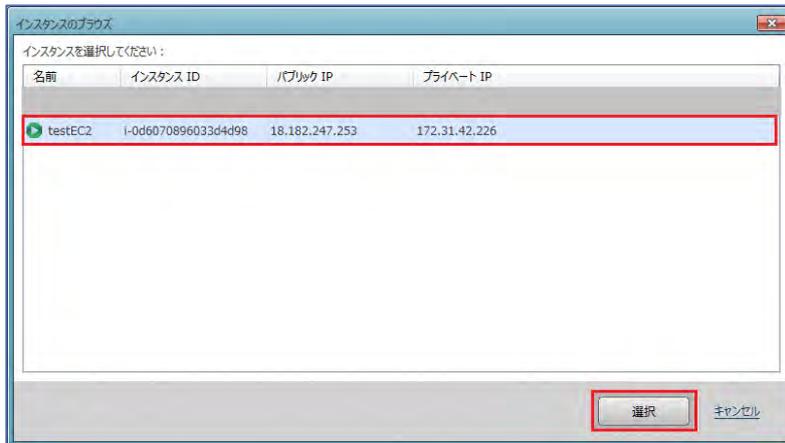


3. 復元先となるインスタンスを選択します。 [...] をクリックします。

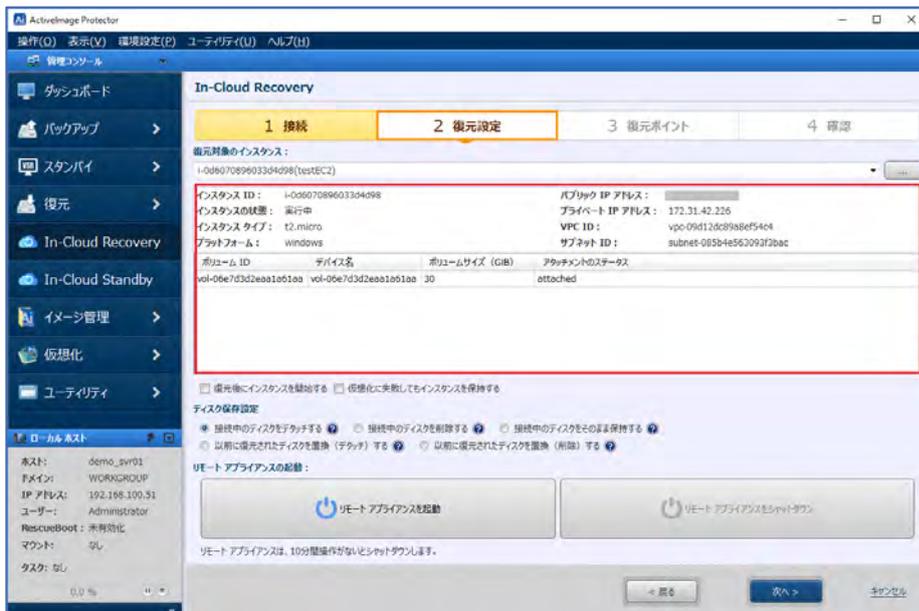


## リストア

4. 復元先となるインスタンスを選択してから、[選択] をクリックします。  
ここでの例として、「testEC2」を選択します。

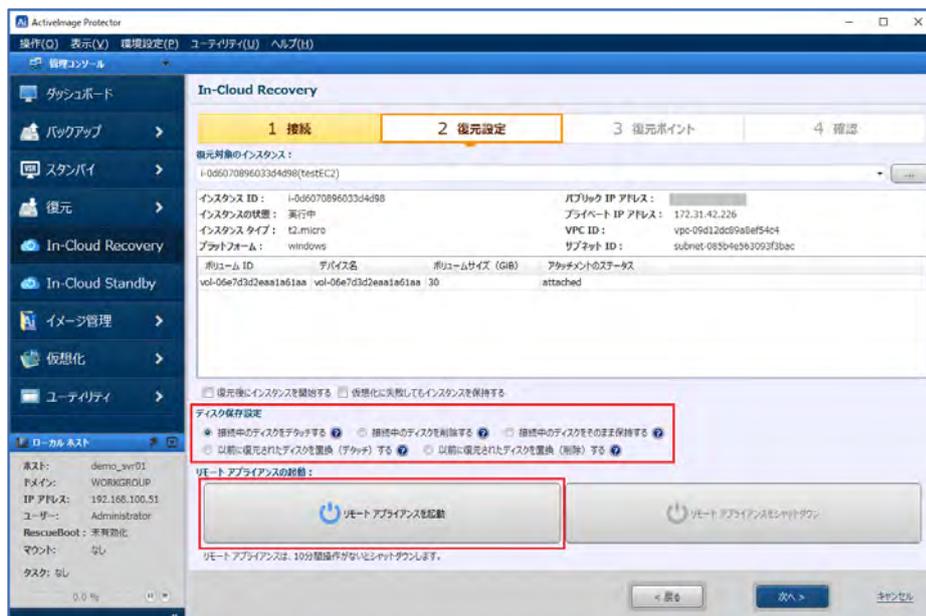


5. 復元先となるインスタンスの情報が表示されます。



## 6. 復元したボリュームの処理方法を選択します。

ここでの例として、[ディスク保存設定] は、標準設定の [標準のディスクをデタッチする] にします。次に、[リモートアプライアンスを起動] をクリックして、「Actiphy Cloud エージェント (起動環境)」を起動します。

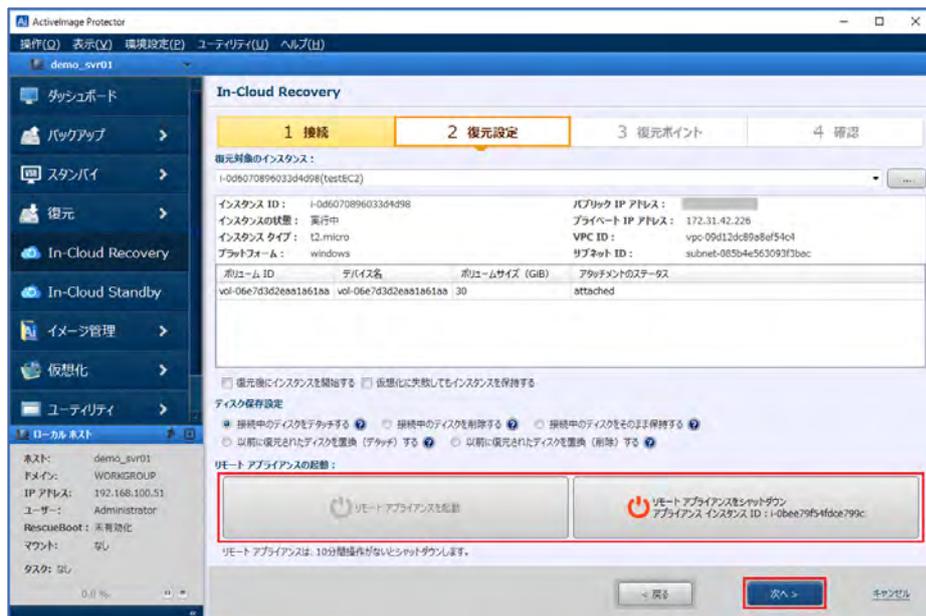


ディスク保存設定：

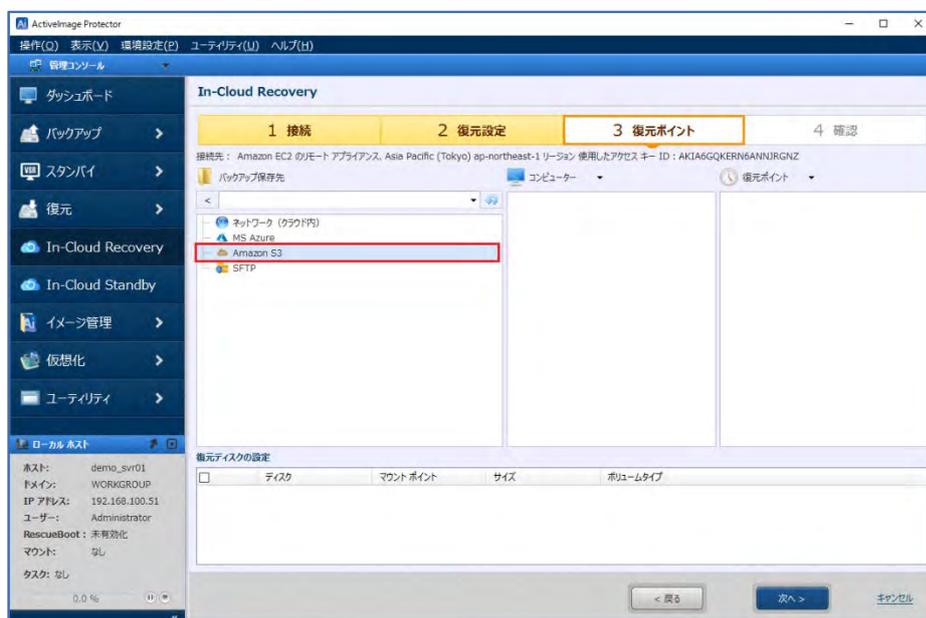
- 接続中のディスクを置換 (デタッチ) する：  
インスタンスに接続中のボリュームをデタッチ (切り離し) して、復元したボリュームをインスタンスに接続します。デタッチされたボリュームは削除されずに残ります。
- 接続中のディスクを置換 (削除) する：  
インスタンスに接続中のボリュームをデタッチ/削除し、復元したボリュームをインスタンスに接続します。
- 接続中のディスクをそのまま保持する：  
インスタンスに接続中のボリュームはデタッチせず、復元したボリュームを追加でアタッチします。
- 以前に復元されたディスクを置換 (デタッチ) する：  
インスタンスに接続中の本製品から復元したボリュームをデタッチし、復元したボリュームをインスタンスに接続します。デタッチされたボリュームは削除されずに残ります。本製品から復元されていないボリュームはインスタンスからデタッチされません。
- 以前に復元されたディスクを置換 (削除) する：  
インスタンスに接続中の本製品から復元したボリュームをデタッチ/削除し、復元したボリュームをインスタンスに接続します。本製品から復元されていないボリュームはインスタンスからデタッチされません。

## リストア

7. 以下の様に、[リモートアプライアンスを起動] ボタンがグレーアウトされ、[リモートアプライアンスをシャットダウン] ボタンが選択可能になったら、「ActiphlyCloud エージェント（起動環境）」の起動は完了です。[次へ] をクリックします。



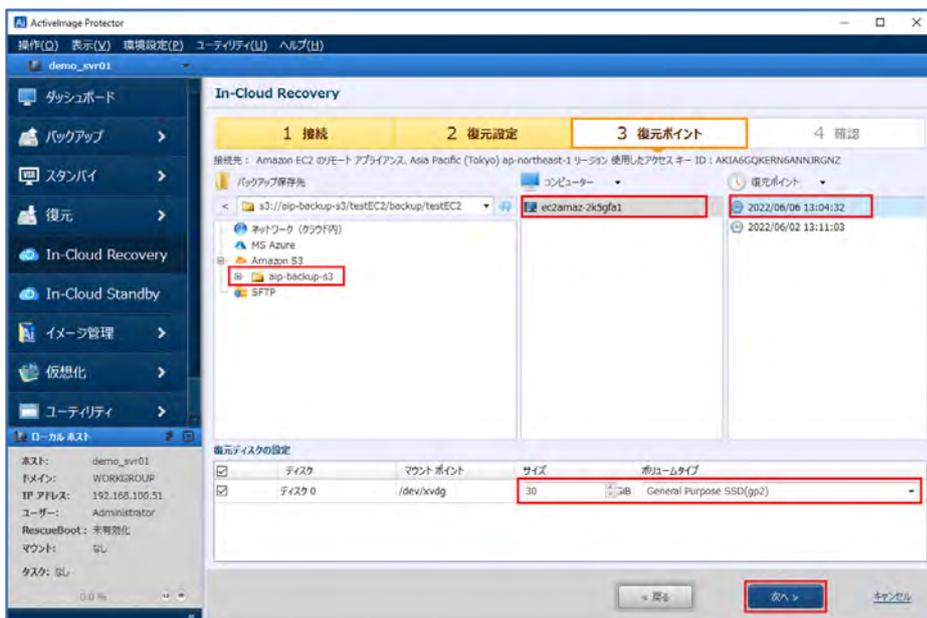
8. 復元したいマシンのバックアップ保存先を選択します。  
ここでの例として、[バックアップ保存先] は [Amazon S3] をクリックします。



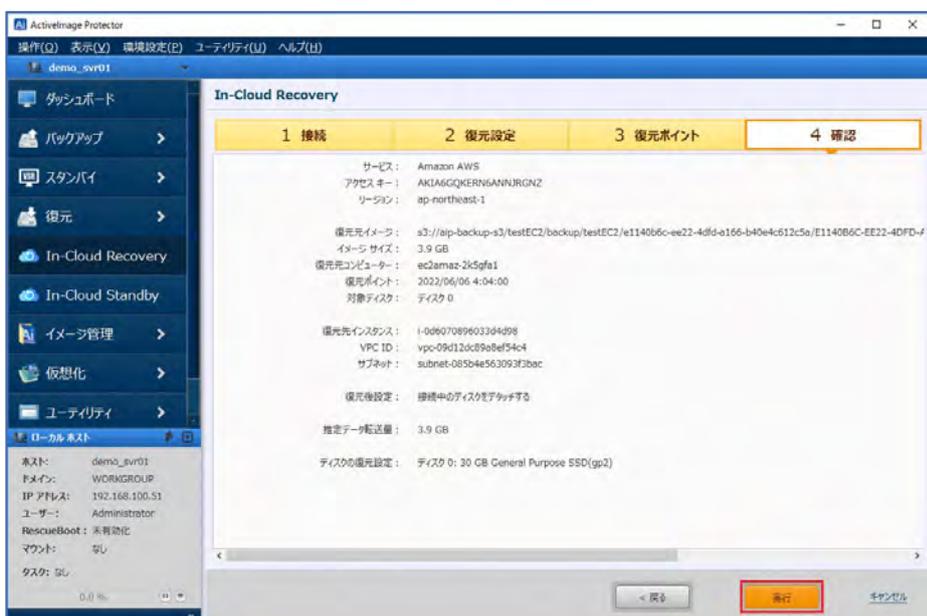
9. Amazon S3 に対する AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [接続] をクリックします。



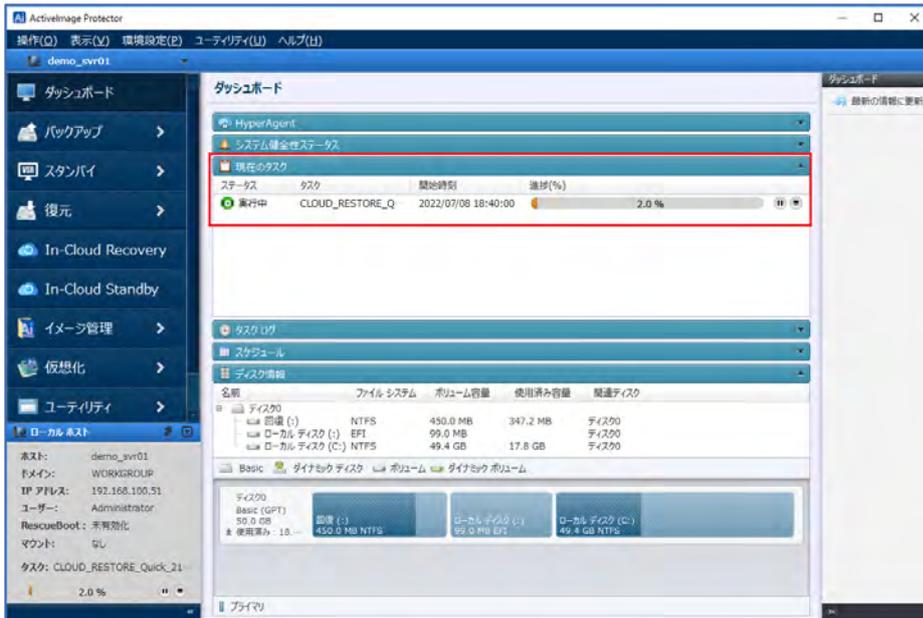
10. バックアップ保存先の「フォルダー」、「コンピューター」、「復元ポイント」を選択して、[次へ] をクリックします。[復元ディスクの設定] において、ディスクのサイズやタイプを設定することもできます。



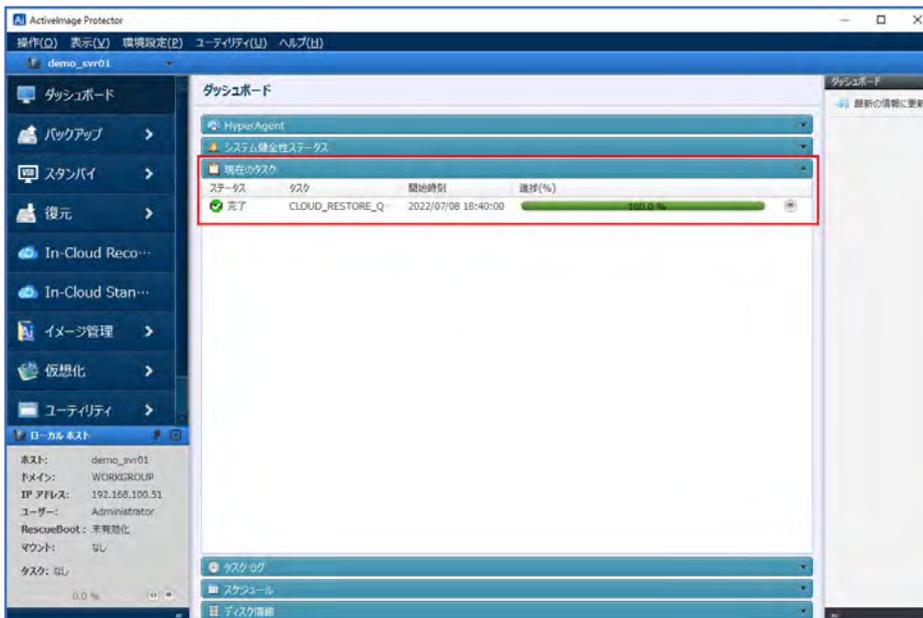
11. 内容を確認して、[次へ] をクリックすると復元が開始されます。



12. 復元が開始されると、タスクの進捗状況が表示されます。



13. 進捗が100%になると復元は完了です。



## リストア

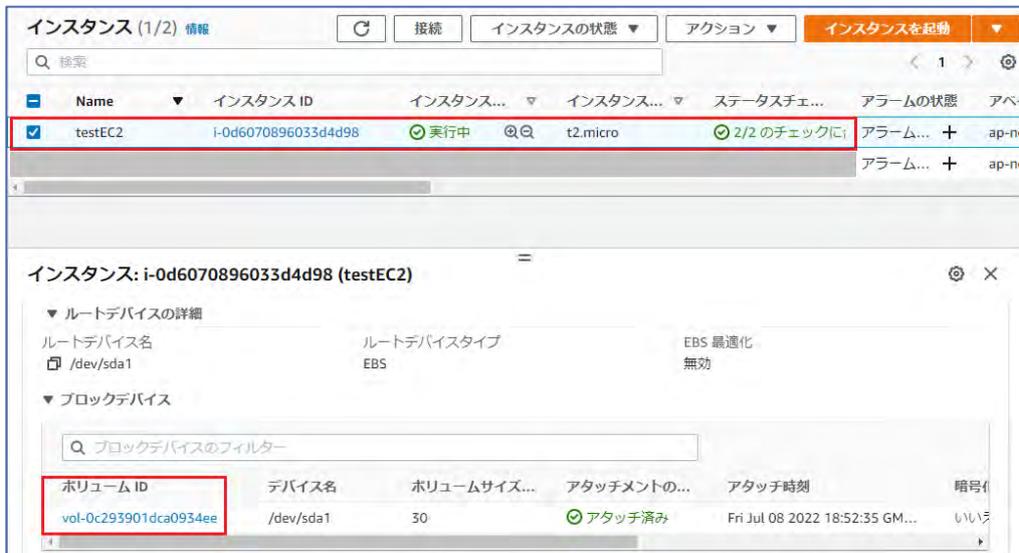
14. AWS コンソールから、インスタンスに接続されていたボリュームがデタッチされ、復元したボリュームがインスタンスに接続されていることが確認できます。

バックアップから新規ボリュームが作成されています。



Name	ボリューム ID	タイプ	サイズ	IOPS	スナップショット	作成日
testEC2_Disk_20220708184007	vol-0c293901dca0934ee	gp2	30 GiB	100	-	2022/07/08 18:40 GMT+9
testEC2	vol-06e7d3d2eaa1a61aa	gp2	30 GiB	100	sn...	2022/06/02 11:58 GMT+9

作成されたボリュームがインスタンスのルートデバイスとして接続されています



Name	インスタンス ID	インスタンス...	インスタンス...	ステータスチェ...	アラームの状態	アペ...
testEC2	i-0d6070896033d4d98	実行中	t2.micro	2/2 のチェックに...	アラーム... +	ap-no

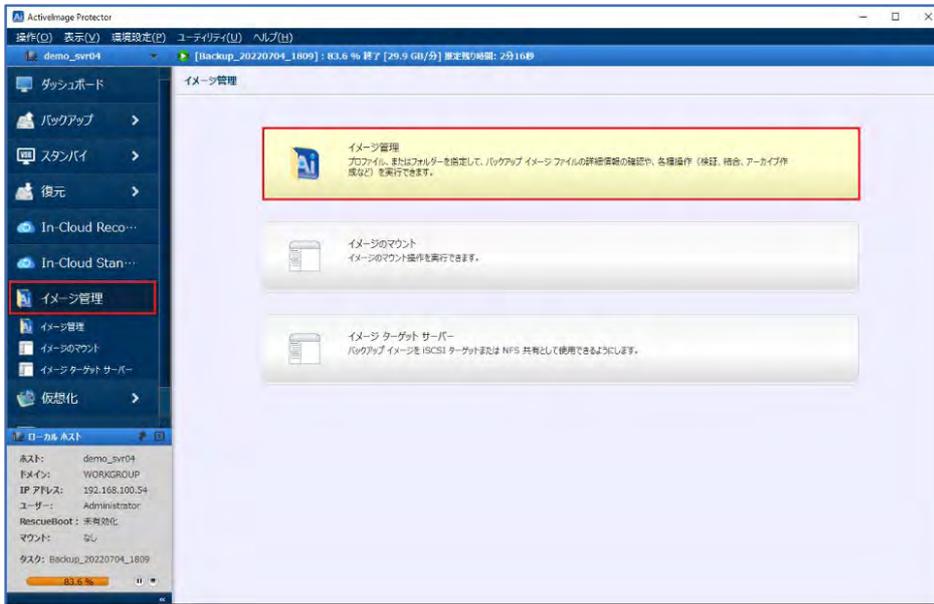
  

ボリューム ID	デバイス名	ボリュームサイズ...	アタッチメントの...	アタッチ時刻	暗号化
vol-0c293901dca0934ee	/dev/sda1	30	アタッチ済み	Fri Jul 08 2022 18:52:35 GM...	いいえ

