

# Dell™ Management Console Version 1.1 ユーザーズ ガイド

[はじめに](#)

[Dell Management Console のインストール、アンインストール、およびアップグレード](#)

[Dell OpenManage ITAssistant の検出設定の移行](#)

[Dell Management Console のユーザーインターフェイス](#)

[検出とインベントリ設定の構成](#)

[Dell OpenManage Server Administrator Solution の展開](#)

[ジョブとタスクの管理](#)

[ハードウェア構成タスク](#)

[監視と警告](#)

[電源監視](#)

[Dell Patch Management Solution](#)

[レポート](#)


[仮想化](#)


[Dell Management Console のセキュリティ](#)

[インベントリの属性](#)

---

## メモ、注意、警告

 **メモ:** メモには、コンピュータのより良い使用に役立つ重要な情報が示されています。

 **注意:** 注意には、使用説明書に従わなかった場合に被る可能性のあるハードウェアの障害またはデータの損失について示されています。

---

**このドキュメント内の情報は、予告なしに変更されることがあります。**

©2010 Dell Inc. All rights reserved.

どのような形式であっても Dell Inc. の書面による許可なしにこれらの資料を複製することは厳しく禁じられています。

このテキストで使用されている商標: Dell, DELL ロゴ, PowerEdge, PowerVault, PowerConnect, OpenManage, および EqualLogic は、Dell Inc. の商標です。Microsoft, Windows, および Windows Server は、米国または他の国、あるいはその両方における Microsoft Corporation の商標または登録商標です。Altiris, Symantec および Notification Server は、Symantec Inc. の商標または登録商標です。Brocade, Itrrepid および McData は、Brocade Communications Systems, Inc. の商標です。

その他の商標および商号は、それらの商標と商号またはその製品であることを明確にするため、このドキュメント内で使用される場合があります。Dell Inc. は、所有していない商標と商号において、一切の所有権を放棄します。

2010 年 3 月

[目次のページに戻る](#)

## 仮想化

### Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [サポートされている仮想オペレーティングシステム](#)
- [仮想サーバーのサポートされている機能](#)
- [ESXi の構成](#)
- [Dell Management Console の構成](#)
- [注意事項](#)

Dell™ Management Console は、仮想サーバーを検出できます。ハードウェア インベントリおよびホスト サーバーのヘルスの監視もサポートします。

Dell Management Console では「**すべてのデバイス**」ツリーの「**サーバー**」ノードの下に物理ホストおよび仮想マシンが表示されます。