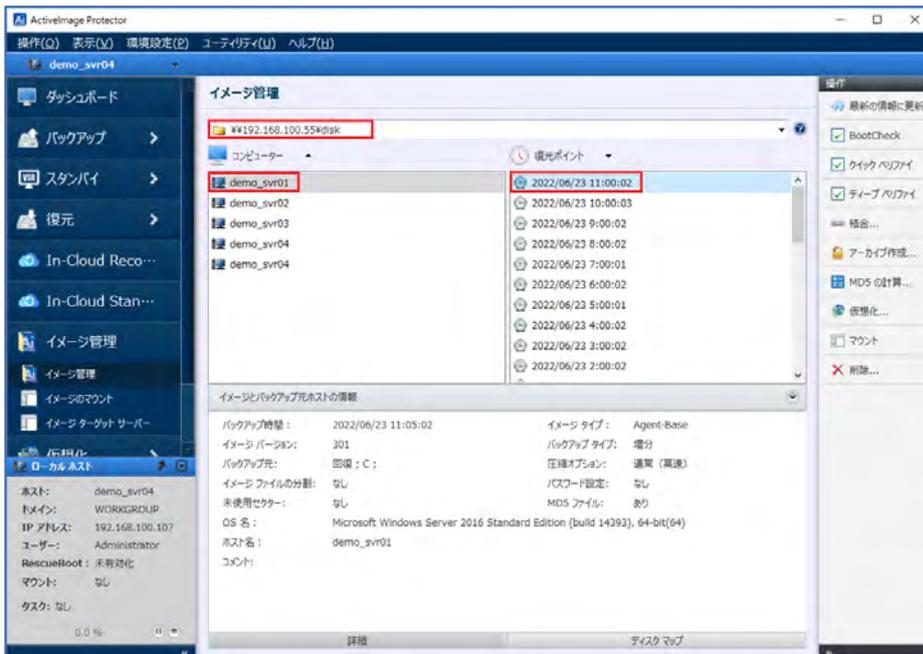
## 7. イメージ管理：イメージ管理

バックアップしたイメージファイルに対し、各種の操作を行います。

1. イメージ管理を行うには、左のメニューペインから、[イメージ管理] → [イメージ管理] を選択します。



2. バックアップが保存されているフォルダーを選択して、イメージ管理を行うバックアップ元の [コンピューター] とバックアップの [復元ポイント] を選択します。

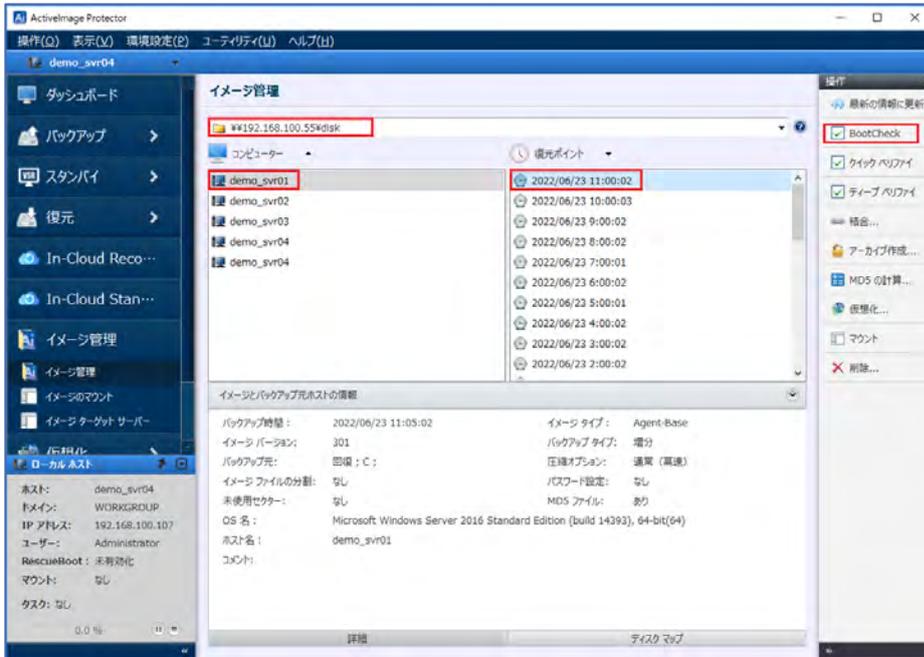


## 7-1. バックアップの起動確認 (BootCheck)

BootCheck は、選択したバックアップの起動確認を指定したホストのハイパーバイザーを使用して行います。

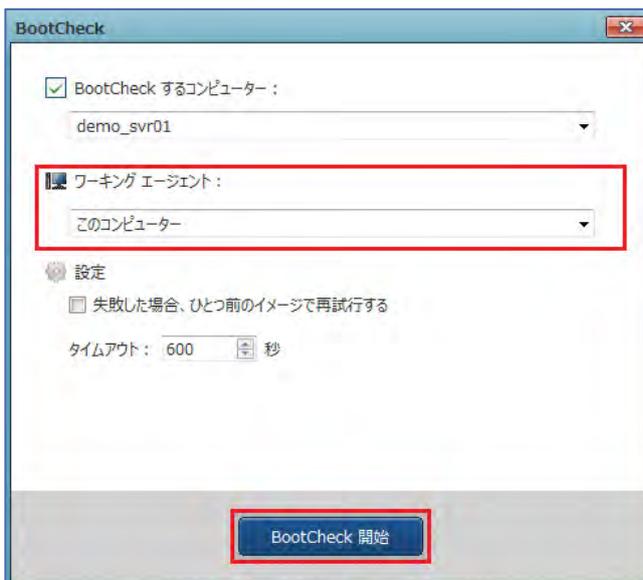
### 1. BootCheck を起動します。

バックアップ元の [コンピューター] とバックアップの [復元ポイント] を選択したら、右のペインから [BootCheck] をクリックします。

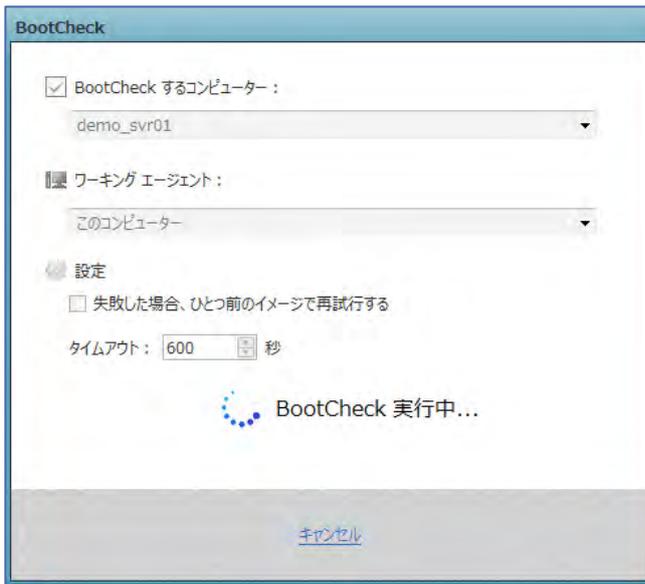


### 2. BootCheck の実行の確認が行われます。

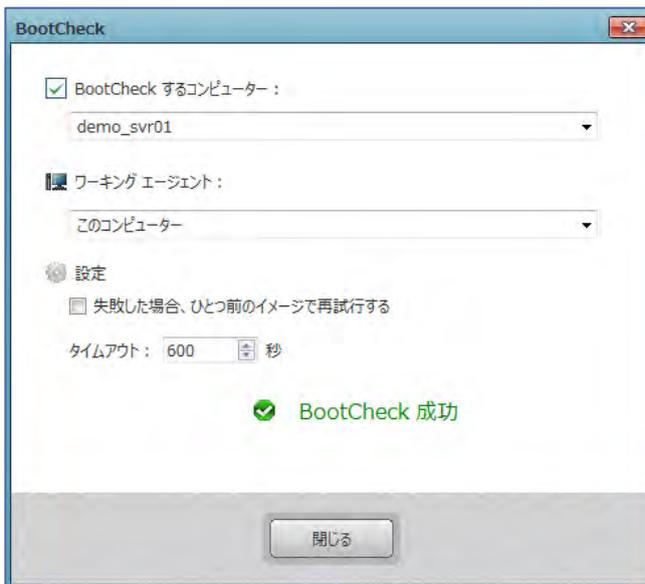
この例では、[ワーキング エージェント:] (起動確認を行うハイパーバイザー) は、「このコンピューター」 (ローカルの Hyper-V) を選択します。問題なければ、[BootCheck 開始] をクリックします。



3. 指定したバックアップの BootCheck が実行されます。



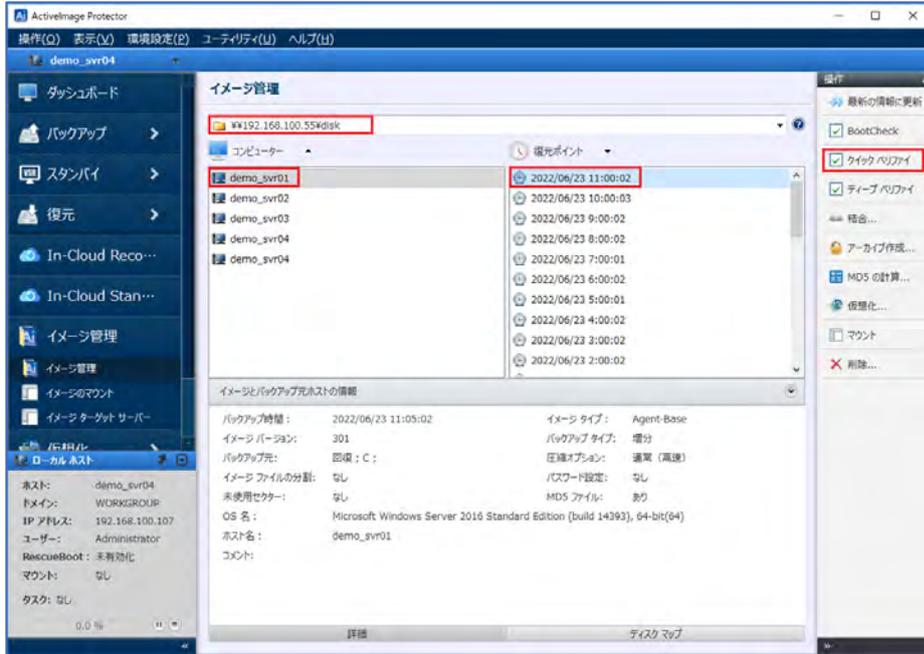
4. 以下のようになれば、BootCheck は完了です。  
任意のタイミングで、バックアップの復元直前などにも起動確認が行えます。



## 7-2. クイック ベリファイ

バックアップが作成時から改ざんされていないかの検証を行います。

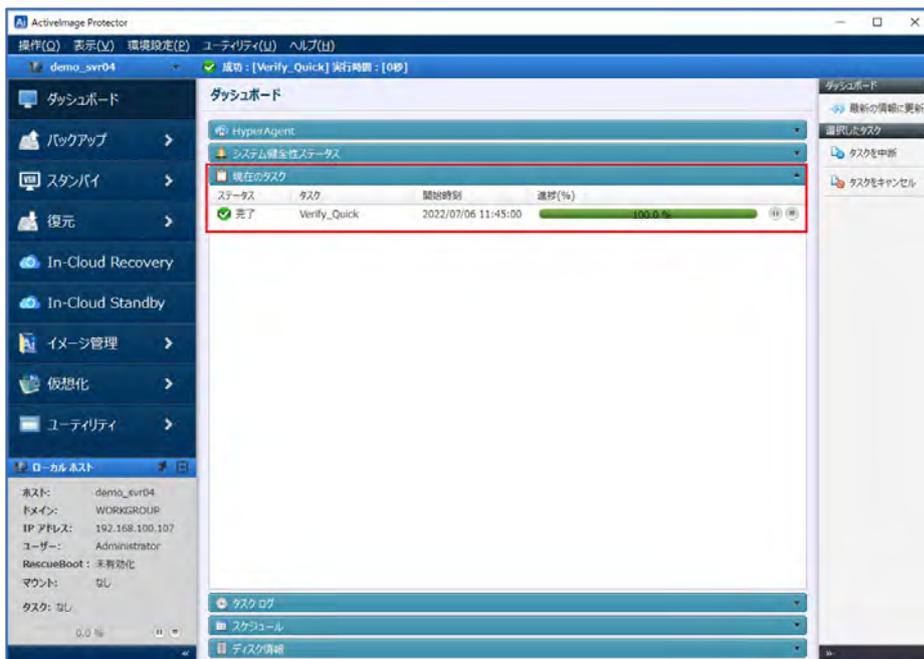
1. バックアップ元の [コンピューター] とバックアップの [復元ポイント] を指定したら、右のペインから [クイック ベリファイ] をクリックします。



2. [OK] をクリックするとバックアップの検証が開始されます。



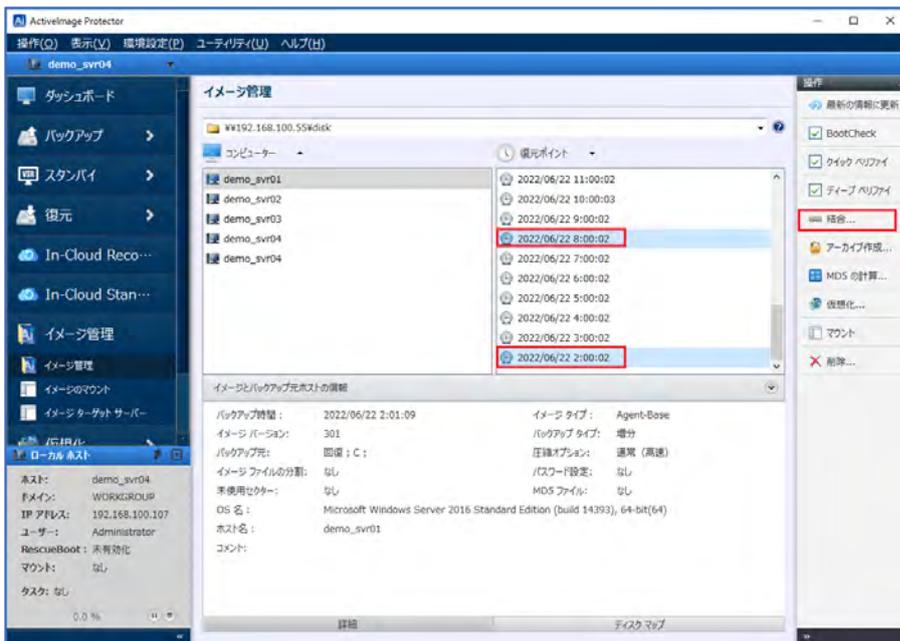
3. 検証が正常に完了すると、以下のようになります。



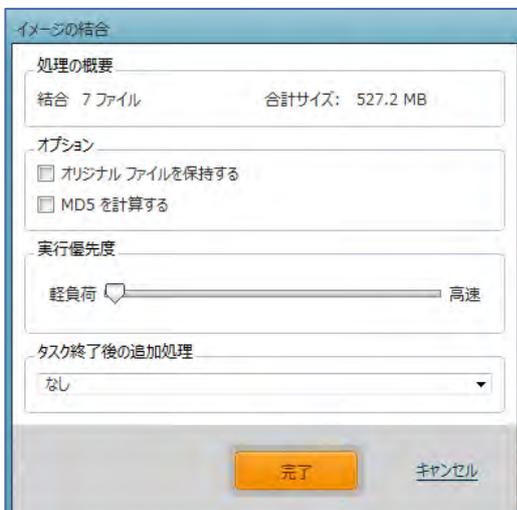
### 7-3. 結合

複数の増分イメージファイルを選択して1つのバックアップに結合することで、保存先の消費量を軽減することができます。

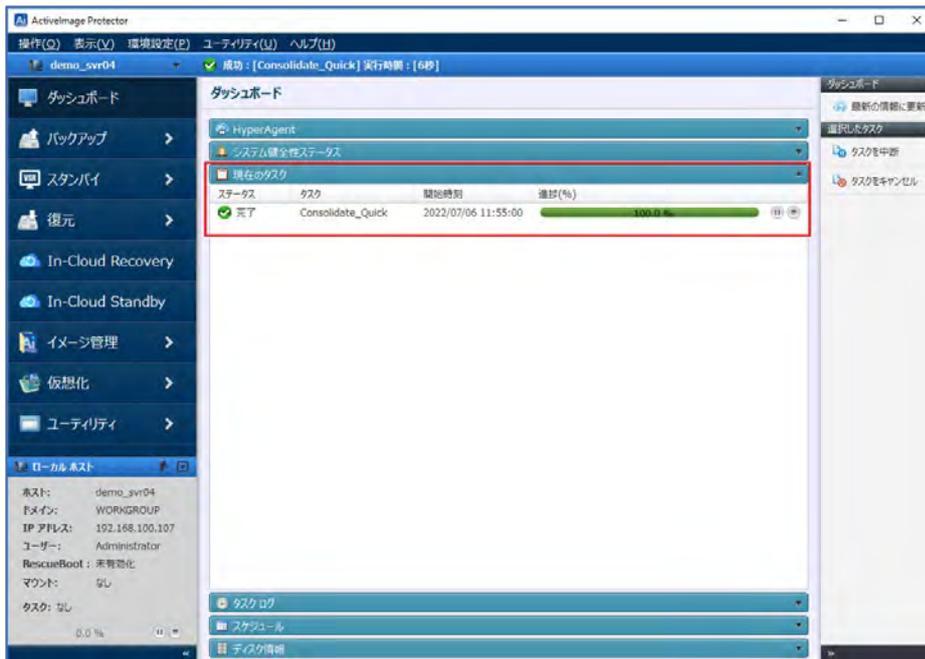
1. [復元ポイント] のリストから結合したい増分バックアップの始点と終点を選択してハイライトさせた後、[結合] をクリックします。  
 ここでの例として、始点の復元ポイントを [2022/06/22 2:00]、終点を [2022/06/22 8:00] とした、7つの増分イメージファイルを結合します。選択は、Ctrl、または Shift キーを押しながら [復元ポイント] を指定します。



2. 次に、オプションを設定します。  
 オリジナルのイメージファイルを保持する場合は、[オリジナル ファイルを保持する] のチェックボックスにチェックを入れます。



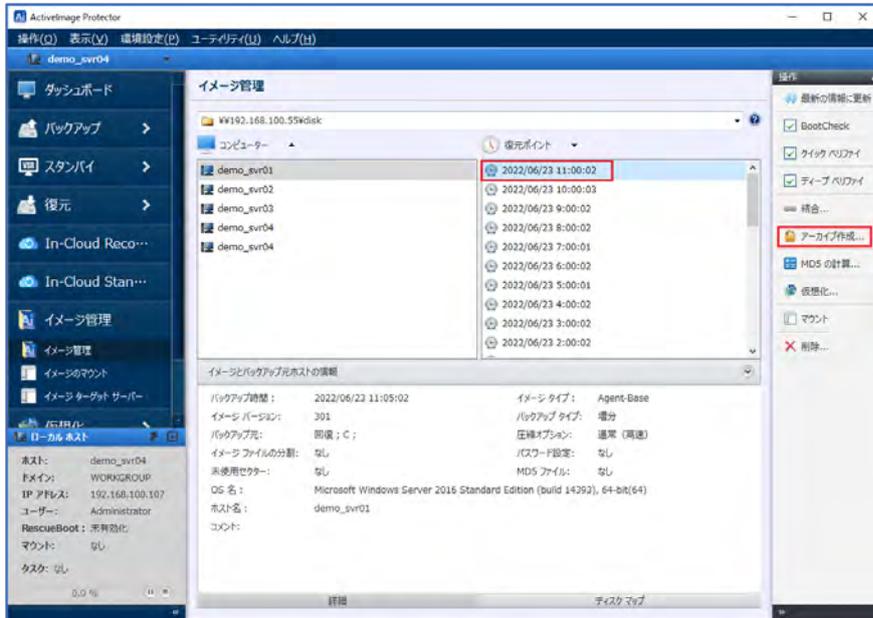
3. 結合が完了すると、以下のようになります。



## 7-4. バックアップのアーカイブ作成

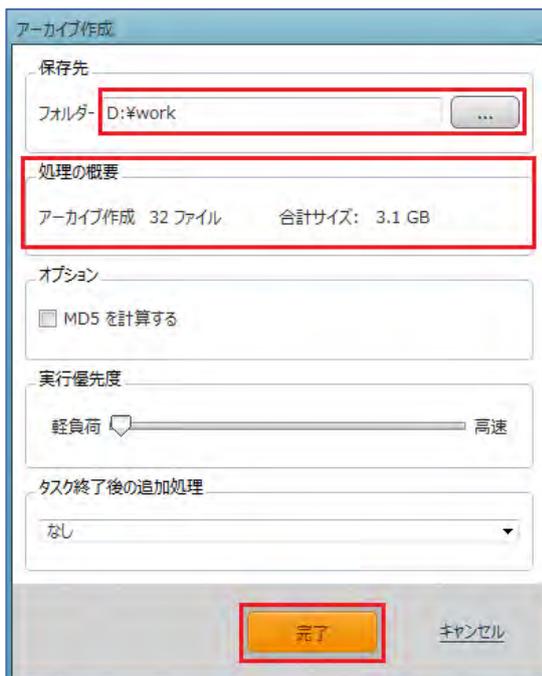
同一世代の指定した範囲のバックアップを統合して、指定した保存先に別名で作成することができます。

1. アーカイブの終点となる [復元ポイント] を選択してハイライトさせた後、 [アーカイブ作成...] をクリックします。同一世代のベースバックアップと指定した範囲の増分バックアップを統合した、アーカイブが作成されます。

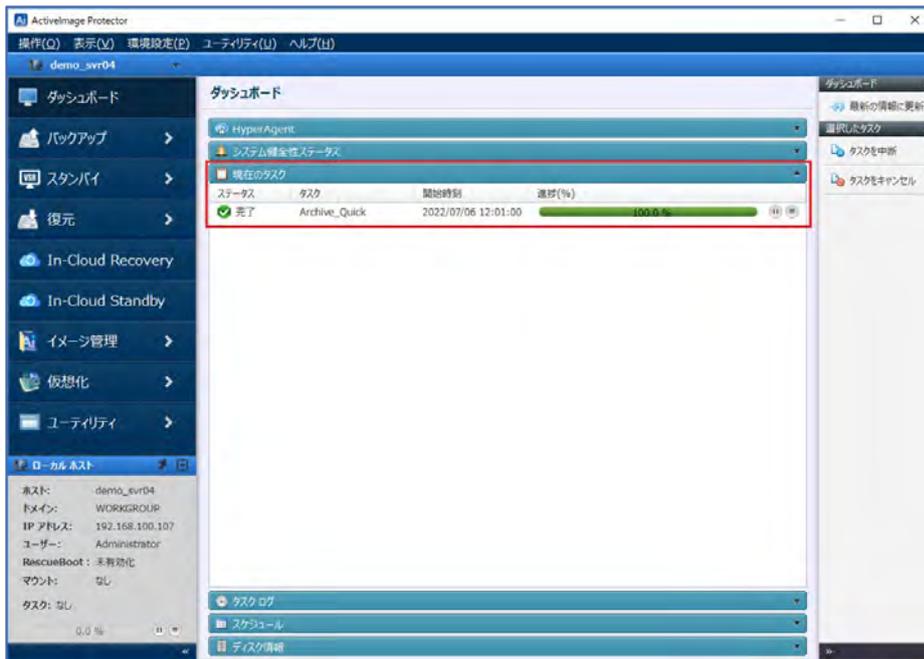


2. 以下のオプションが選択可能です。

処理の概要に選択したバックアップ数の合計とサイズが表示されますので、合計サイズを参考に作成するアーカイブ化したバックアップの保存先を指定します。 [完了] をクリックするとアーカイブ処理が開始されます。



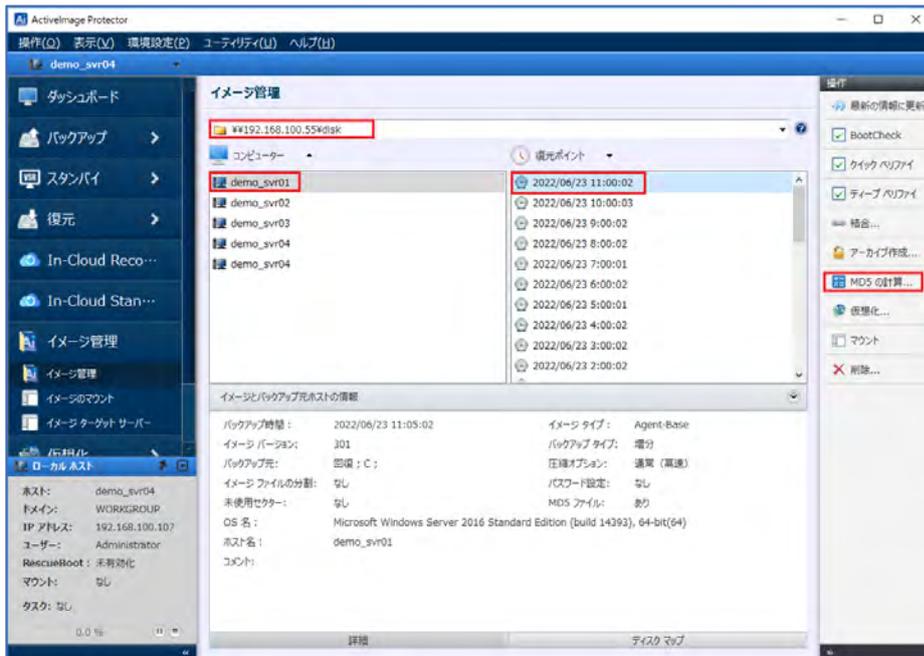
3. アーカイブが作成されると、以下のようになります。



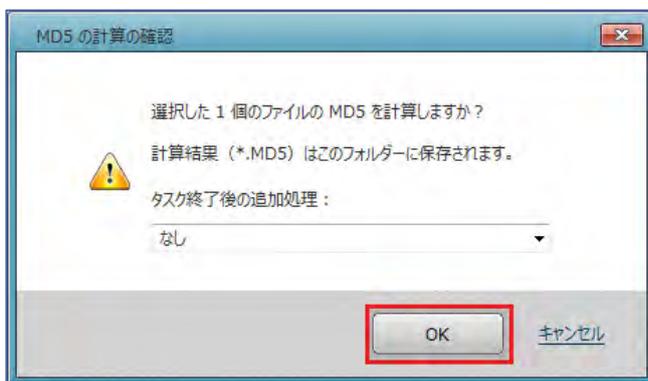
## 7-5. バックアップファイルの同一性確認（MD5 の計算）

選択したバックアップの MD5 ハッシュをファイルとして出力します。ファイルの同一性確認に使用できます。

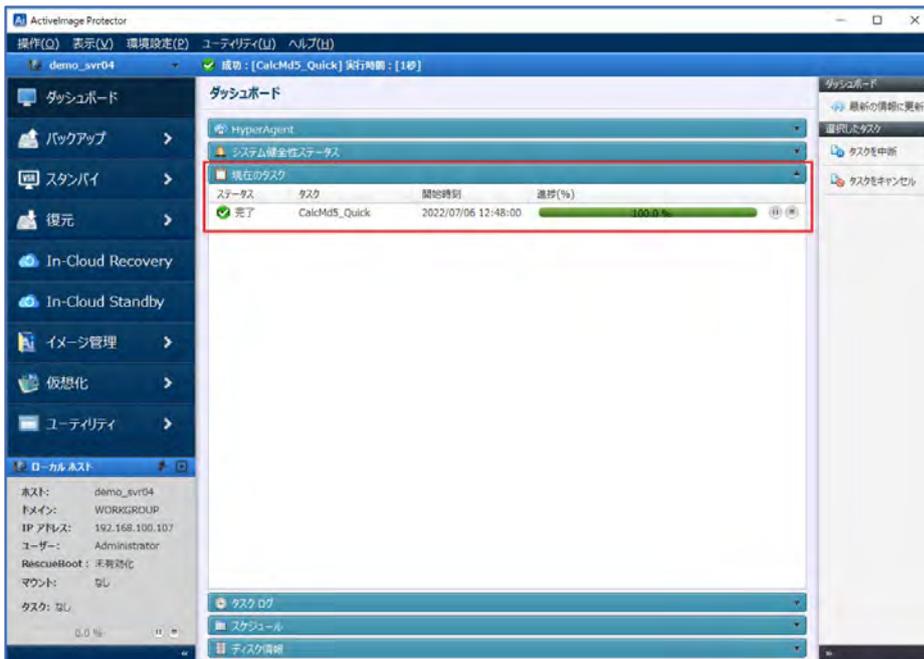
1. バックアップ元の [コンピューター] とバックアップの [復元ポイント] を選択してハイライトさせた後、[MD5 の計算...] をクリックします。複数のバックアップの MD5 ハッシュ値を求める場合は、Ctrl、または Shift キーを押しながら選択します。



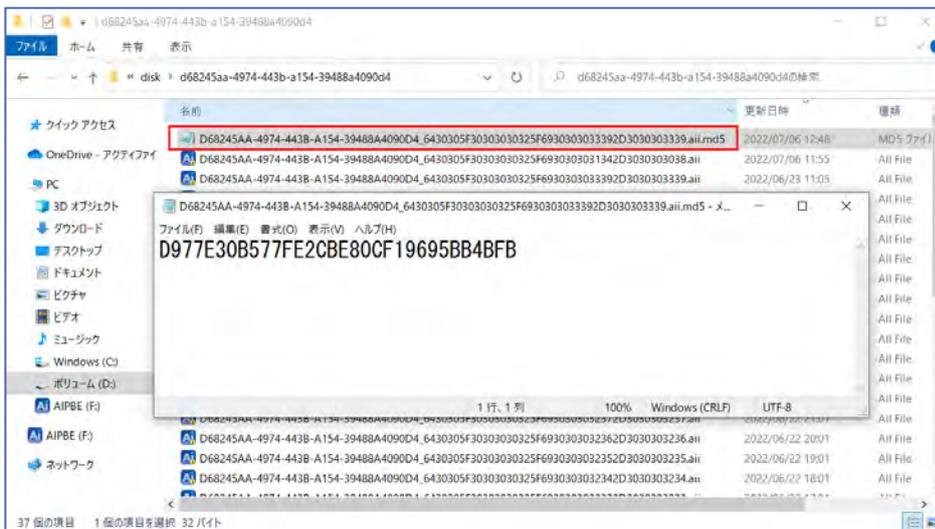
2. [OK] をクリックします。



3. MD5 の計算の出力が行われると、以下のようになります。



4. 作成された MD5 ファイルを Windows 上で確認します。

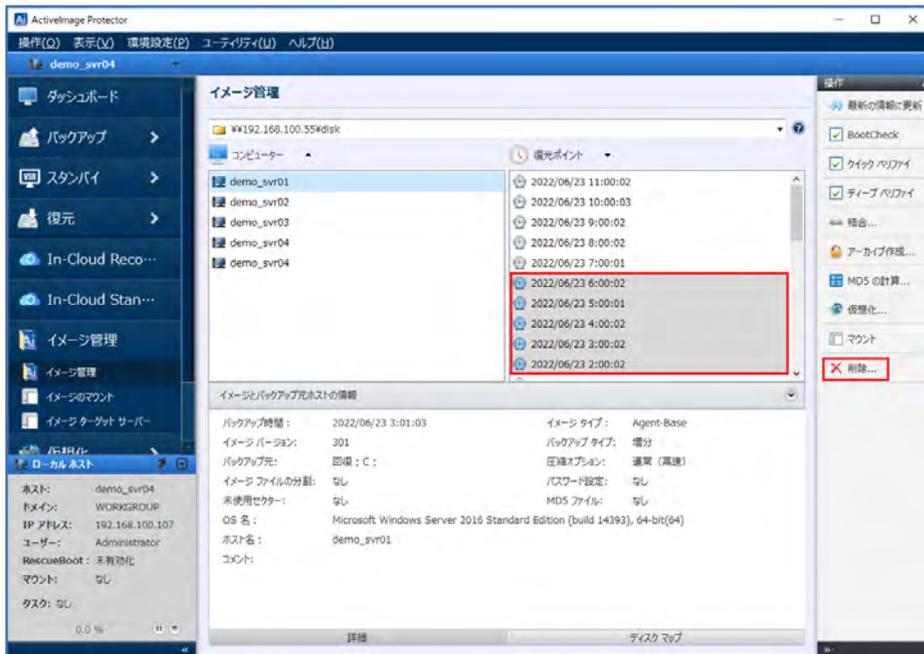


## 7-6. バックアップファイルの削除

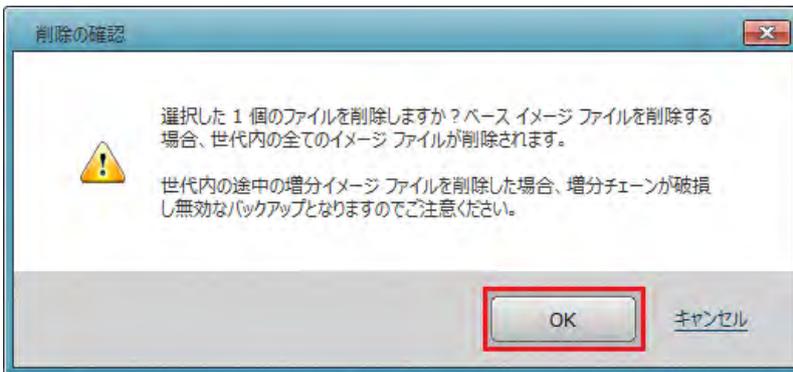
指定したバックアップファイルを削除します。

注意：処理実行後のキャンセルはできませんので慎重に操作してください。

1. 削除したいバックアップの [復元ポイント] を選択してハイライトさせた後、[削除...] をクリックします。複数のバックアップを削除したい場合は、Ctrl、または Shift キーを押しながら選択します。



2. [OK] をクリックすると指定したバックアップが削除されます。

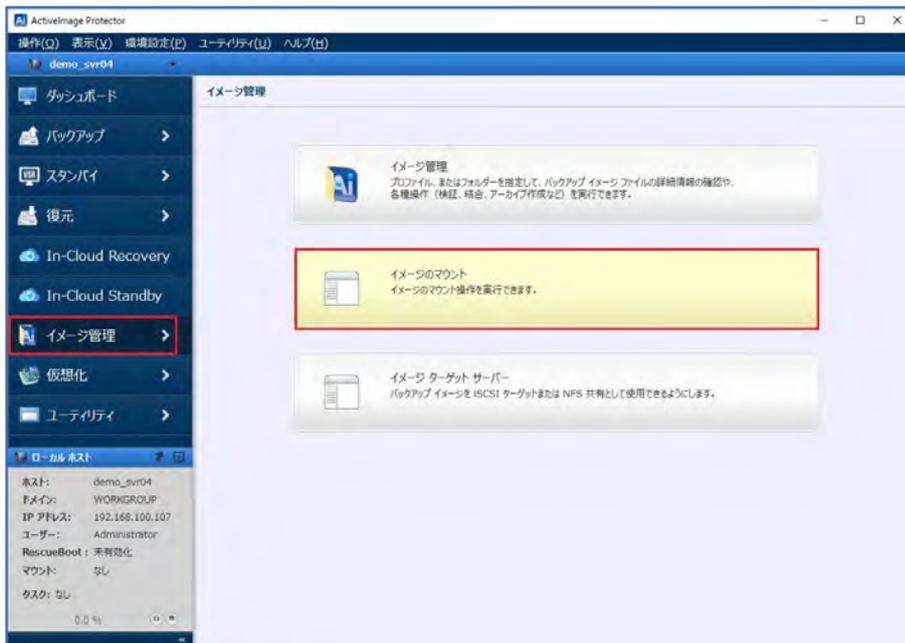


## 8. イメージ管理：イメージのマウント

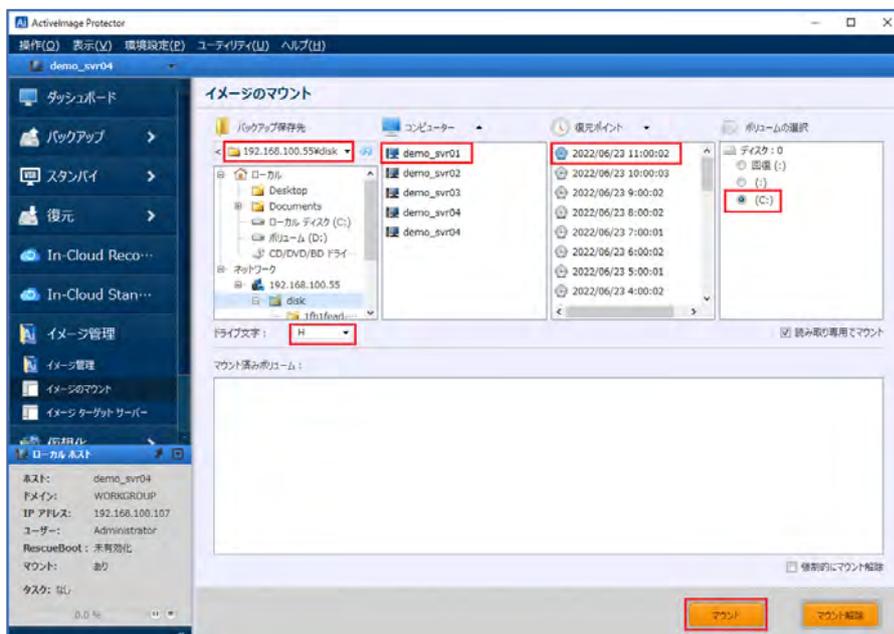
バックアップを OS のファイルシステムとして、ドライブレターをつけてマウントします。ファイルやフォルダのコピーや追加を行うことができます。

1. イメージマウントを起動します。

[イメージ管理] → [イメージのマウント] を選択します。

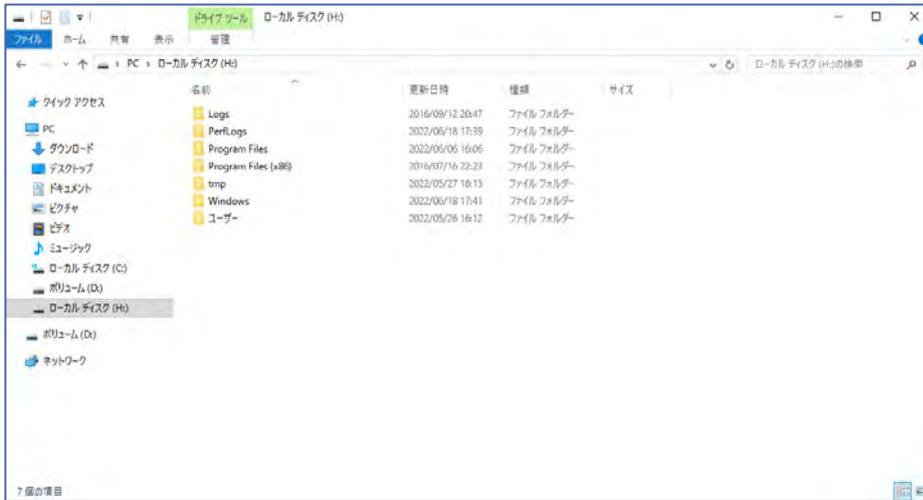


2. マウントしたいマシンのバックアップの復元ポイントを選択します。複数のディスクが含まれている場合は、マウントするバックアップ中のボリュームを選択します。マウント先のドライブレターを指定して [マウント] をクリックします。[読み取り専用でマウント] のチェックボックスにチェックを入れると、読み取り専用でマウントできます。

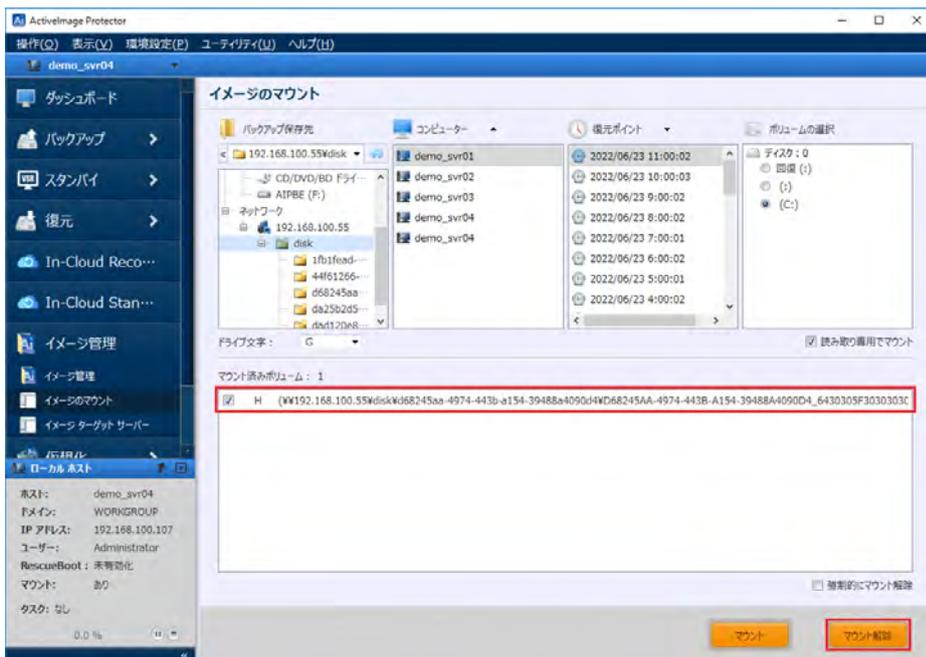


## イメージ管理：イメージのマウント

- マウントすると、以下のようになります。通常の読み取り専用ドライブと同様にファイルのオープンやコピーができます。



- マウントを解除するには、[マウント済みボリューム] から解除するマウントを選択します。その後、[マウント解除] をクリックします。



- ※ 読み取り専用のチェックをはずすと書き込み可になります。更新したデータは別の差分ファイル (.aix) として保存されます。

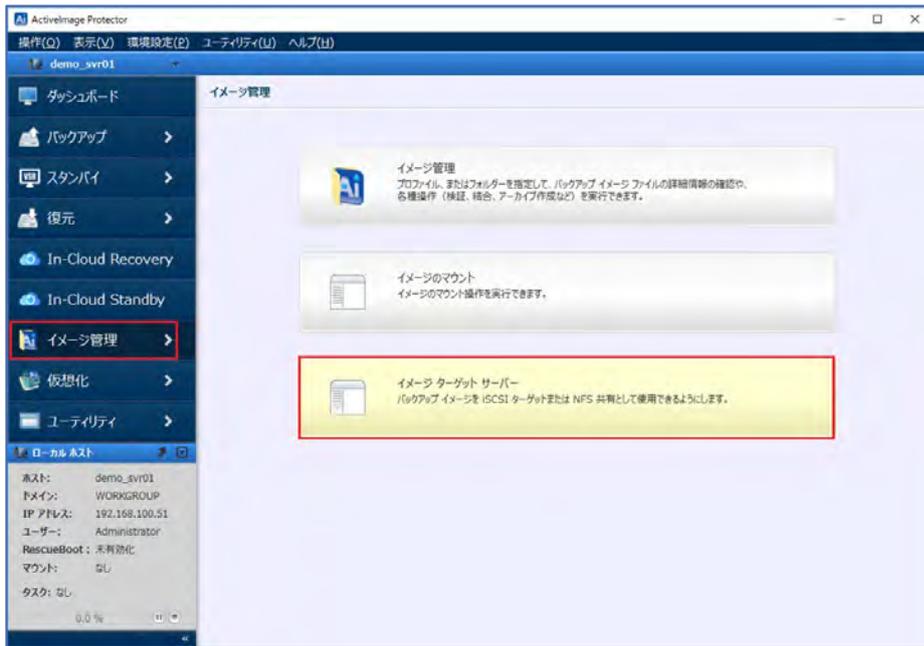
## 9. イメージ管理：イメージ ターゲット サーバー

バックアップを iSCSI、または NFS ターゲット サーバーとして設定できます。

ここでの例として、バックアップを iSCSI ターゲット サーバーとして設定します。iSCSI ターゲットを直接、ローカルディスクにすることで、そのままローカルのファイルシステムとして利用することができます。