「**すべてのデバイス**」ツリーに仮想マシンとホストの関連付けを表示する新規グループを作成します。

ホストを選択すると各仮想マシンはこのノードの下に表示され、そのサーバー上で実行中のすべての仮想マシンは右側のウィンドウに表示されます。

ハードウェア インベントリは、**[概要]**→ **[ハードウェアの概要]** の下の **[リソース マネージャ]** で表示できます。

---

## サポートされている仮想オペレーティングシステム

- 1 Classic ESX
- 1 Embedded ESX
- 1 HyperV

---

## 仮想サーバーのサポートされている機能

- 1 検出
- 1 ホスト-仮想マシンの関連付け
- 1 ハードウェア インベントリ

## 検出

ゲストおよびホスト マシンはネットワーク上で別々に検出されます。

 **メモ:** 仮想サーバーの検出後に仮想マシンを追加する場合、DellManagement Console はゲストをホストと関連付けません。この問題を解決するには、仮想マシンを再検出してください。

## Classic ESX

Dell Management Console は、VMware® SNMP Agent を使用してホスト デバイスを検出します。

ホストを検出するための必須条件は次のとおりです。

- 1 SNMP サービスをサーバー上で有効にする
- 1 検出タスクで使用されている接続プロファイルで SNMP を有効にする

## HyperV

Dell Management Console は、WMIプロバイダを使用してホストデバイスを検出します。

ホストを検出するための必須条件は次のとおりです。

- 1 WMI サービスをサーバー上で有効にする
- 1 検出タスクで使用されている接続プロファイルで WMI を有効にする

## Embedded ESX

Dell Management Console は、VMware が提供するCIM プロバイダを使用してホスト デバイスを検出します。

ホストを検出するための必須条件は次のとおりです。

- 1 WSMAN サービスをサーバー上で有効にする
- 1 検出タスクで使用されている接続プロファイルで WSMAN を有効にする

## ホスト-仮想マシンの関連付け

- 1 仮想ホスト サーバーは、これらのホスト サーバーで実行されているハイパーバイザ オペレーティング システムに基づいて識別されます。
- 1 仮想ホスト サーバーは、**【仮想ホスト】** ノードの下の **【すべてのデバイス】** ツリーに表示されます。
- 1 サーバー上で実行中の仮想マシンはネットワーク上で単独に検出されます。
- 1 ホストとホスト上で実行されている仮想マシン間の関連付けは、検出後に仮想マシンの MAC アドレス、IP アドレス、および UUID を使用して作成されます。
- 1 ホストに関連付けられている仮想マシンは、左側のウィンドウのホスト サーバーをクリックすると右側のウィンドウに表示されます。

## インベントリ

### Classic ESX

ハードウェア インベントリは、Dell OpenManage™ Server Administrator SNMP Agent を使用して表示されます。

Classic ESX Server のインベントリ取得の必須条件は次のとおりです。

- 1 サーバーに Server Administrator がインストールされている
- 1 サーバー上で SNMP サービスが有効になっている
- 1 インベントリ タスクで使用されている接続プロファイルでSNMPが有効になっている

### HyperV

ハードウェア インベントリは、Server Administrator SNMP Agent または WMI Agent を使用して表示されます。

HyperV のインベントリ取得の必須条件は次のとおりです。

- 1 サーバーに Server Administrator がインストールされている
- 1 サーバー上で SNMP または WMI サービスが有効になっている

- 1 インベントリ タスクで使用されている接続プロファイルで SNMP または WMI あるいはその両方が有効になっている

## Embedded ESX

ハードウェア インベントリは、VMware が提供する CIM プロバイダを使用して表示されます。情報は WSMAN プロトコルを使用して収集されます。

Embedded ESX Server のインベントリ取得の必須条件は次のとおりです。

- 1 サーバー上で WSMAN サービスが有効になっている
- 1 インベントリタスクで使用されている接続プロファイルで WSMAN が有効になっている

---

## ESXi の構成

### CIM OEM プロバイダの有効化

ESXi Server から Dell Management Console の監視で報告されるヘルス情報を受信するには、CimOemProvidersEnabled 構成設定を有効にし (値 1 に設定)、ESXi インストール後初めて Management Agent を再起動します。

CIM OEM プロバイダを有効化する方法

- 1 VMware Web サイト (vmware.com/go/remotecli/) から RCLI ツールをダウンロードしてインストールします。
- 2 リモートの Windows または Linux Server から次の VmWare RCLI コマンドを実行します。

```
vicfg-advcfg.pl --server <ip_address> --username <user_name> --password <password> --set 1 Misc.CimOemProvidersEnabled
```

- 3 ESXi Server Direct Console User Interface (DCUI) メニューから再起動するか、サーバーから再起動します。

 **メモ:** VI クライアント ([構成] → [ソフトウェア] → [高度な設定] → [Misc] → [OEM プロバイダの有効化]) を使用して CimOemProvidersEnabled プロパティを設定することもできます。

---

## Dell Management Console の構成


### セキュリティで保護された展開モード - HTTPS を介して WSMAN に接続


Dell Management Console が ESXi Server 上でセキュア モードで実行している WS-MAN に接続する場合に必要な構成は、次のとおりです。

- 1 WS-MAN 資格情報セットは Credential Manager を使用して作成されています。

すべての ESXi Server が同じユーザー名とパスワードの設定を所有する場合には、資格情報のセットは 1 つだけ必要です。

- 2 WS-MAN プロトコルを使用する接続プロファイルが有効で、次の設定が適用されています。
  - a. ステップ 1 で示されているように資格情報のセットが作成されています。
  - b. セキュア モードが選択されています。
  - c. セキュア ポート テキスト ボックスには ESXi Server 上の HTTPS サービスのポート番号が定義されています。デフォルトでは、この値は 443 です。
  - d. SSL 証明書ファイルは ESXi Server からダウンロードされた SSL 証明書 (自己署名入り) にポイントしています。複数の SSL 証明書を Dell Management Console 接続プロファイルにインポートする方法のセクションを参照してください。