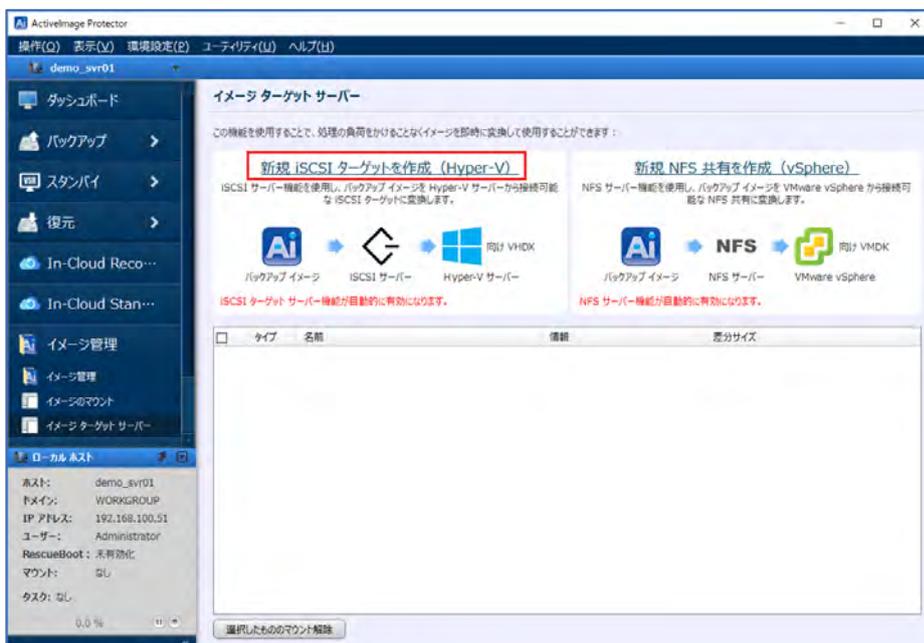
1. イメージ ターゲット サーバーを起動します。

左ペインから、[イメージ管理] → [イメージ ターゲット サーバー] を選択します。

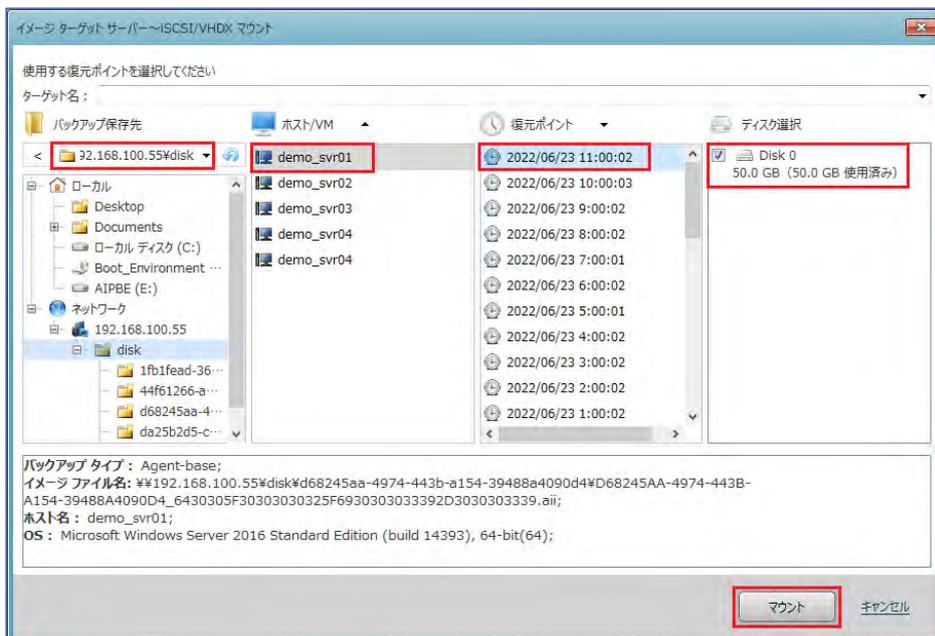


2. イメージ ターゲット サーバーの設定画面になります。

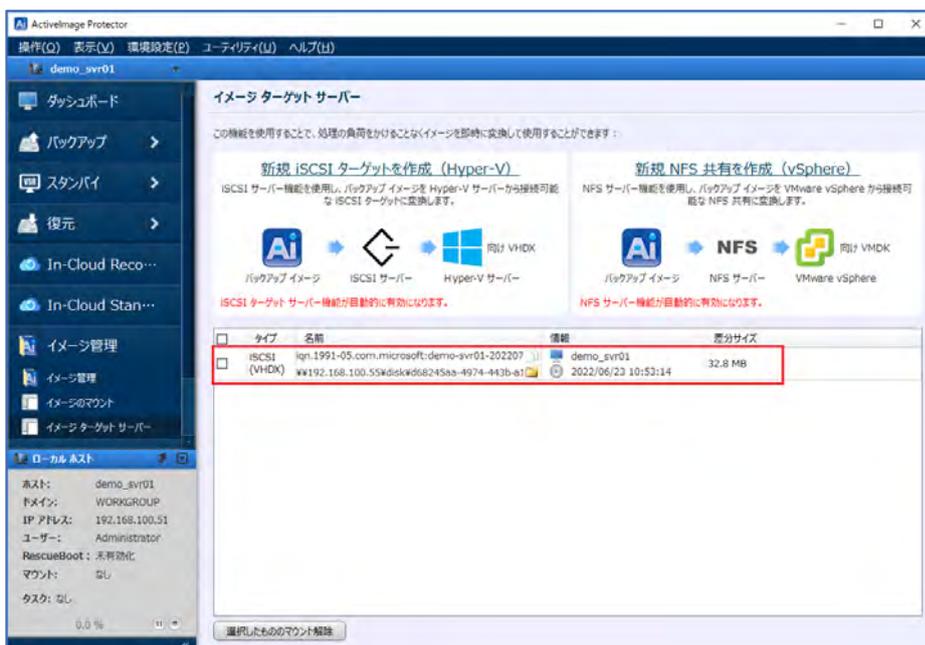
[新規 iSCSI ターゲットを作成 (Hyper-V)] をクリックします。



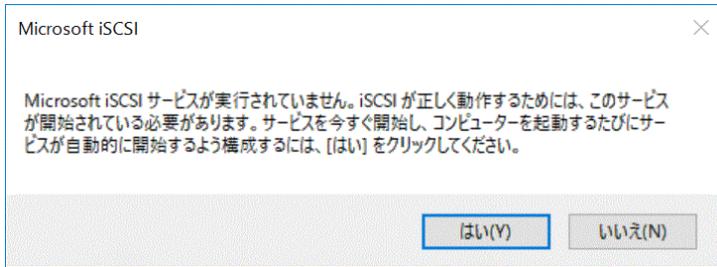
- 対象マシンのバックアップの復元ポイントとディスクを選択して、[マウント] をクリックします。複数のディスクが含まれている場合は、対象のディスクを選択します。



- マウント実行後、接続を行うコンピューターから iSCSI イニシエーターで接続すると、指定したバックアップを iSCSI ディスクとして扱うことができます。



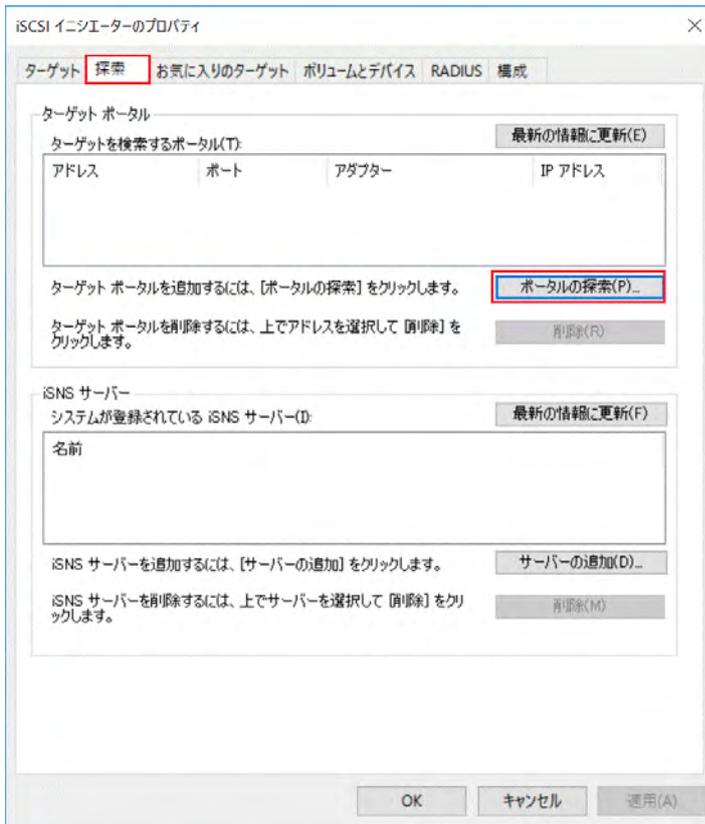
- 次に、iSCSI ターゲットを接続するサーバーに移ります。  
Windows スタートメニューから、[iSCSI イニシエーター] を選択します。
- 初回起動時には、以下の確認メッセージが表示されますので、[はい] をクリックします。



- iSCSI イニシエーターが起動します。

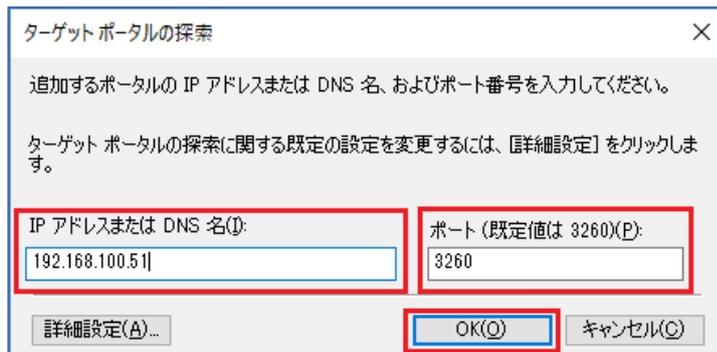


8. [探索] タブを選択します。次に、[ポータルの探索] をクリックします。

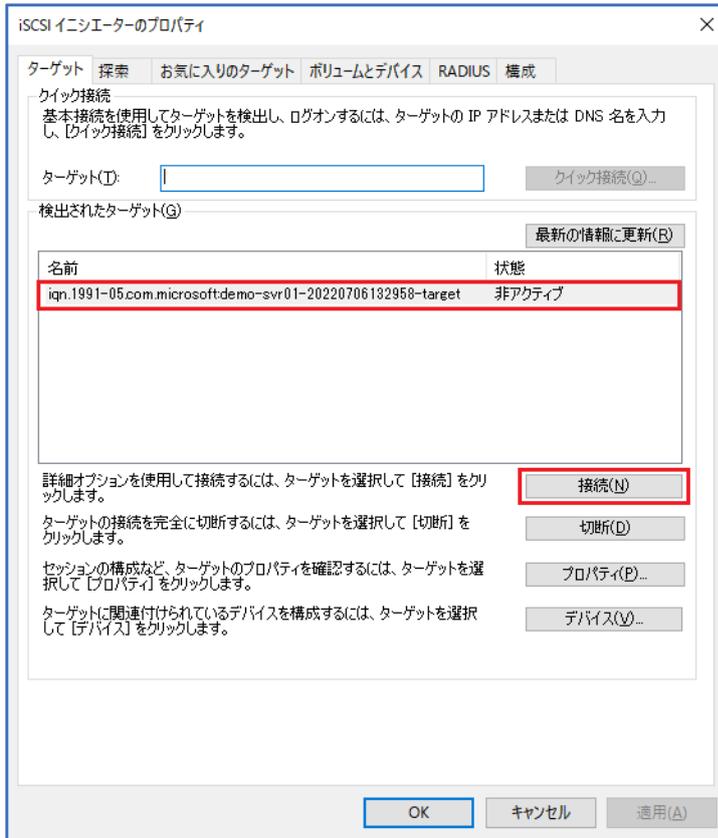


9. ターゲットポータルの探索となります。

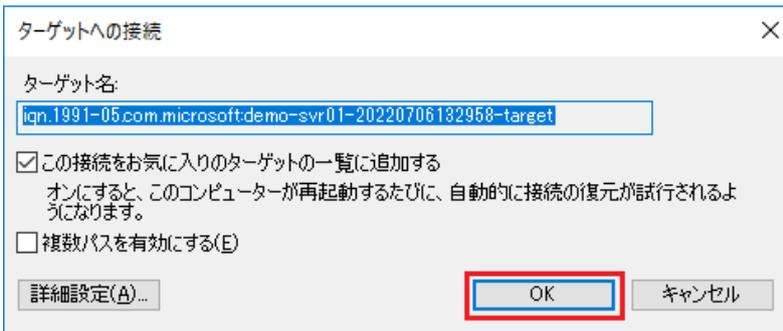
ここでの例では、[IP アドレスまたは DNS 名] は、iSCSI ターゲット化したサーバーの IP アドレス「192.168.100.51」を入力します。[ポート] は、デフォルトの「3260」のまま、[OK] をクリックします。



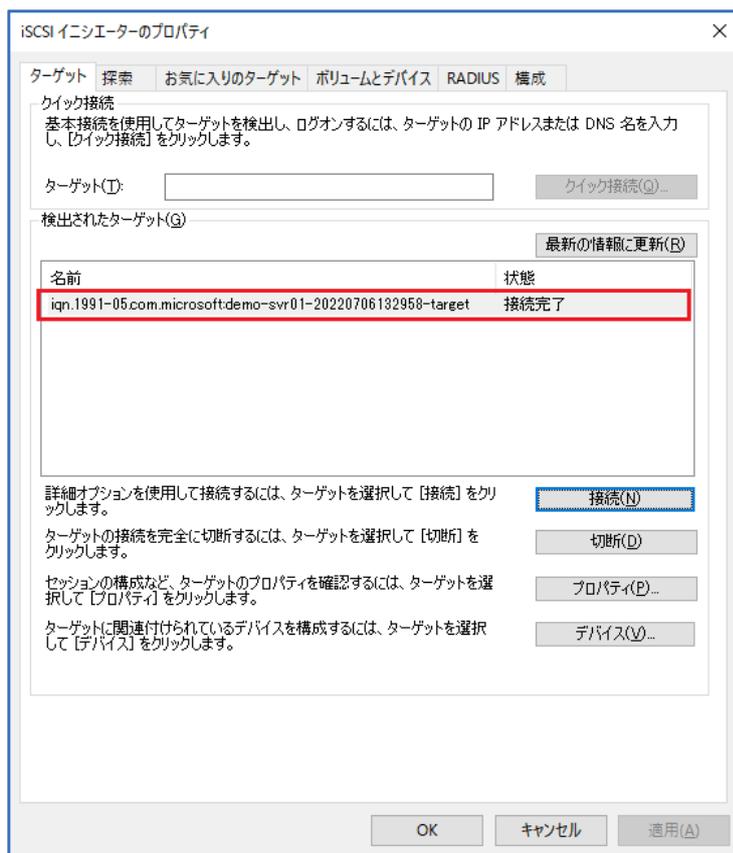
10. 再度、[ターゲット] タブに戻ります。[検出されたターゲット] に、iSCSI ターゲットが表示されます。  
[接続] をクリックします。



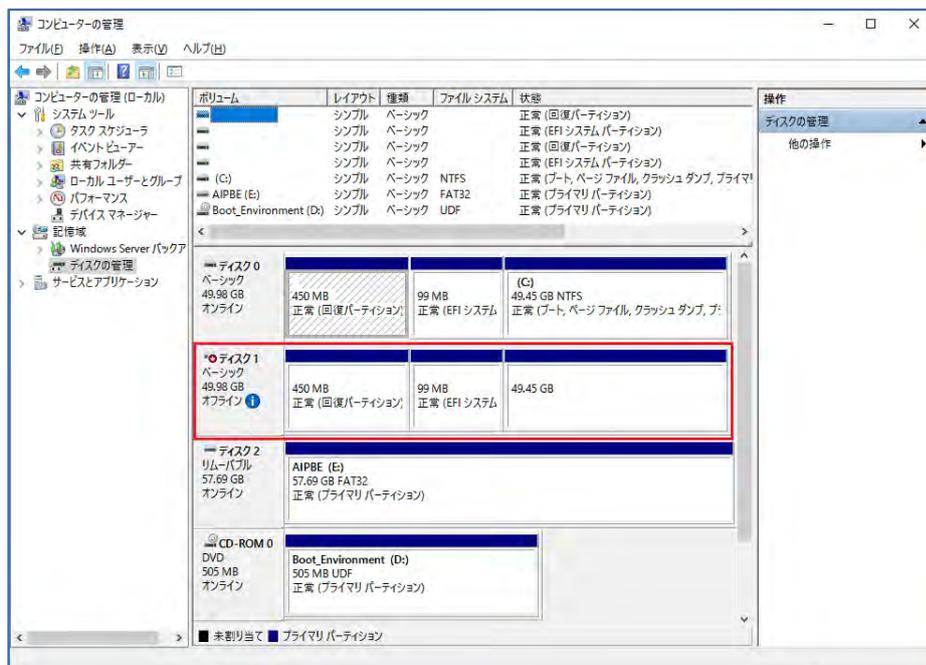
11. ターゲットへの接続では、デフォルトで、[この接続をお気に入りのターゲットの一覧に追加する] のチェックボックスにチェックが入っています。その下の説明にもあるように、このサーバーが起動されるたびに、この iSCSI ターゲットが接続されるようになります。[OK] をクリックすると、接続されます。



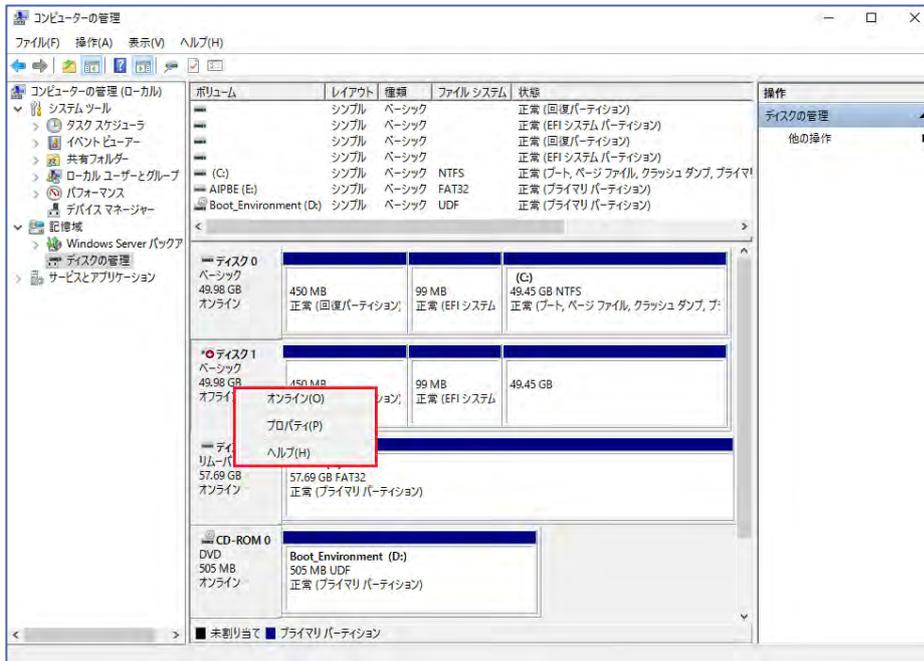
12. [ターゲット] タブの [検出されたターゲット] の [状態] が「接続完了」に変わっています。



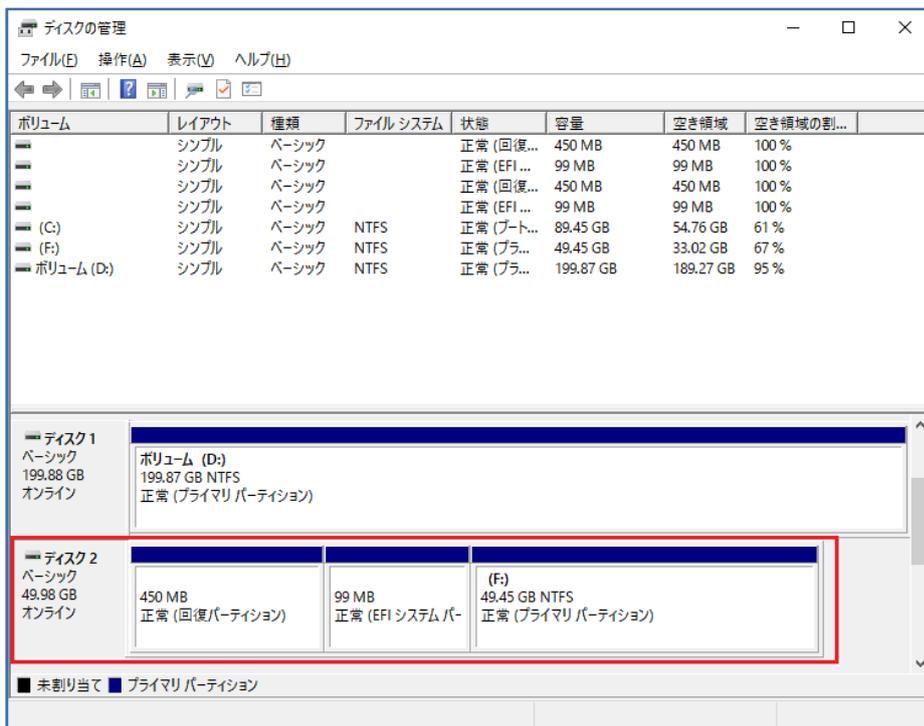
13. 次に、管理ツールから [コンピューターの管理] を起動し、左のメニューから [ディスクの管理] を選択します。ディスク 1 が追加され、オフライン状態であることがわかります。



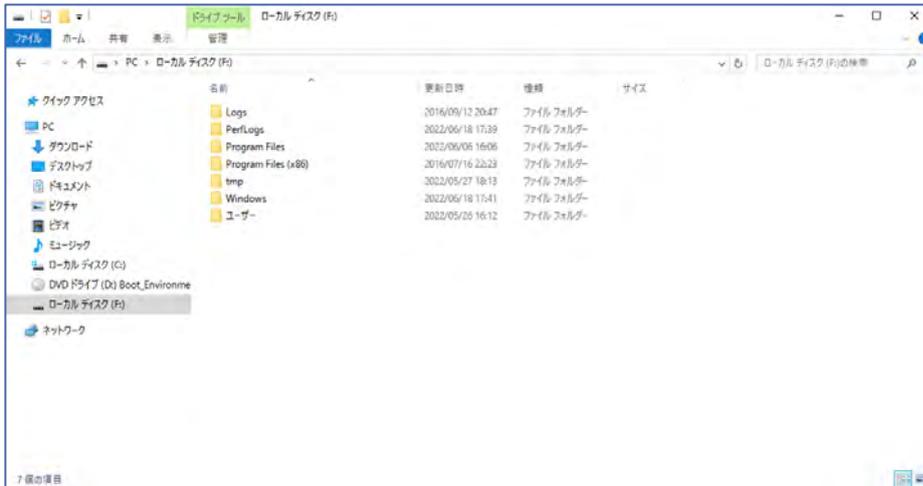
14. ディスク 1 のあたりを右クリックすると、以下のようなコンテキストメニューが表示されます。ここから、[オンライン] を選択すると、ローカルディスクとして認識されます。



15. ローカルディスクとして認識され、パーティションにドライブレターが割り当てられています。

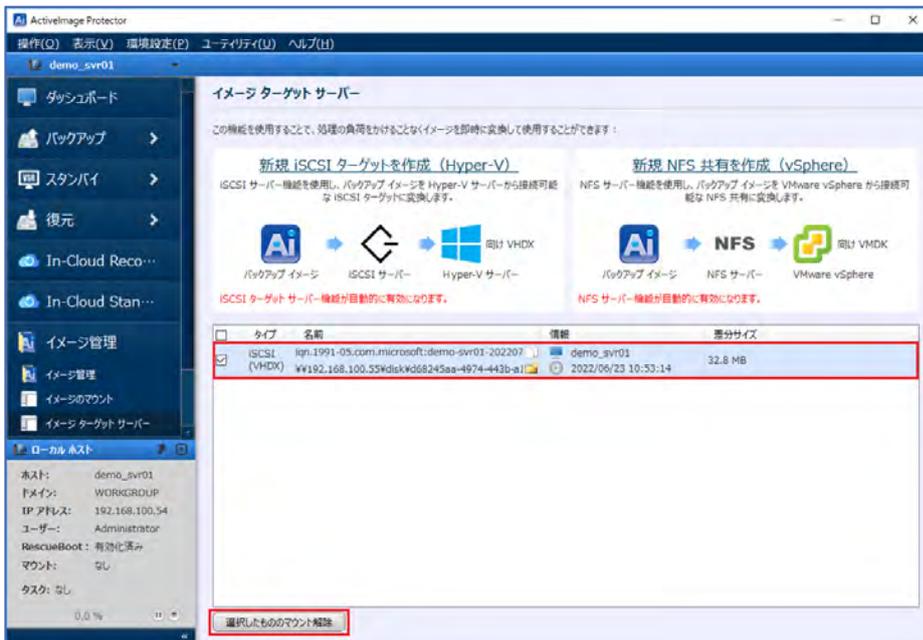


16. 実際に、ファイルエクスプローラーで表示すると、以下のようになります。



17. 使用が終了した後はイニシエーターから切断してください。

接続を解除する iSCSI ターゲットのチェックボックスにチェックを入れて、[選択したもののマウント解除] をクリックします。「セッション上のデバイスが使用中のため、セッションをログアウトできません。」と表示され切断ができない場合は、[ディスクの管理] で接続している iSCSI ディスクをオフラインに変更してから切断を試行してください。



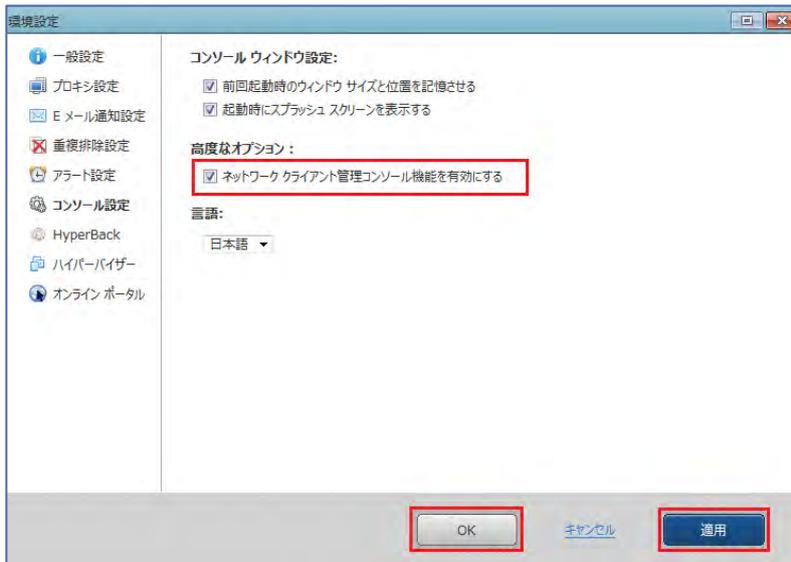
## 10. リモート管理コンソール

ネットワーク上のホストにインストールされている AxiImage Protector の管理をリモートで行うことができます。

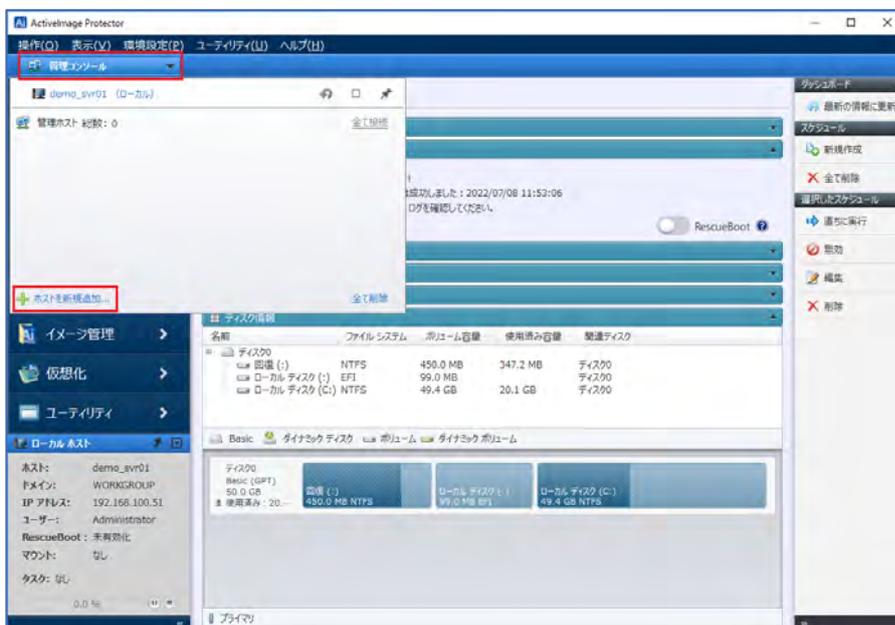
1. AxiImage Protector を起動します。

Windows スタートメニューから [Actiphy] → [AxiImage Protector] をクリックします。

2. 最初に、環境設定の [コンソール設定] → [ネットワーク クライアント管理コンソール機能を有効にする] のチェックボックスにチェックを入れ、[適用] をクリックします。[OK] をクリックしてダッシュボードに戻ります。

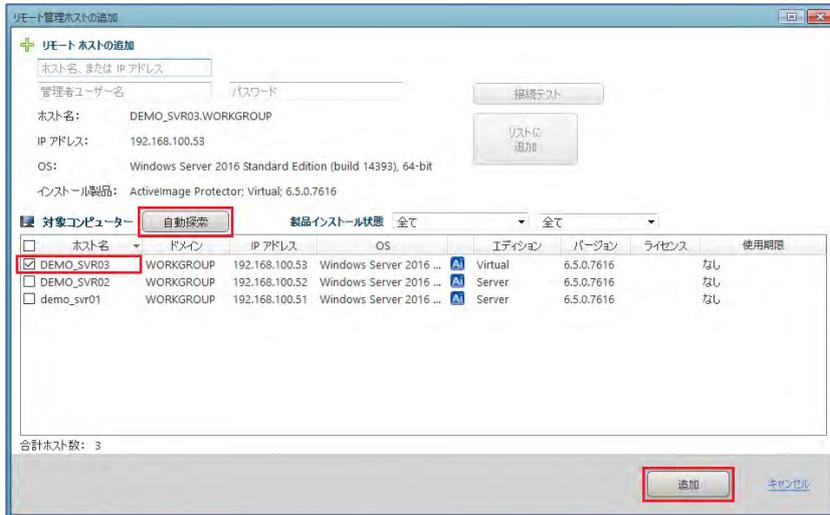


3. コンソール左上にある [管理コンソール] から操作を行います。リモート管理を行うためには、最初にホストリストを作成します。[ホストを新規追加] をクリックします。

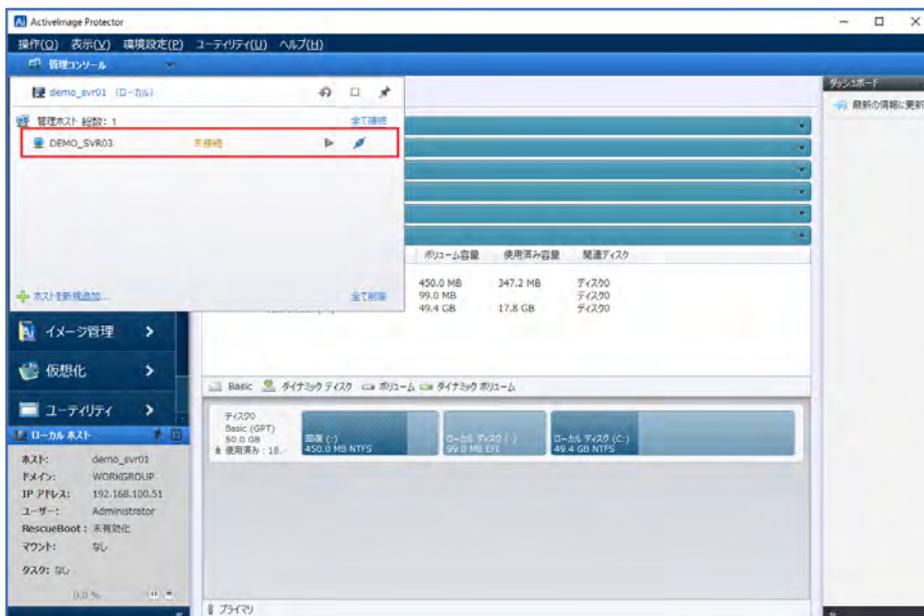


## リモート管理コンソール

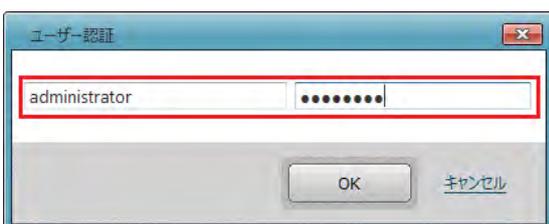
- リストに追加するホストを指定します。指定方法は [検索] と [手動設定] の2つがあります。この例では [検索] を選択し、検索条件で [全てのホストを検索] を選択しました。ホスト一覧から ActiveImage Protector がインストールされているホスト (DEMO\_SVR03) のチェックボックスにチェックを入れ、 [追加] をクリックします。



- 管理対象ホストとして、リモートホストが追加されます。ホストリストから任意のホストを選択し、ダブルクリックすると認証が行われます。

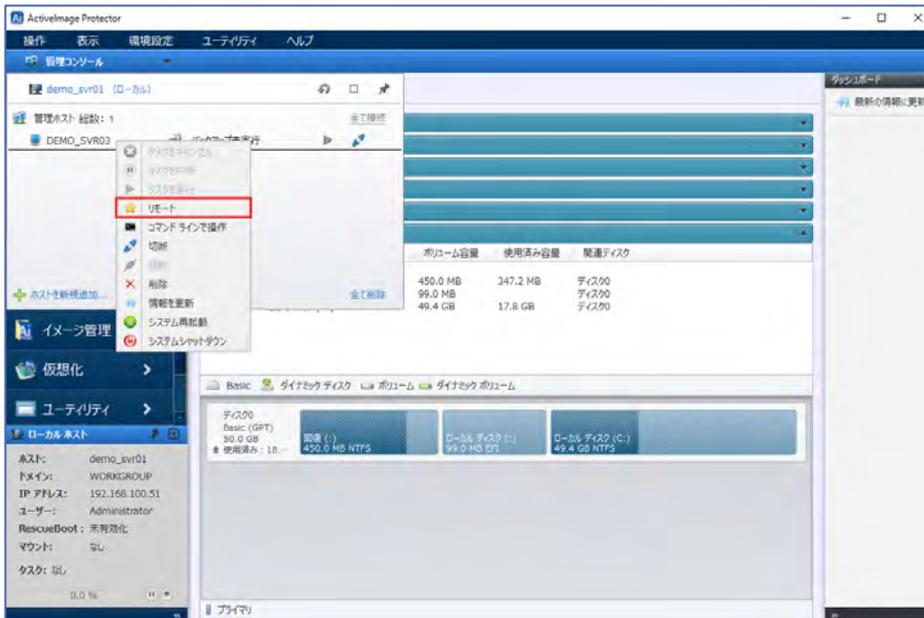


- リモート管理するホストの認証情報を入力します。

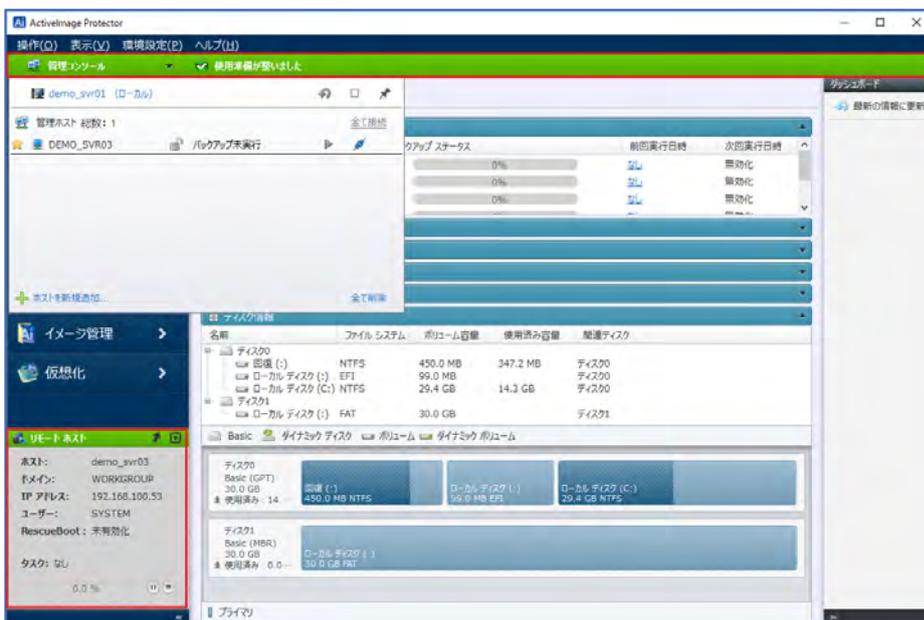


## リモート管理コンソール

7. ホストリストから任意のホスト選択し、右クリックメニューから [リモート] をクリックするとエージェントにリモート接続できます。



8. 接続に成功すると、ステータスバーの色が緑になります。バックアップスケジュールの作成や復元、イメージ管理などの各種操作、ログ等の閲覧ができます。ローカルホスト名をダブルクリックするとリモートホストへの接続を解除します。



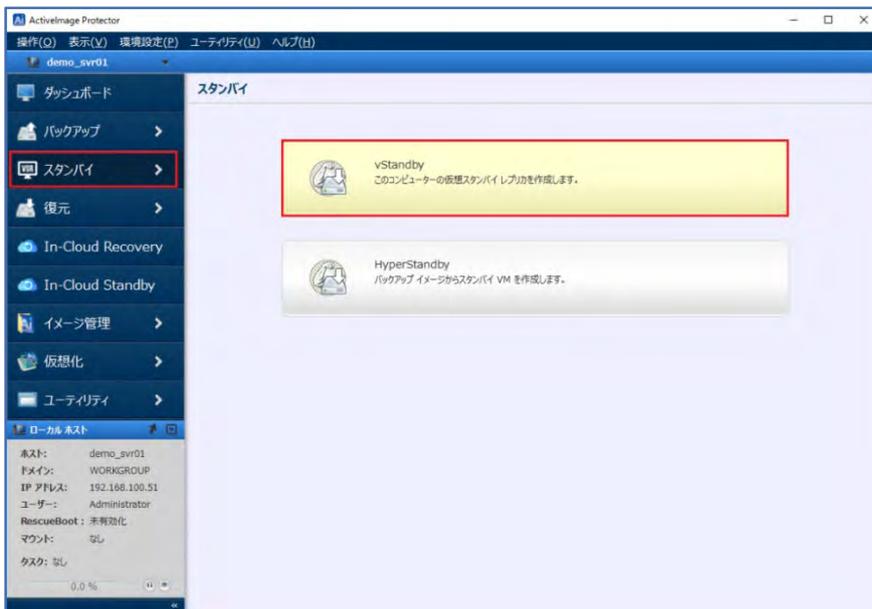
## 11.仮想スタンバイ（待機）マシンの作成

### 11-1. vStandby

ソースマシンのディスクから、ハイパーバイザー上に即時起動が可能な仮想スタンバイレプリカを作成することができます。スケジュール機能を使い、ソースマシンのディスクの更新状態を、仮想スタンバイマシンのブートポイントとして追加します。緊急時には、仮想スタンバイマシンを起動し、代替のサーバーとして利用することができます。ここでは、vStandby のバックアップ設定手順について説明します。

#### 1. vStandby を起動します。

左のメニューから [スタンバイ] → [vStandby] をクリックします。



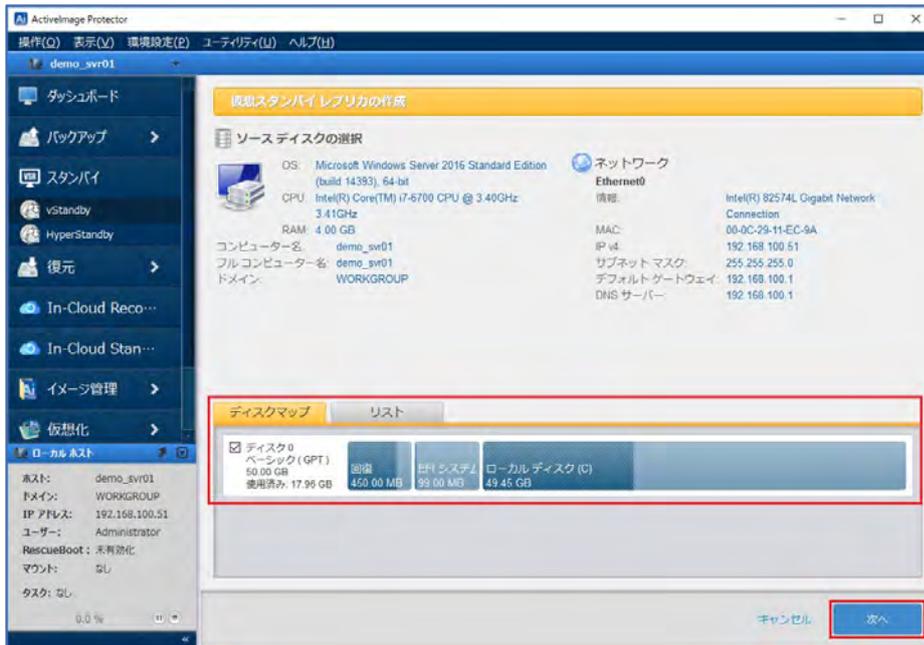
#### 2. ようこそ！画面が表示されますので、[仮想スタンバイレプリカの作成] をクリックします。



## 仮想スタンバイ（待機）マシンの作成

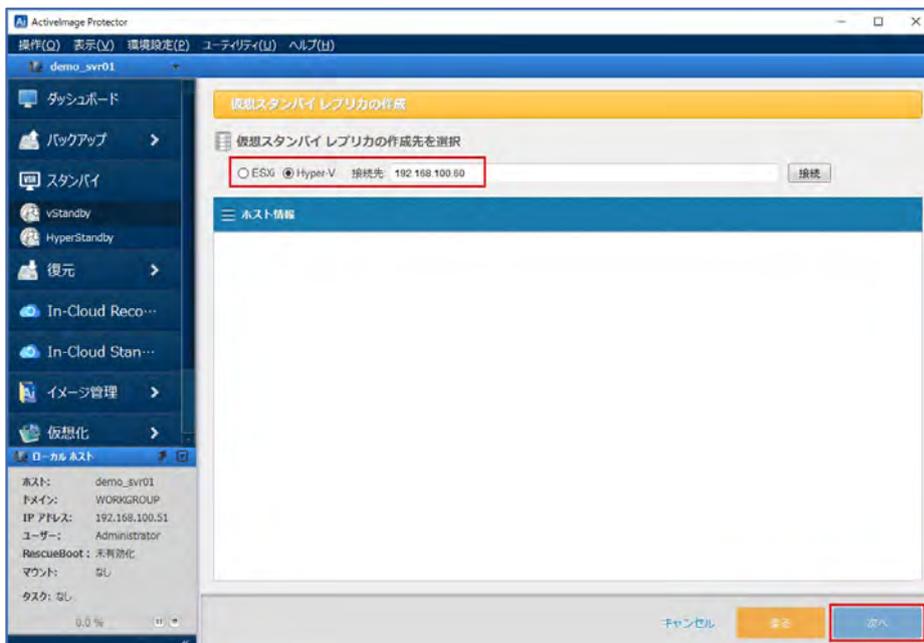
### 3. ソースディスクを選択します。

ここで選択したディスクのレプリカが仮想マシン上に作成されます。ディスクマップ、または、リストでバックアップ対象にするディスクのチェックボックスにチェックを入れ、[次へ] をクリックします。



### 4. 仮想スタンバイレプリカの作成ターゲットを ESXi、Hyper-V から選択します。

ここでの例では、[Hyper-V] を選択し [接続先:] には、Hyper-V ホストの「192.168.100.60」を入力して [接続] をクリックします。

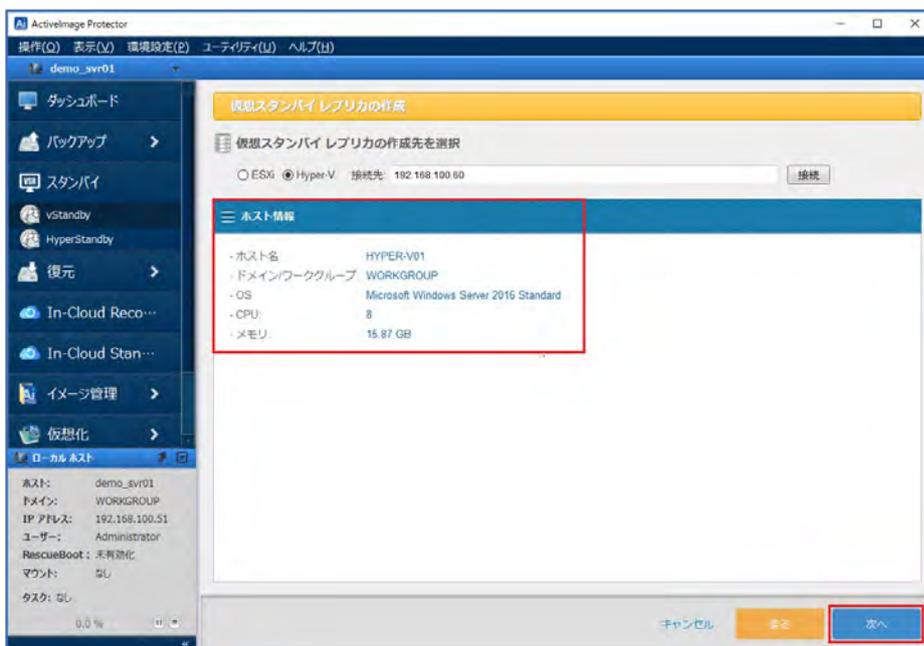


## 仮想スタンバイ（待機）マシンの作成

5. 認証画面となりますので、Hyper-V ホストの認証情報を入力します。[ユーザー名:] に「Administrator」、[パスワード:] に設定されたパスワードを入力します。