 **メモ:** 複数の ESXi Server からの自己署名入りの証明書 (デフォルトによりインストール済み) が接続プロファイルにインポートされた単一の証明書に統合され、すべての ESXi Server 全体で資格情報が同じ場合、複数の ESXi Server の検出と同じ接続プロファイルを使用できます。

 **メモ:** 同じ資格情報を使用している ESXi Server では、単一の接続プロファイルを使用して接続プロファイルの [信頼済みサイト] のオプションを有効にすることで複数の ESXi Server を検出することができます。接続プロファイルに ESXi 証明書をインポートする必要はありません。

すべての ESXi Server が同じ CA によって生成された証明書を所有する場合、Dell Management Console の接続プロファイルに個々の証明書をインポートするのではなく、CA の証明書をインポートするだけで十分です。

## 複数の SSL 証明書を Dell Management Console 接続プロファイルにインポートする方法

Dell Management Console では、接続プロファイルの一部としてセキュア モードで WS-MAN を構成した時に SSL 証明書をインポートすることができます。

HTTP を介した WS-MAN を使用して複数のデバイスを検出する必要がある場合、自己署名入りの証明書 (デフォルトによりインストール済み) を含む単一のファイルを別のサーバーから Dell Management 接続プロファイルにインポートすることができます。

複数の ESXi Server から取得された SSL 証明書を使用してマルチ証明書ファイルを作成することができます。それからマルチ証明書ファイルを接続プロファイルにインポートし、単一の接続プロファイルを使用して複数の ESXi Server の検出を有効にすることができます。(すべての ESXi Server で同じ資格情報を使用していることを前提としています。)

次の手順では、自己署名入りの証明書 (デフォルトによりインストール済み) について説明します。この手順は CA 署名付き証明書にもまた有効です。すべての ESXi Server が同じ CA によって生成された証明書を所有する場合、Dell Management Console の接続プロファイルに CA の証明書をインポートするだけで十分なため、次の手順をスキップすることができます。

### ステップ 1: VMware からリモート CLI ツールをインストールする

VMware Infrastructure Remote CLI を Windows コンピュータにダウンロードします。

1. VMware Web サイト ([vmware.com/go/remotecli/](http://vmware.com/go/remotecli/)) から Infrastructure Remote CLI ツールをダウンロードします。

ページにある VMware Infrastructure Remote CLI セクションでダウンロードのリンクを探します。

2. 既定の場所 (例: C:\Program Files\VMware\VMware VI Remote CLI) にツールをインストールします。この後のステップは既定のインストール パスを想定しています。インストール パスを変更する場合は、それに応じて次のステップに変更を加えてください。
3. コマンド ウィンドウで次のコマンドを実行します。

```
Set path=%path%; "C:\Program Files\VMware\VMware VI Remote CLI\Per\bin"
```

### ステップ 2: マルチ証明書ファイルの作成

1. `combinecerts.bat` DOS バッチ ファイルを作成します。
2. 次の `combinecerts.bat` ファイルを実行します。

```
combinecerts <userName> <password> <servers ip list file> <output certificate file> [create|append]
```

**userName:** ESXi Server へのログインに使用するユーザー名

**password:** ユーザーのパスワード

**servers ip list file:** 各行に IP アドレスが 1 つある ASCII ファイル (このマニュアルのサンプル ファイルを参照)

**output certificate file:** すべての証明書が含まれるファイルの名前

create|append:

**create:** スクリプトが新しい出力証明書ファイルを作成するようにします。

**append:** スクリプトが出力証明書ファイルに新しい証明書を追加するようにします。このパラメータが指定されていない場合のデフォルトは、append です。

このバッチ ファイルを使用し、サーバーの IP リスト ファイルにある IP アドレスを 1 つだけ指定し作成オプションを使用して、ESXi Server から単一の証明書をインポートします。