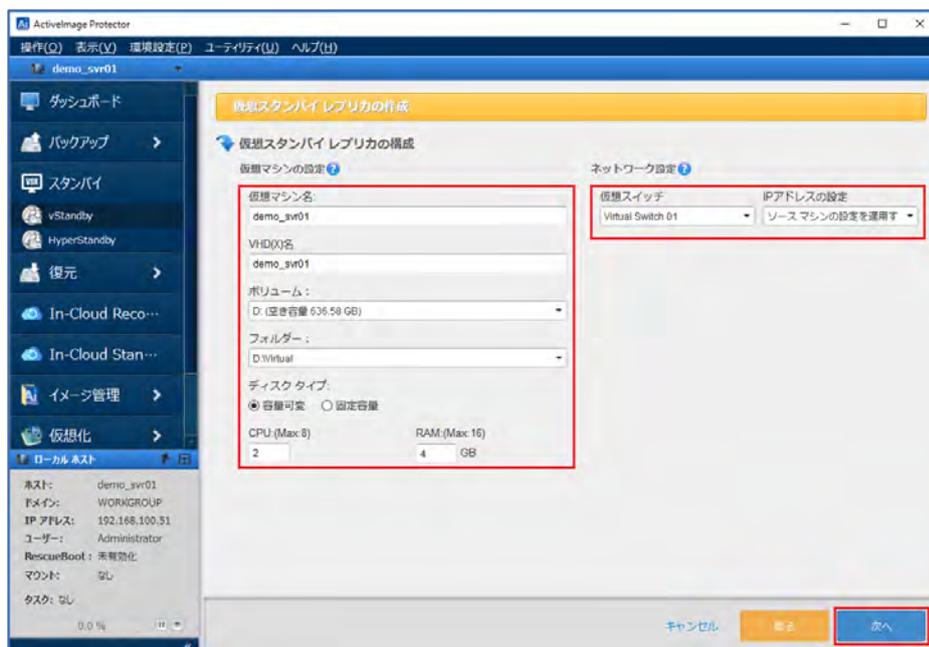


6. Hyper-V の「ホスト情報」が表示されます。[次へ] をクリックします。

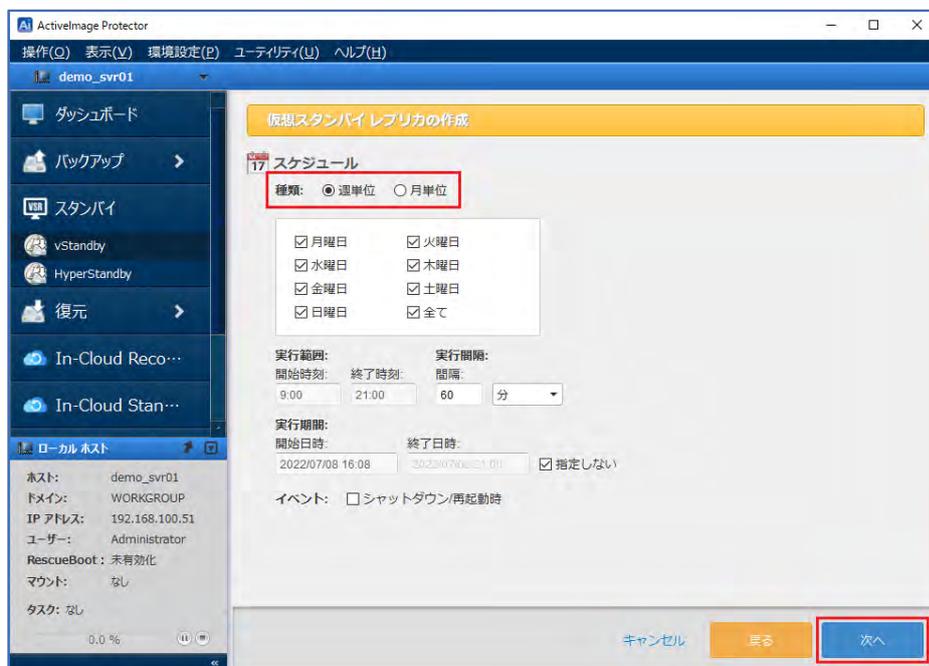


## 仮想スタンバイ（待機）マシンの作成

7. スタンバイレプリカの仮想マシンの各種設定を行います。[仮想マシン名:]、[仮想ディスク名:]、[ボリュームの選択:]、[ディスクタイプ:]、ハードウェアリソースを設定します。ネットワーク設定では、[仮想スイッチ]、[IP アドレス] 設定を行います。[次へ] をクリックします。[仮想スイッチ] は、ホスト側に作成した仮想スイッチ、IP アドレスは「ソースマシンの設定を引き継ぐ」を設定します。

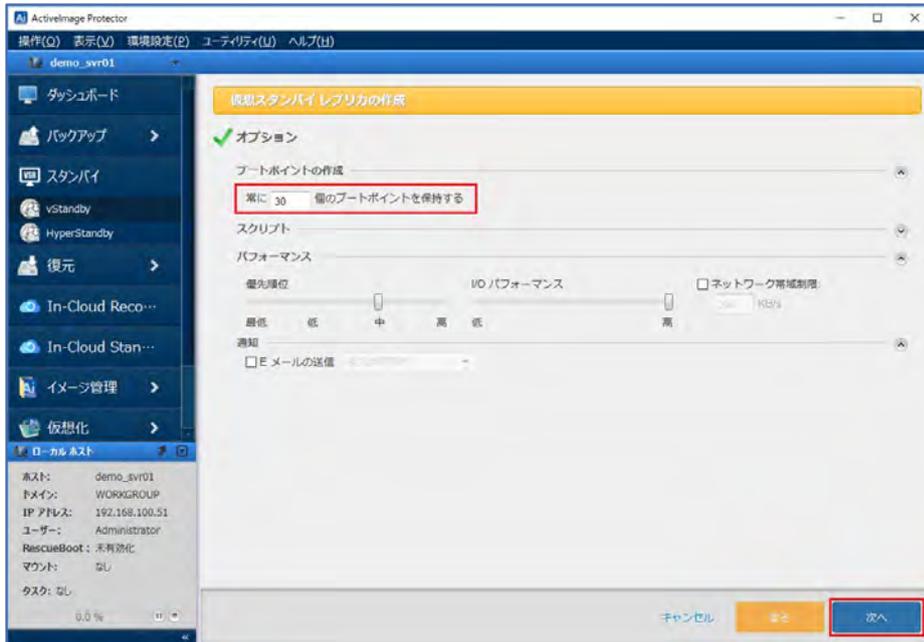


8. 仮想スタンバイレプリカの増分ブートポイントを作成するためのスケジュールを、週単位、もしくは月単位で設定します。以下は、週単位での設定画面です。毎日、9:00 から 21:00 の間に 60 分間隔で実行されます。スケジュールを設定したら、[次へ] をクリックします。

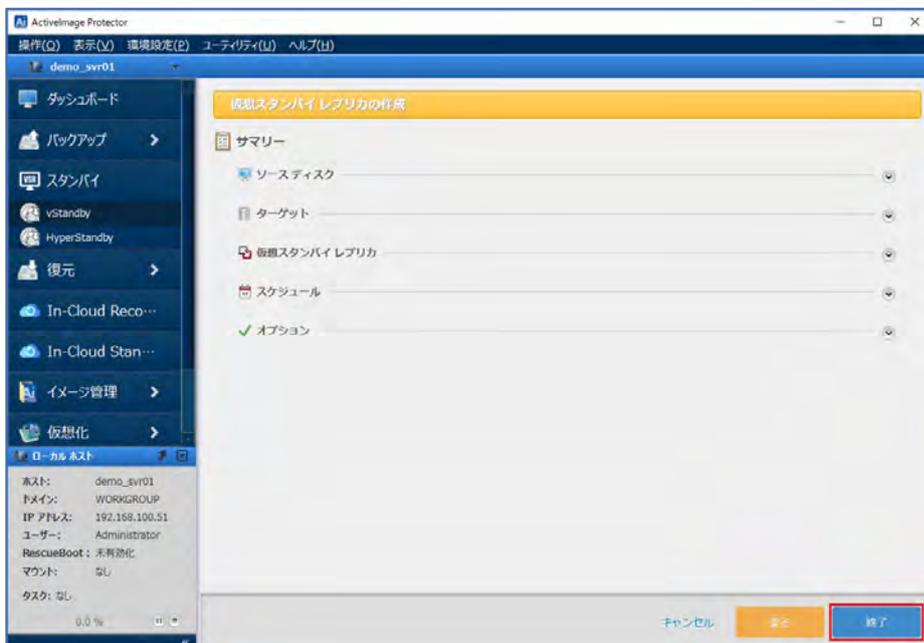


## 仮想スタンバイ（待機）マシンの作成

9. オプションの設定をします。ブートポイントは最大 30 個作成できます。ブートポイントが指定した数に達すると、いちばん古いものと 2 番目に古いものがマージされます。設定が完了したら、[次へ] をクリックします。

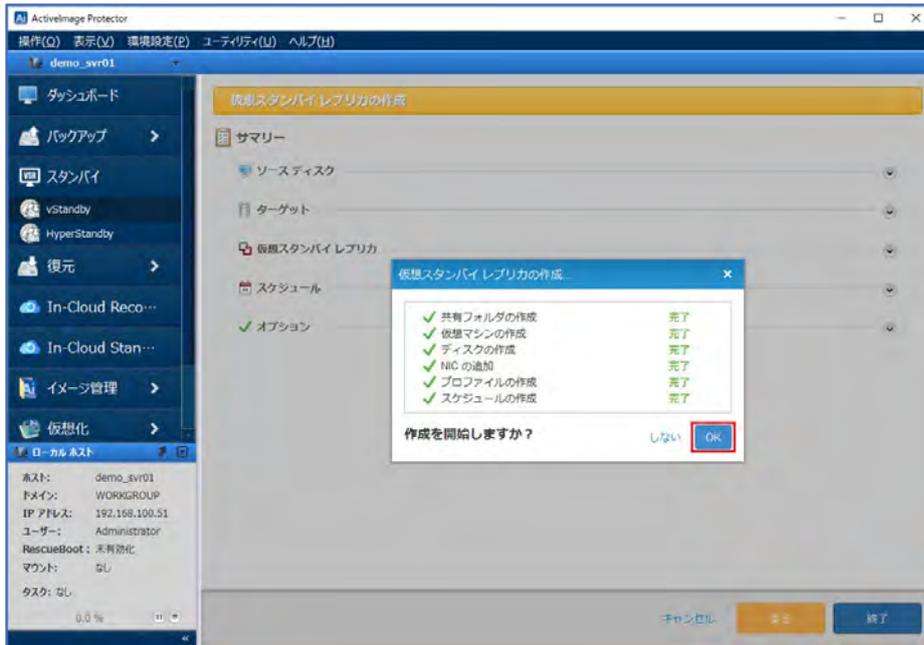


10. サマリーが表示されますので、内容を確認し、[終了] をクリックします。

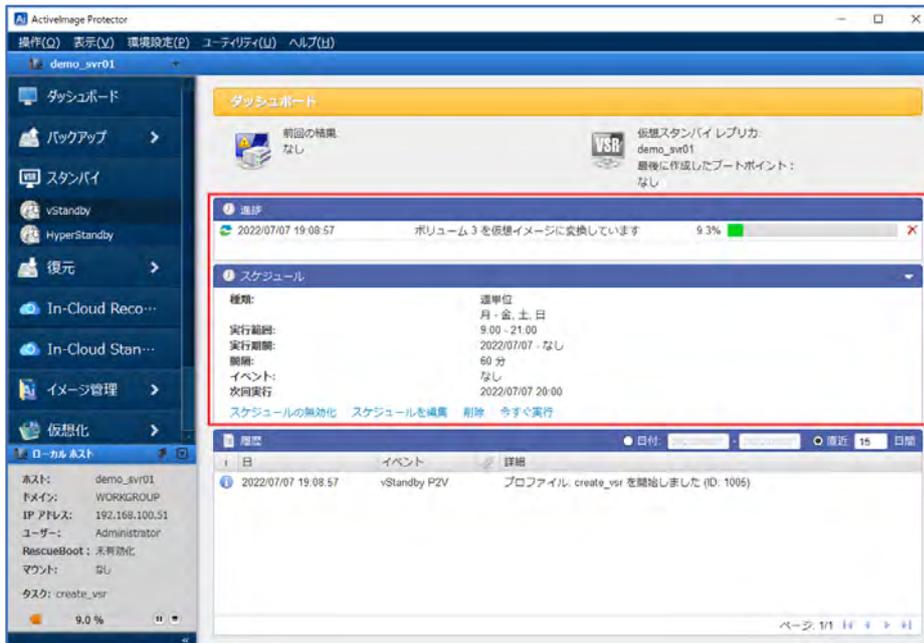


## 仮想スタンバイ（待機）マシンの作成

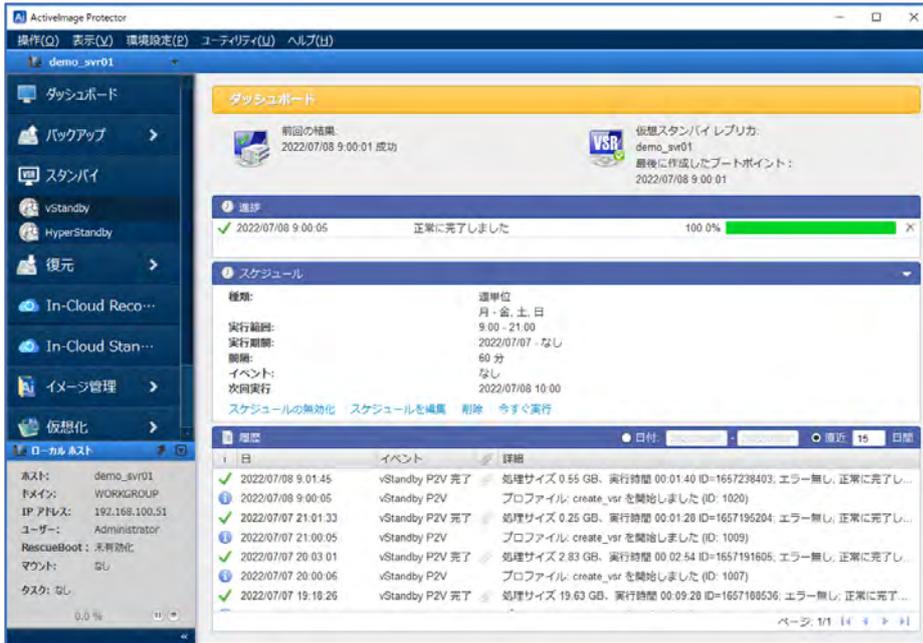
11. 仮想スタンバイレプリカの作成が開始されます。作成が完了したら、すぐさまタスクを実行する場合、[OK]をクリックします。



12. ダッシュボードには、実行中のタスクの進捗状況が表示されます。

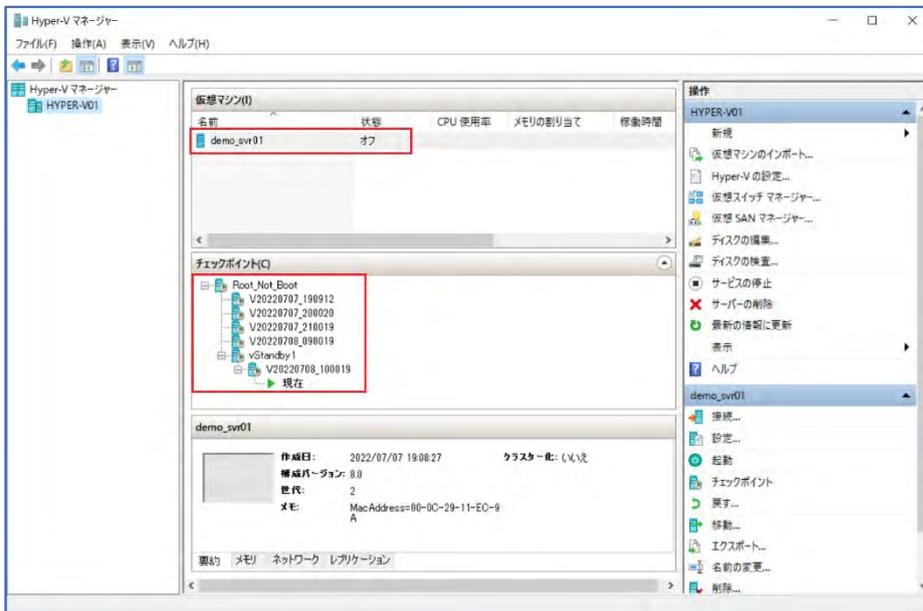


13. 仮想スタンバイレプリカが完成すると、以下ようになります。



14. Hyper-V マネージャー上では、以下のように仮想スタンバイレプリカが確認できます。

60 分間隔で、ソースマシンのディスクの更新状態を、仮想スタンバイマシンのチェックポイントに追加しています。

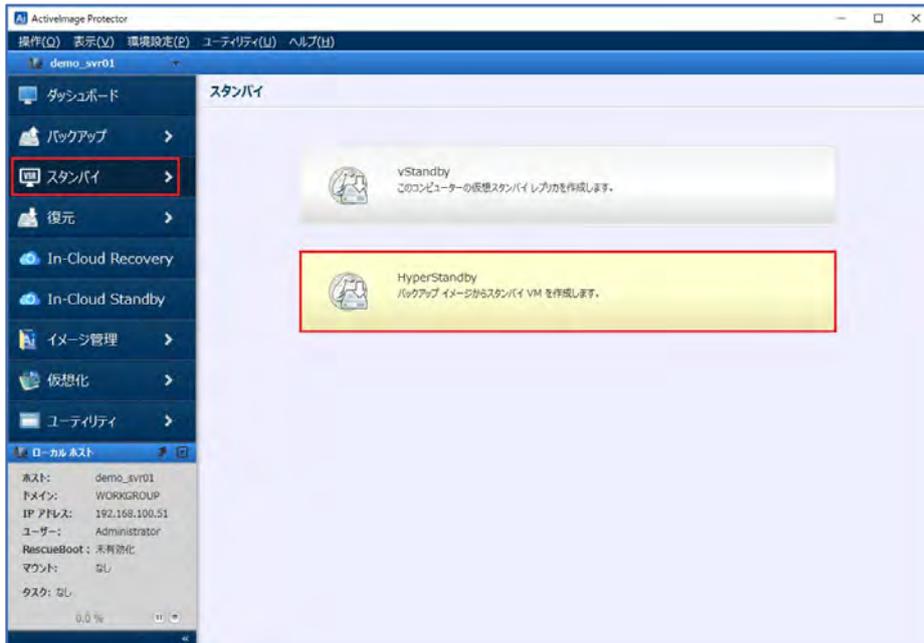


## 11-2. HyperStandby

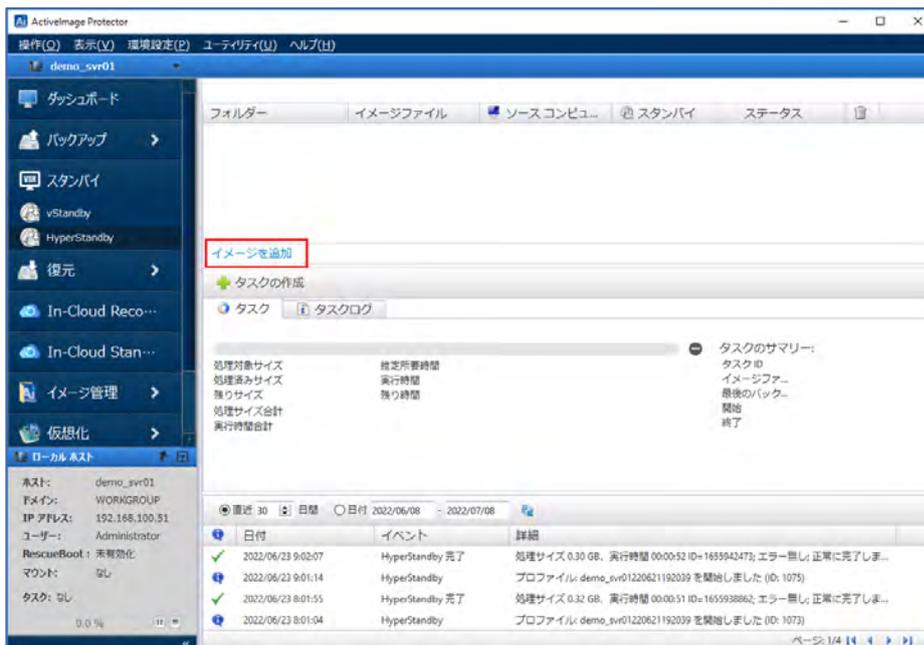
ソースマシンのバックアップからハイパーバイザー上に仮想スタンバイ マシンを作成します。スケジュール機能を使い、ソースマシンの日々のバックアップを仮想スタンバイマシンのブートポイントとして追加します。緊急時には、仮想スタンバイマシンから起動し、代替のサーバーとして利用することができます。ここでは、HyperStandby のバックアップ設定手順について説明します。

1. [HyperStandby] を起動します。

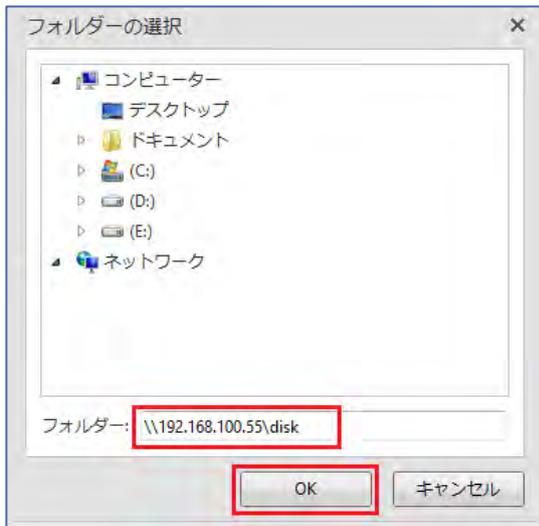
左のメニューから [スタンバイ] → [HyperStandby] をクリックします。



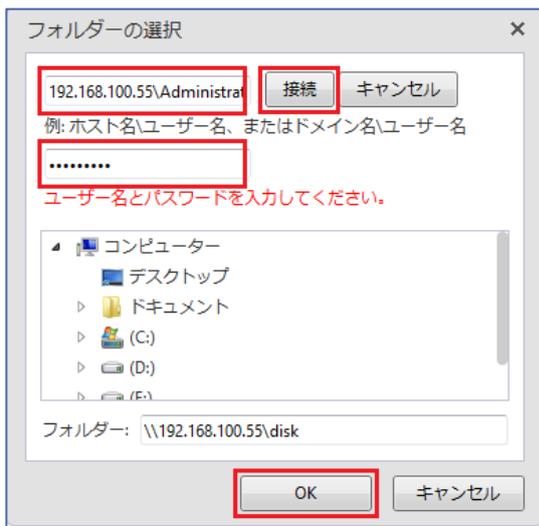
2. [イメージを追加] をクリックして、対象マシンのバックアップを追加します。



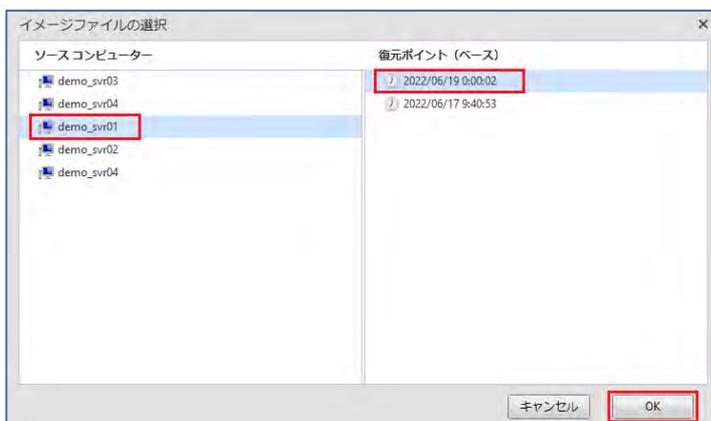
- 対象マシンのバックアップが保存されているフォルダーを指定します。  
 ここでの例として、[フォルダー:]には、共有フォルダーのパス「¥¥192.168.100.55¥disk」を入力して、  
 [OK] をクリックします。