## Combinecerts.bat DOS バッチ ファイル

次のテキストを「combinecerts.bat」という名前のファイルにコピーします。

```
----- DOS バッチ ファイルの初め -----
```

```
@echo off
```

```
rem Usage: combinecerts <user> <password> <servers ip list file> <output certificate file> [create|append]
```

```
rem (assuming same user and password for all servers)
```

```
rem option "create" causes the script to create a new <output certificate file>.
```

```
rem option "append" causes the script to append new certificates to the <output certificate file>.
```

```
if "%5"=="create" (del /F /Q %4 2>NUL)
```

```
for /f %%X in (%3) do (
```

```
echo.
```

```
echo.
```

```
echo Importing certificate from server: %%X
```

```
vifs.pl --server %%X --username %1 --password %2 --get /host/ssl_cert tmpcert.crt
```

```
if not errorlevel 1 (type tmpcert.crt >> %4)
```

```
del /F /Q tmpcert.crt 2>NUL
```

```
)
```

echo.

----- DOS バッチ ファイルの終わり -----

### サンプル サーバー IP リスト ファイルのコピー

----- サーバー IP リスト ファイルの初め -----

192.168.22.243

192.168.11.45

192.168.22.31

192.168.22.65

----- サーバー IP リスト ファイルの終わり -----

---

## 注意事項

- 1 **【すべてのデバイス】** ツリーに表示されている仮想マシンを削除するには、先ずグループの下のデバイスを削除してからグループを削除します。検出範囲からもグループを削除します。そうしないと各検出サイクルの後にグループが表示されることになります。
- 1 仮想マシンの検出後に仮想マシンにゲストを追加する場合、ゲストはホストに関連付けられません。ゲストをホストに関連付けるには、ホストを再検出します。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## インベントリの属性

Dell™ Management Console Version 1.1 ユーザーズ ガイド

このセクションではレポートの作成のために Dell Management Console が使用する属性を表示します。

表 C-1. レポート用のサーバーおよび MD1000 ストレージのインベントリ属性

コンポーネント	属性
エージェント	エージェントの説明
	エージェントのグローバル ステータス
	エージェントの ID
	エージェントの製造元
	エージェントの名前
	エージェントの URL
	エージェントのバージョン
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	デバイス シャーシ サービス タグ
	DeviceDescription(デバイスの説明)
	デバイス ロケーション
	シャーシ内のデバイスの場所
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム ID
	デバイス システム モデルの種類
	ファームウェア
ファームウェアのインデックス	
ファームウェアの名前	
ファームウェアのリリース日	
ファームウェアの種類	
ファームウェア バージョン	
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)
	NIC の製造元
	NIC ネットマスク
	Ping 可能 NIC
	NIC TOE 可能
	NIC TOE 有効
BIOS	BIOSChassisIndex(BIOS シャーシのインデックス)
	BIOSReleaseDate(BIOS リリースの日付)
	BIOS バージョン
	BIOSName(BIOS の名前)
	BIOSType(BIOS の種類)
オペレーティング システム	OS 合計物理メモリ
	OSType(OS タイプ)
	OSRevision(OS の改訂版)



	OSMajorVersion(OS のメジャー バージョン)
	OSMinorVersion(OS のマイナー バージョン)
	OSArchitecture(OS アーキテクチャ)
	OSVendor(OS ベンダ)
	OSSP メジャー バージョン
	OSSP マイナー バージョン
メモリ	メモリ デバイスのサイズ
	メモリ デバイスのフォーム ファクタ
	メモリ デバイスの製造元の名前
	メモリ デバイスのシリアル番号名
	MemoryDeviceAssetTagName(メモリ デバイスの資産タグ名)
	メモリ デバイスのステータス
	メモリ デバイスの種類
	メモリ デバイスのパーツ番号名
	メモリ デバイスのエラー モード
	メモリ デバイスのバンクの名前
	メモリ デバイスのインデックス
	MemoryDeviceLocationName(メモリ デバイスのロケーション名)
	電源
電源装置の種類	
電源装置の出カワット数	
電源装置のステータス	
電源装置の状態	
電源装置の冗長性の状態	
電源装置シャーンシのインデックス	
電源装置のインデックス	
プロセッサ	プロセッサ ブランド名
	プロセッサのファミリ
	プロセッサのステップング名
	プロセッサ コア数
	プロセッサの最大速度
	プロセッサのロット番号
	プロセッサのステータス
	プロセッサの現在の速度
	プロセッサのモデル名
	プロセッサ シャーンシのインデックス
FRU	FruIndex(FRU のインデックス)
	FruStatus(FRU のステータス)
	FruState(FRU の状態)
	FruDeviceName(FRU デバイス名)
	FruManufacturer(FRU メーカー)
	FruSerialNumber(FRU のシリアル番号)
	FruPartNumber(FRU のパーツ番号)
	FruRevision(FRU のリビジョン)
	FruManufacturingDate(FRU の製造日)
デバイス カード	デバイス カード アダプタ速度
	デバイス カードの製造元
	デバイス カードの説明
	デバイス カード スロット番号
	デバイス カード データ バス幅
	デバイス カード バス速度
	デバイス カード スロット長
アレイ ディスク	アレイ ディスクの番号
	アレイ ディスクの名前
	アレイ ディスクのベンダ名
	アレイ ディスクの状態
	アレイ ディスクのステータス