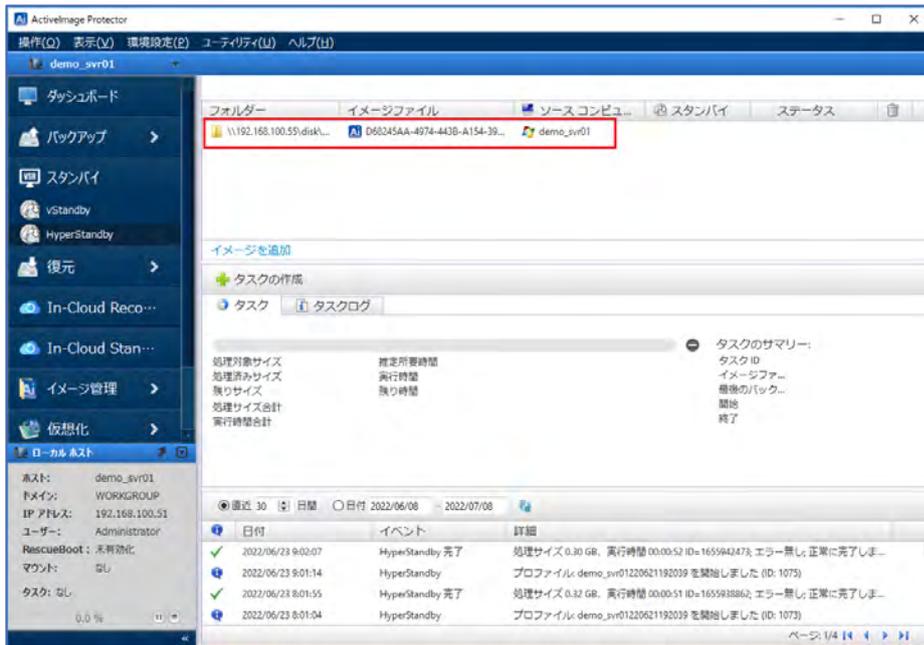
- 共有フォルダーの認証を行います。



- ソースコンピュータとベースバックアップの復元ポイントを選択して、[OK] をクリックします。

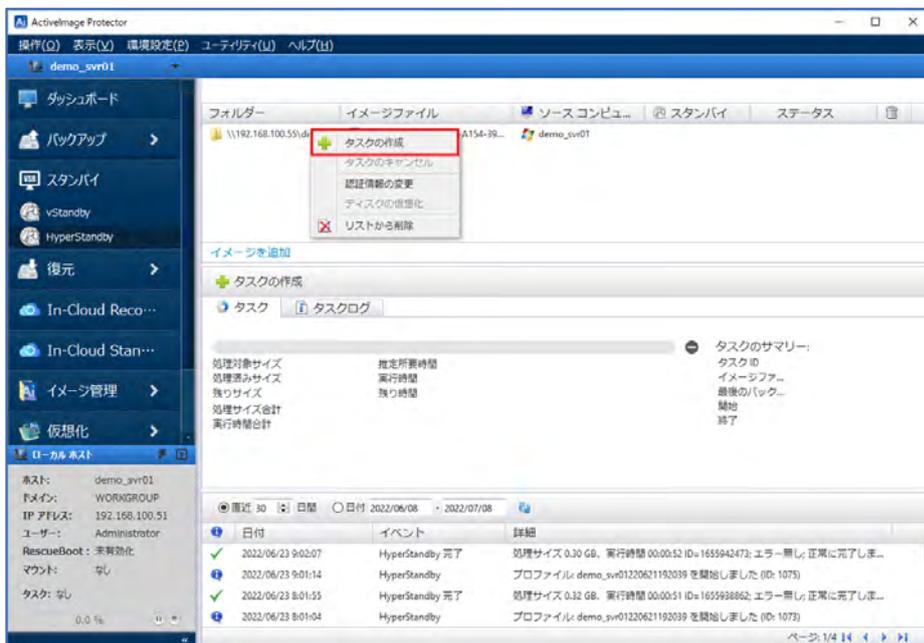


6. イメージリストにバックアップが追加されます。

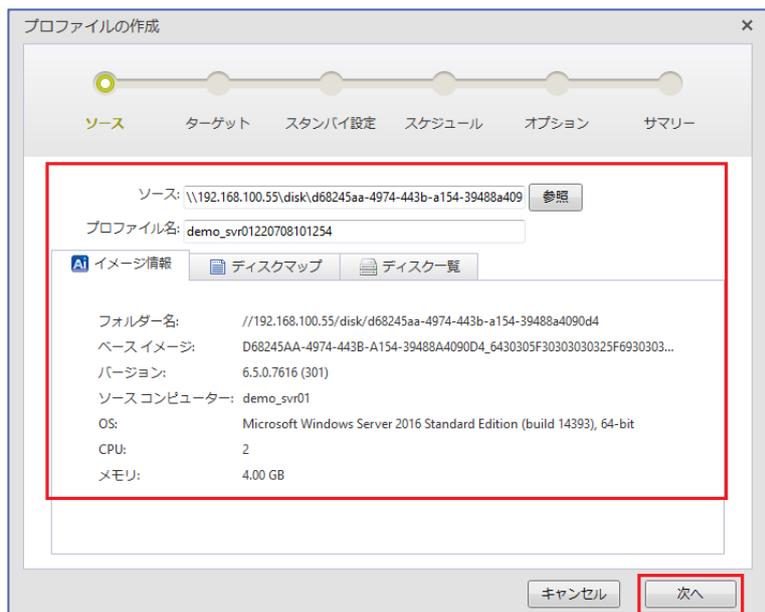


7. タスクを作成します。

登録されたベースバックアップにカーソルを合わせて右クリックすると、プルダウンメニューが表示されます。メニューから [タスクの作成] をクリックします。



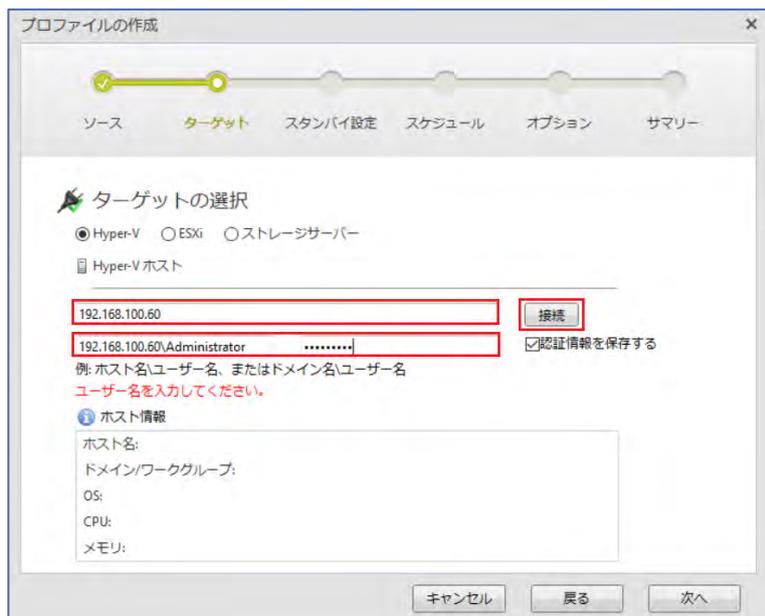
8. タスクの作成ウィザードを起動すると、ソースとなるバックアップの情報が表示されます。確認後に、[次へ] をクリックします。



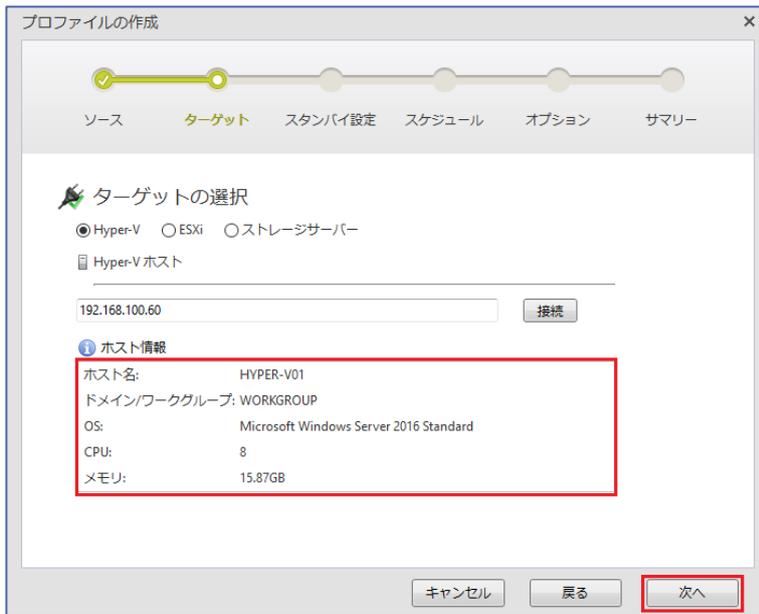
9. ハイパーバイザーのタイプを選択します。

ハイパーバイザーは、Microsoft Hyper-V、または VMware vSphere (ESXi) が使用できます。

ここでの例として、[ハイパーバイザータイプ:] に「Microsoft Hyper-V」を選択し、[ホスト名、または IP アドレス:] に Hyper-V ホストの IP アドレス「192.168.100.60」を入力し、[接続] をクリックします。次に、認証情報を入力します。[ユーザー名:] に「Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。

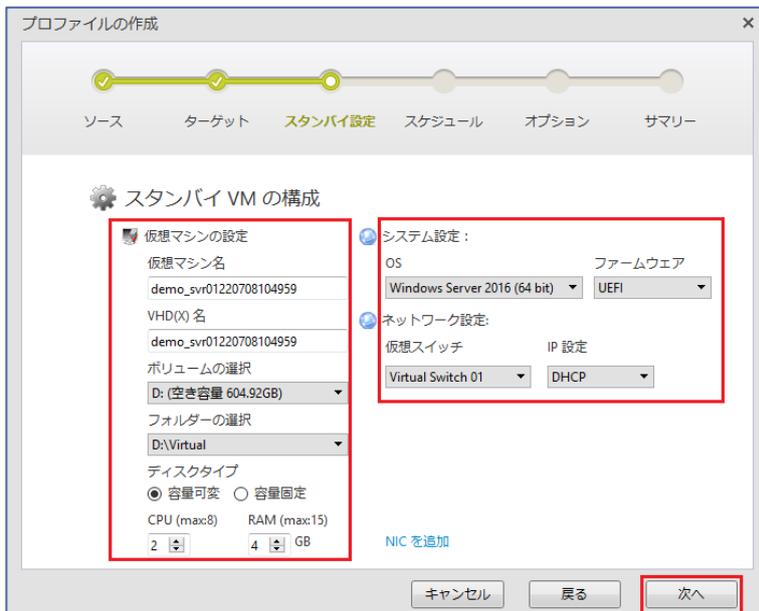


10. ホスト情報を確認してから [次へ] をクリックします。



11. [スタンバイ VM の構成] からスタンバイ VM の各種設定を行います。

ここでの例として、仮想マシンの保存先として「D ドライブ」のフォルダー「Virtual」を選択します。CPU 数、RAM は、バックアップ元と同じ「CPU 数：2」、「RAM：4GB」にします。[システム設定:] は、バックアップ元と同じ OS、ファームウェアが自動的に選択されています。バックアップ元と異なるファームウェアを選択した場合、作成された仮想マシンは起動できませんので、注意してください。[仮想スイッチ:] は、ホスト側に作成した仮想スイッチ、[IP アドレス:] は、「DHCP」にします。設定が完了したら、[次へ] をクリックします。



12. バックアップから仮想スタンバイマシンのブートポイントを作成するためのスケジュールを、週単位、もしくは月単位で設定します。

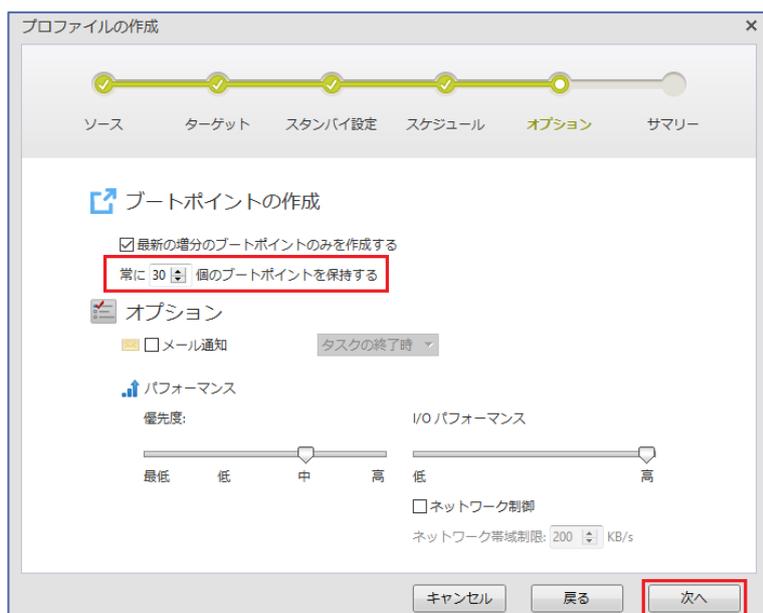
ここでの例では、[即時] を選択して、[OK] をクリックします。バックアップが作成されるたびに、ブートポイントとして追加していきます。



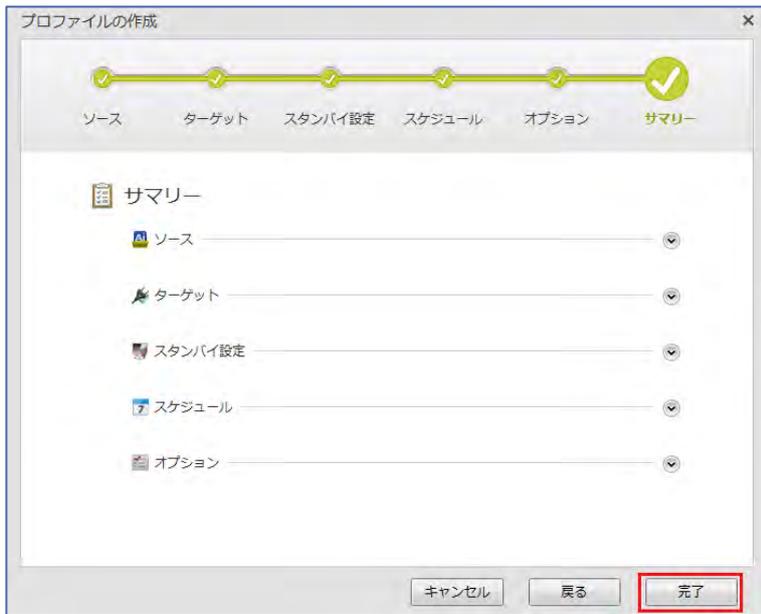
13. オプションを設定します。

仮想スタンバイマシンに保有するブートポイントの数を指定できます（最大 30 個）。ブートポイントが指定数に達すると、一番古いものと 2 番目に古いものがマージされます。

[最新の増分のブートポイントのみを作成する] を有効にすると、最新の増分イメージファイルを元に 1 回のタスクでブートポイントを 1 つだけ作成します。



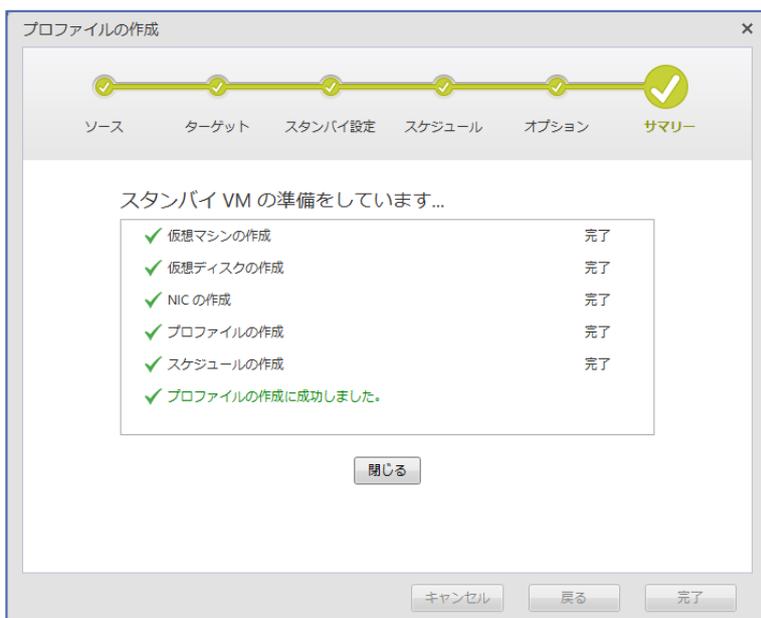
14. 内容を確認したら [完了] をクリックしてください。以下の確認ダイアログが表示されます。



15. [OK] をクリックすると仮想スタンバイマシンとプロファイルが作成されます。

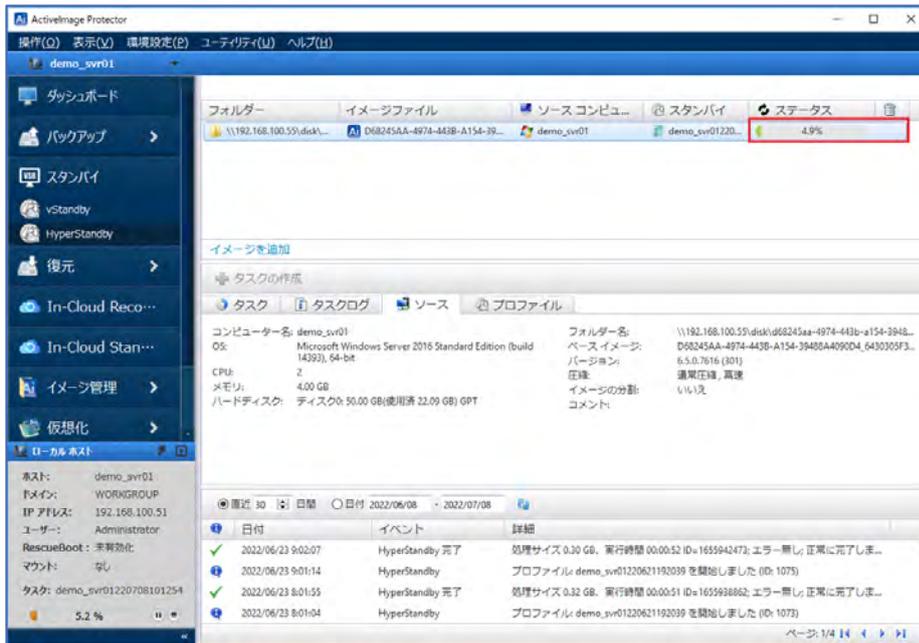


16. 仮想スタンバイマシンとプロファイルの作成が完成すると、以下のようになります。[閉じる] をクリックするとダッシュボードに戻ります。

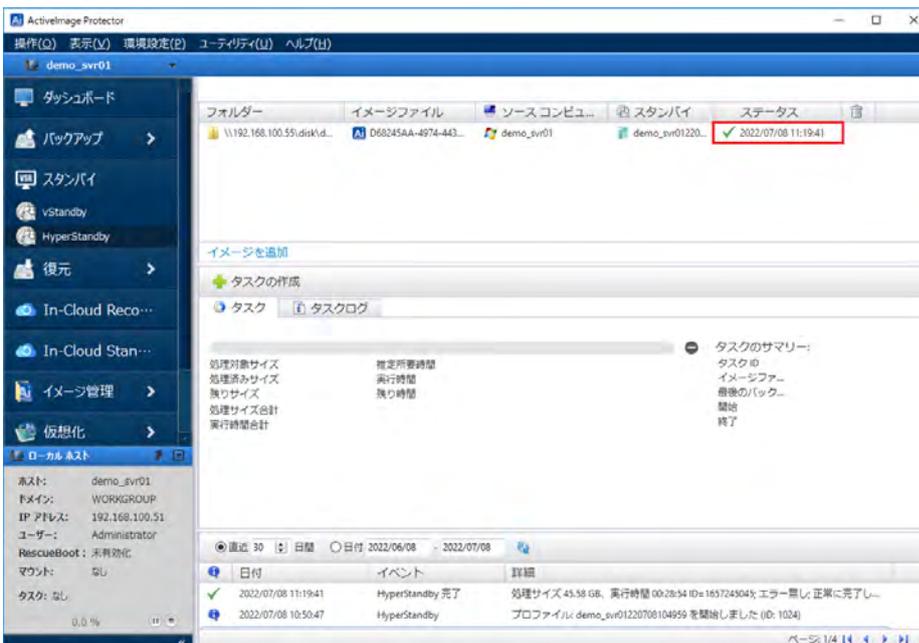


## 仮想スタンバイ（待機）マシンの作成

17. ダッシュボードには、実行中のタスクが表示されます。

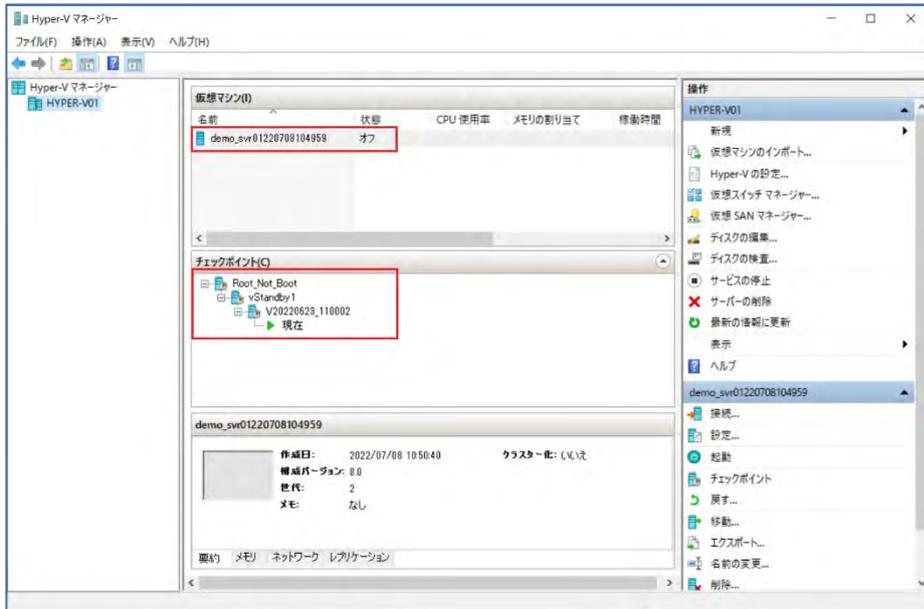


18. タスクが完成すると、以下のようになります。



## 仮想スタンバイ（待機）マシンの作成

19. Hyper-V マネージャー上では、以下のように仮想スタンバイマシンが確認できます。  
日々のバックアップから、仮想スタンバイマシンのチェックポイントに追加されていきます。



### 11-3. HyperBoot

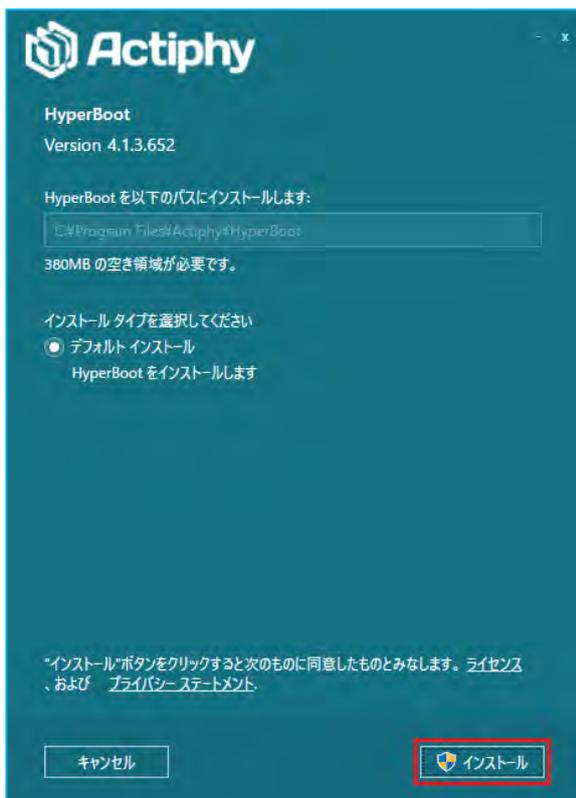
HyperBoot は、バックアップから直接仮想マシンとして起動させることができる、無償のオプションツールです。HyperBoot は、ActiveImage Protector の製品メディア内のインストーラーからインストールすることができます。ここでは、HyperBoot の操作手順について説明します。

1. 製品メディア内の「Setup.exe」を直接実行してインストーラーを起動します。[関連製品をインストールする] → [Actiphy HyperBoot] → [実行] をクリックします。

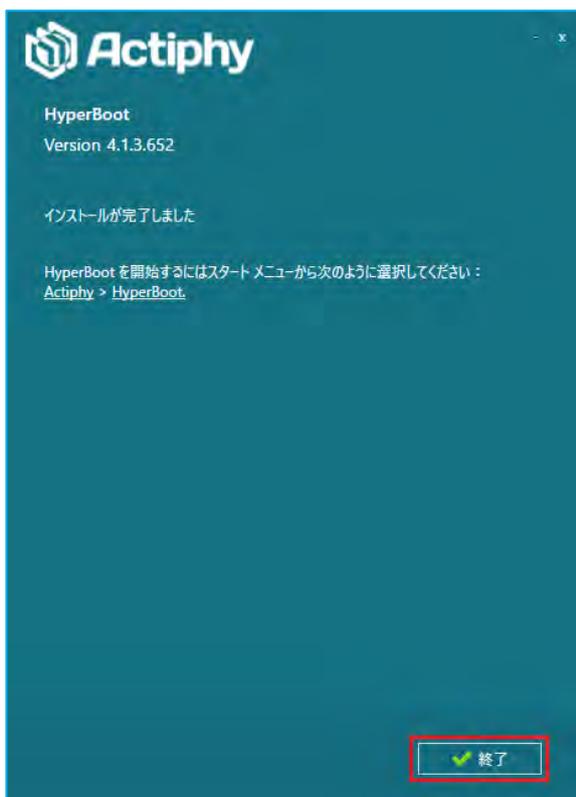


- 2.