	アレイ ディスクのモデル番号
	アレイ ディスクのシリアル番号
	アレイ ディスク リビジョン
	アレイ ディスク エンクロージャ ID
	アレイ ディスクのチャンネル
	アレイ ディスク長
	アレイ ディスクの空き容量
	アレイ ディスクの使用済み領域
	アレイ ディスクのバスの種類
	アレイ ディスク スペアの状態
	アレイ ディスク ターゲット ID
	アレイ ディスク LUNid
	アレイ ディスクのパーツ番号
コントローラ	コントローラ番号
	コントローラ名
	コントローラのベンダ
	コントローラの種類
	コントローラの状態
	コントローラ ステータス
	コントローラ ファームウェア バージョン
	コントローラ キャッシュ サイズ
	コントローラ物理デバイスの数
	コントローラ論理デバイスの数
	コントローラ パートナー ステータス
	コントローラのメモリ サイズ
	コントローラのドライブ チャンネルの数
	コントローラの充電回数
	コントローラ ドライバのバージョン
	ControllerPatrolReadState(コントローラ パトロール読み取り状態)
エンクロージャ	エンクロージャの番号
	エンクロージャの名前
	エンクロージャのベンダ
	エンクロージャの状態
	エンクロージャ ステータス
	エンクロージャの ID
	エンクロージャ サービス タグ
	エンクロージャの資産タグ
	エンクロージャの資産名
	エンクロージャの製品 ID
	エンクロージャの種類
	エンクロージャのチャンネル番号
	エンクロージャのバックプレートのパーツ番号
	エンクロージャ SCSI ID
	エンクロージャのパーツ番号
	エンクロージャ シリアル番号
EMM	EMM の番号
	EMM の名前
	EMMRevision(EMM リビジョン)
	EMM ベンダ
	EMM の状態
	EMM のパーツ番号
	EMM のファームウェア バージョン
	EMM のステータス
仮想ディスク	仮想ディスク番号
	仮想ディスク名
	仮想ディスク デバイス名

	仮想ディスクの状態
	仮想ディスクのステータス
	仮想ディスク長
	仮想ディスク書き込みポリシー
	仮想ディスク読み取りポリシー
	仮想ディスク キャッシュ ポリシー
	仮想ディスク レイアウト
	仮想ディスクのストライプ サイズ
	仮想ディスクのターゲット ID
所有権	購入費
	運送状番号
	インストール日
	注文書番号
	購入日
	署名局名
	支出した初期システム構成
	初期システム構成ベンダ名
	コスト センター情報ベンダ名
	ユーザー情報ユーザー名
	延長保証の開始日
	延長保証の終了日
	延長保証のコスト
	延長保証の提供社名
	所有者コード
	企業所有者名
	危険廃棄物コード名
	DeploymentDurationUnitType(展開期間の単位のタイプ)
	トレーニング名
	外注に関する問題の説明
	外注サービス料金
	外注署名局
	外注プロバイダ料金
	外注プロバイダのサービス レベル
	保険会社名
	資産タグ名ボックス
	システム名ボックス
	CPU シリアル番号名ボックス
	減価償却期間
	減価償却期間単位の種類
	減価償却のパーセント
	減価償却の方法
	登録済み申請