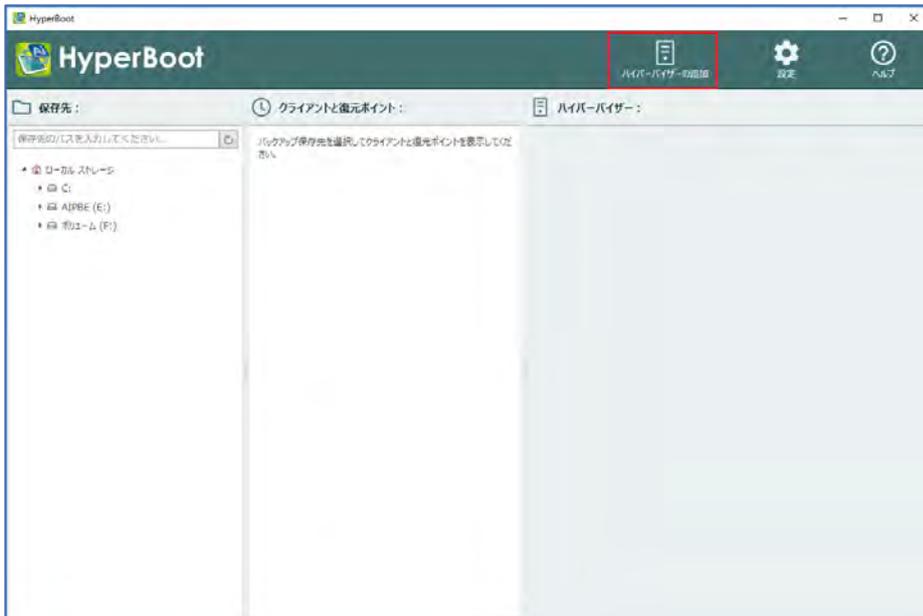
3. セットアップにあたり、特に設定すべき項目はありません。[インストール] をクリックします。インストールが開始されます。



4. 次の画面でインストールは完了です。[終了] をクリックして、セットアップウィザードを終了します。



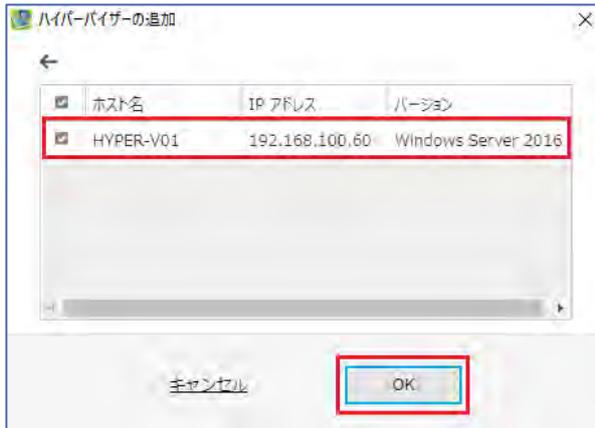
- HyperBoot を起動します。  
Windows スタートメニューから [Actiphy] → [HyperBoot] をクリックします。
- 最初に、仮想マシンを起動するハイパーバイザーの登録を行います。  
[ハイパーバイザーの登録] をクリックします。



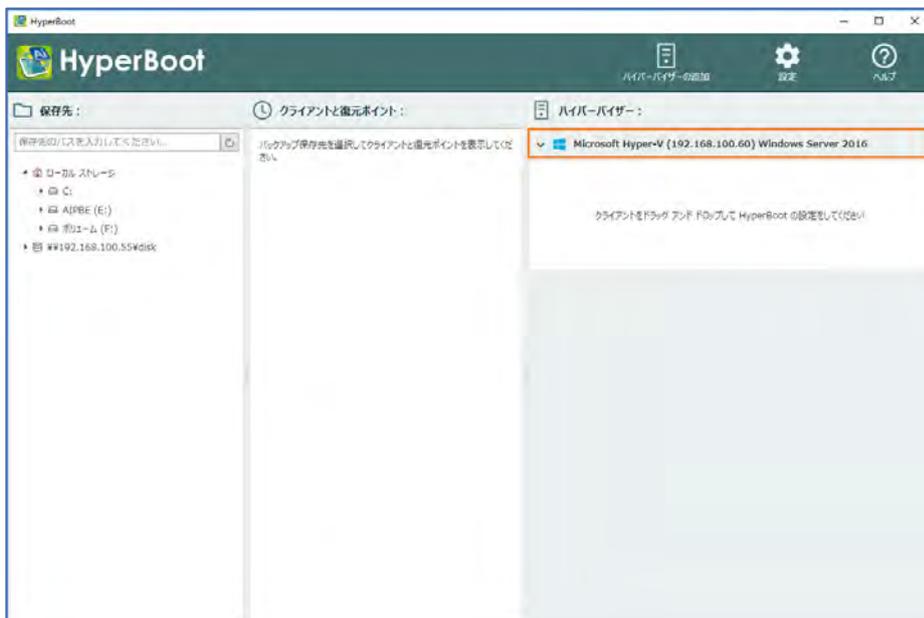
- ハイパーバイザーを追加します。  
ここでの例として、[ターゲットの選択:] は「Hyper-V」を選択して、[Hyper-V ホスト:] は Hyper-V ホストの IP アドレス「192.168.100.60」、[ユーザー名:] は「Administrator」と設定されたパスワードを入力し、[追加する] をクリックします。



8. 指定したハイパーバイザーが追加されたら、[OK] をクリックして HyperBoot のコンソールに戻ります。

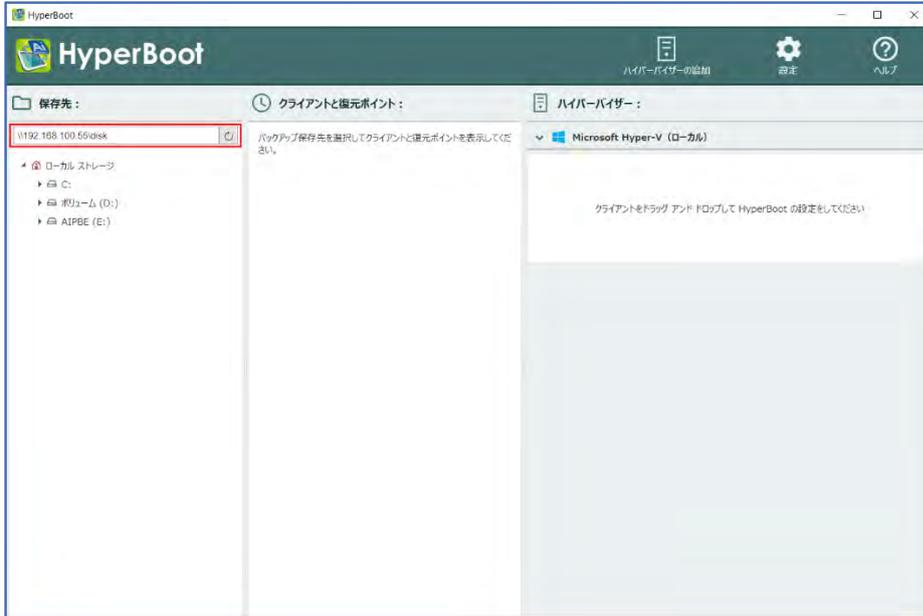


9. ハイパーバイザーに Hyper-V が登録されたことが確認できます。

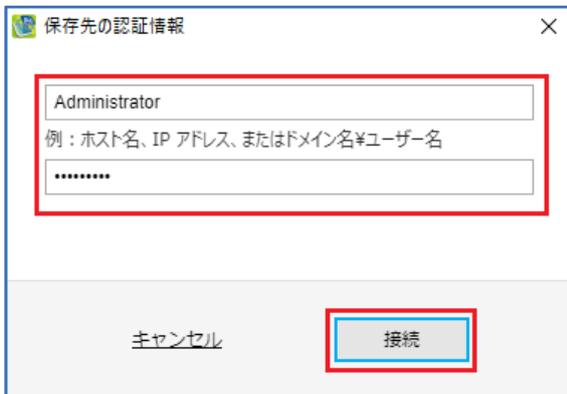


10. [保存先:] から、ActiveImage Protector でバックアップされたバックアップの復元ポイントを選択します。

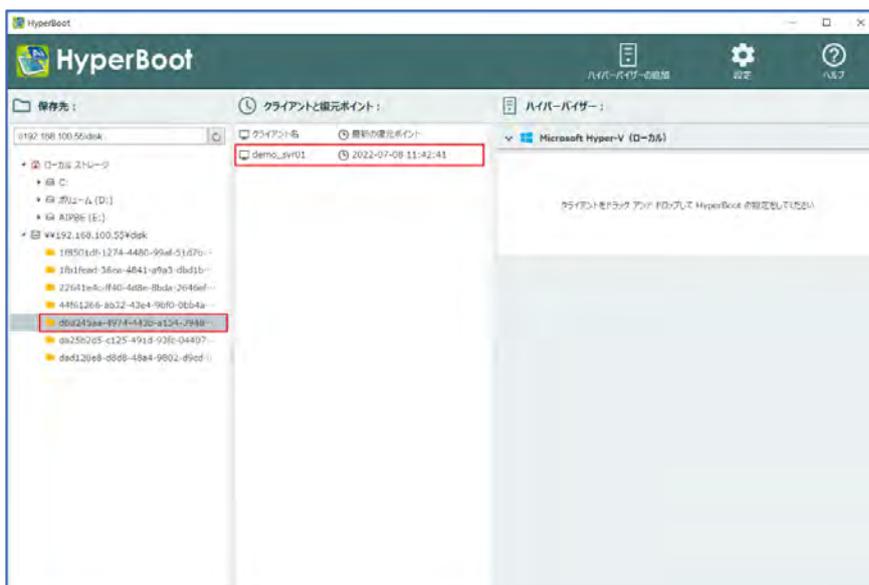
ここでの例では、下記の場所に保存先の共有フォルダーのパス「¥¥192.168.100.55¥disk」を入力し、Enter キーを押します。



11. [保存先の認証情報] には、[ユーザー名:] に「Administrator」、[パスワード:] に設定されているパスワードを入力してから、[接続] をクリックします。

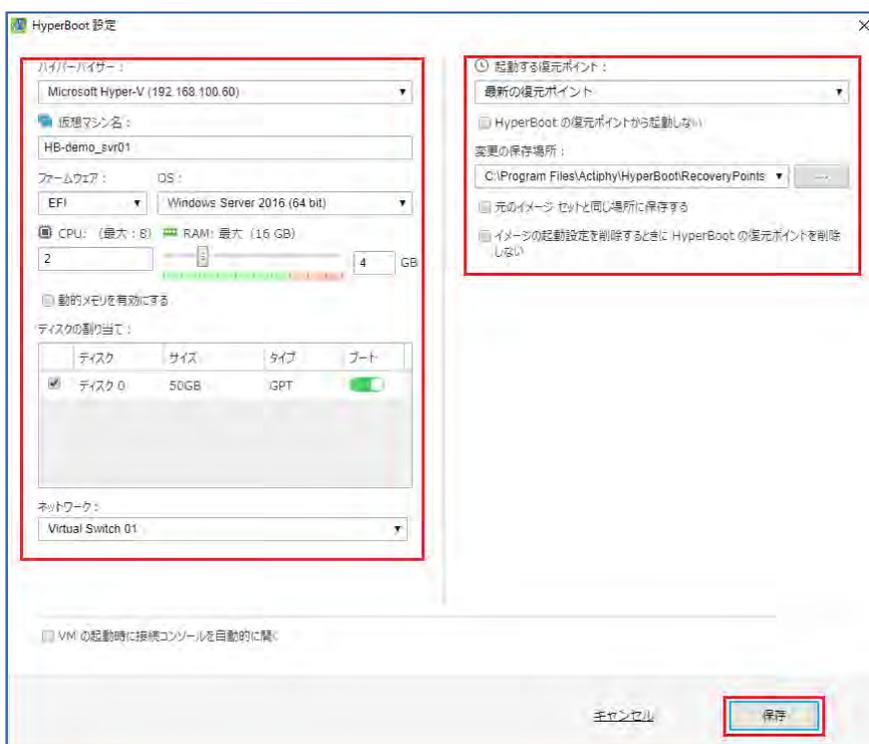


12. バックアップを選択後、起動したい復元ポイントを右のペインの白い部分に、ドラッグ&ドロップすると、HyperBoot の設定になります。



13. ハイパーバイザーを選択します。

ここでの例として、「Microsoft Hyper-V」を選択しています。同様に CPU 数、RAM、ネットワーク設定等を行います。必要に応じて [仮想マシン名:] も変更します。[変更の保存場所:] では、デフォルトでは HyperBoot で定められたフォルダーになります。しかし、[元のイメージセットと同じ場所に保存する] のチェックボックスにチェックを入れると、イメージファイルと同じ場所に設定ファイルが作成されます。他のホストなどで、HyperBoot でイメージ起動をする場合等に使いやすくなります。設定が完了したら、[保存] をクリックします。

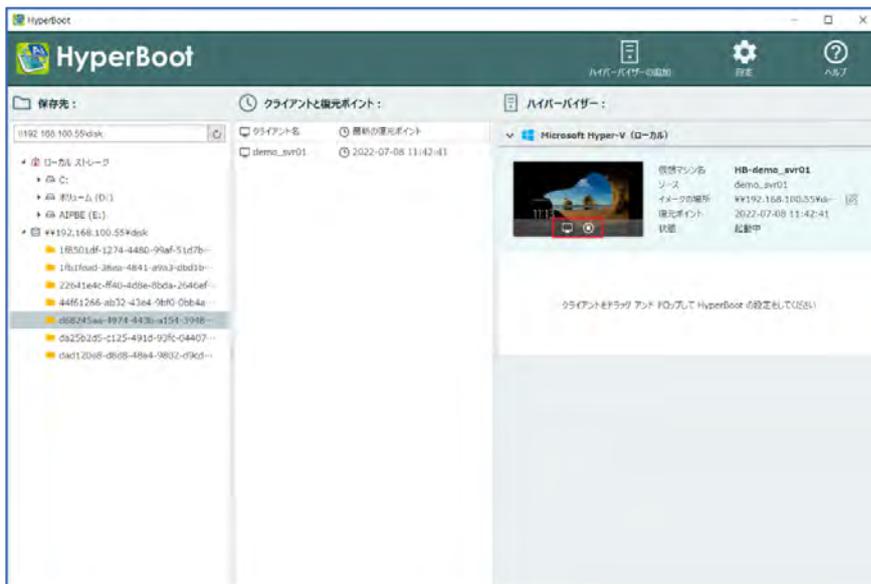


## 仮想スタンバイ（待機）マシンの作成

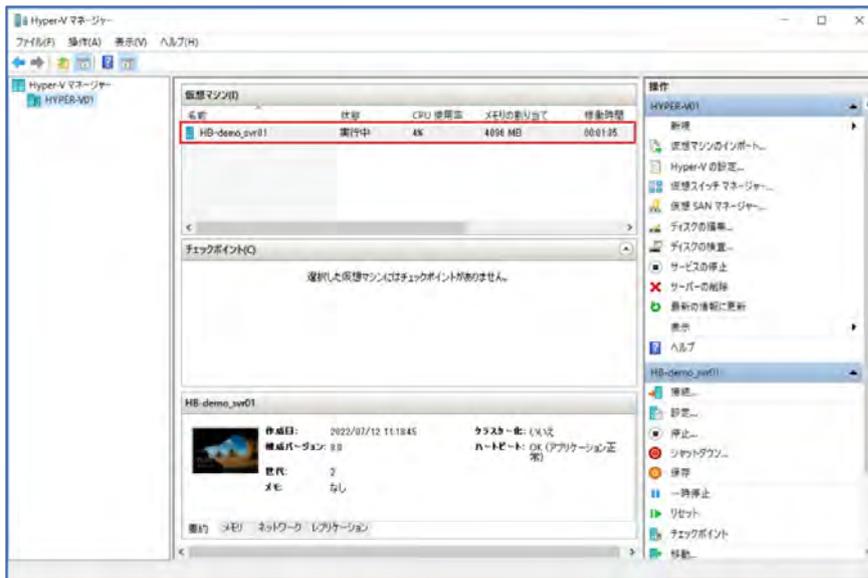
14. [ハイパーバイザー:] に起動する仮想マシンなどが登録されます。サムネイルの三角をクリックすると、仮想マシンが起動します。



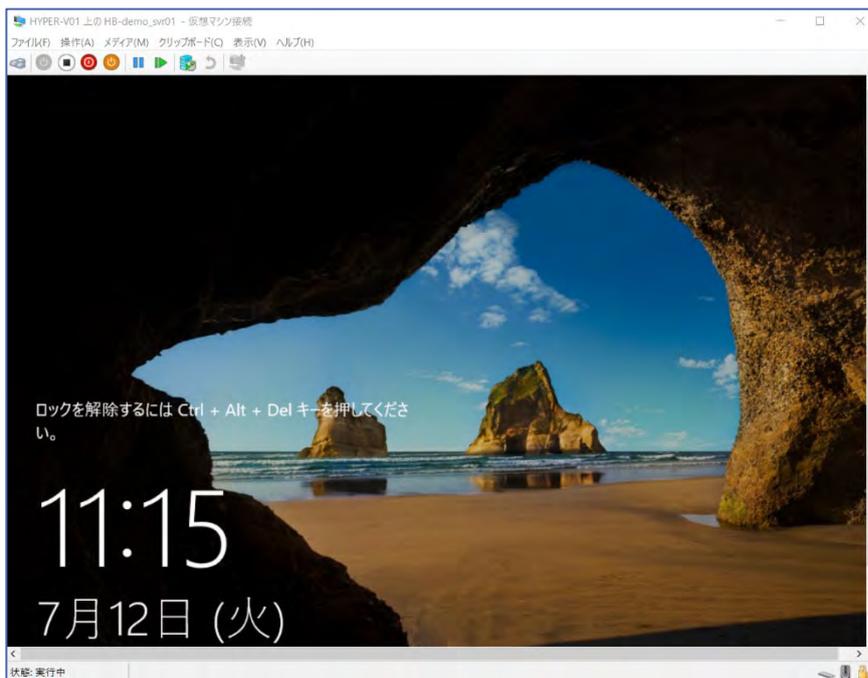
15. サムネイルの左のボタンをクリックすると接続コンソールが開きます。



16. バックアップから Hyper-V 上の仮想マシンとして起動しています。

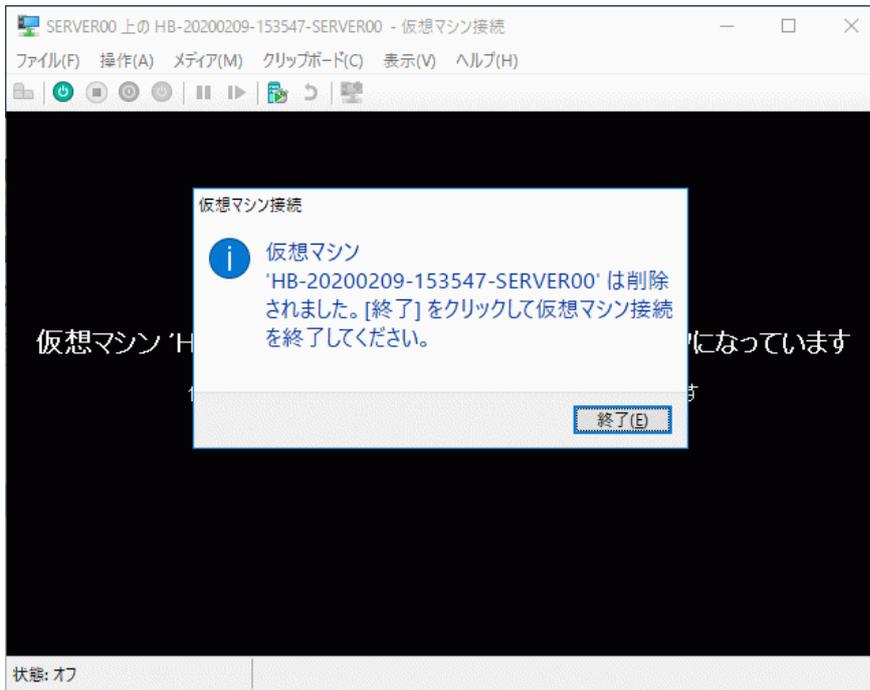


17. 接続コンソールから稼働した仮想マシンに接続できます。



## 仮想スタンバイ（待機）マシンの作成

18. 仮想マシンを終了すると、次の画面になりますので、[終了] をクリックし、仮想マシンとの接続を終了します。仮想マシンを終了すると、自動的に作成された仮想マシンも削除されます。



## 12. 参考情報

---

### アクティファイの Web サイト

製品情報の他、各種資料やサポート情報、アップデートなど、総合的にご案内しています。

<https://www.actiphy.com>

### ActiveImage Protector の FAQ

サポート情報のデータベースです。

<https://jpkb.actiphy.com/>

### ActiveImage Protector に関するお問い合わせ先：

株式会社 アクティファイ

営業本部

E-mail:sales@actiphy.com

TEL: 03-5256-0877

FAX: 03-5256-0878

© 2024 Actiphy, Inc. 無断複写・転載を禁止します。

本ソフトウェアと付属ドキュメントは株式会社アクティファイに所有権および著作権があります

本ガイド中のその他のブランド名及び製品名は、それぞれ帰属する所有者の商標または登録商標です。