表 C-2. レポート用の EMC および MD3000 ストレージのインベントリ属性

コンポーネント	属性
アレイ ディスク	アレイ ディスクの番号
	アレイ ディスクの名前
	アレイ ディスク長
	アレイ ディスクのバスの種類
	アレイ ディスク LUNid
	アレイ ディスクのパーツ番号
	ArrayDiskUserCapacity(アレイ ディスク ユーザー容量)
	アレイ ディスクのベンダ名
	アレイ ディスクの状態
	アレイ ディスクのモデル番号

	アレイ ディスクのシリアル番号
	アレイ ディスク リビジョン
	アレイ ディスクのチャネル
	アレイ ディスク エンクロージャ ID
コントローラ	コントローラ番号
	コントローラ名
	コントローラのメモリ サイズ
	コントローラのドライブ チャネルの数
	コントローラの充電回数
	ControllerSPAReadCacheSize(コントローラの SPA 読み取りキャッシュ サイズ)
	ControllerSPAWriteCacheSize(コントローラの SPA 書き込みキャッシュ サイズ)
	ControllerSPBReadCacheSize(コントローラの SPB 読み取りキャッシュ サイズ)
	ControllerSPBWriteCacheSize(コントローラの SPB 書き込みキャッシュ サイズ)
	ControllerCachePageSize(コントローラ キャッシュ ページ サイズ)
	コントローラのベンダ
	ControllerSPAReadCachePolicy(コントローラの SPA 読み取りキャッシュ ポリシー)
	ControllerSPAWriteCachePolicy(コントローラの SPA 書き込みキャッシュ ポリシー)
	ControllerSPBReadCachePolicy(コントローラの SPB 読み取りキャッシュ ポリシー)
	ControllerSPBWriteCachePolicy(コントローラの SPB 書き込みキャッシュ ポリシー)
	コントローラ ファームウェア バージョン
	コントローラ キャッシュ サイズ
	コントローラ物理デバイスの数
	コントローラ論理デバイスの数
	コントローラの種類
	ControllerNumberOfPorts(ポートのコントローラ番号)
エンクロージャ	エンクロージャの番号
	エンクロージャの名前
	エンクロージャの種類
	エンクロージャのパーツ番号
	エンクロージャ シリアル番号
	エンクロージャのベンダ
	EnclosureLocationOfManufacture(エンクロージャの製造場所)
	エンクロージャ サービス タグ
	エンクロージャの製品 ID
	EnclosureNumberOfFanPacks(Fan Pack のエンクロージャ番号)
	EnclosureNumberOfControllers(コントローラのエンクロージャ番号)
	EnclosureNumberOfDisks(ディスクのエンクロージャ番号)
	エンクロージャの ID
	エンクロージャの資産タグ
ストレージ グループ	StorageGroupIndex(ストレージ グループのインデックス)
	StorageGroupLUNId(ストレージ グループの LUN ID)
	StorageGroupName(ストレージ グループ名)
	StorageGroupHostName(ストレージ ホスト名)
仮想ディスク	仮想ディスク番号
	仮想ディスク名
	仮想ディスクのストライプ サイズ
	仮想ディスクのターゲット ID
	VirtualDiskStripeElementSize(仮想ディスクのストライプ エlement サイズ)
	VirtualDiskLUNId(仮想ディスクの LUN ID)
	仮想ディスク デバイス名
	仮想ディスク長
	仮想ディスク書き込みポリシー
	仮想ディスク読み取りポリシー
	仮想ディスク レイアウト
ソフトウェア エージェント	ソフトウェアの種類
	ソフトウェアのバージョン
	ソフトウェアの説明

表 C-3. レポート用のテープ ライブラリのインベントリ属性

コンポーネント	属性
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	DeviceDescription(デバイスの説明)
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム モデルの種類
ファームウェア	ファームウェアの名前
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)
テープドライブ	TapeDriveCleaningRequired(テープドライブ クリーニング必須)
	TapeDriveFirmwareVersion(テープドライブのファームウェア バージョン)
	TapeDriveIndex(テープドライブのインデックス)
	TapeDriveModel(テープドライブのモデル)
	TapeDriveMotionHrs(テープドライブの動作時間)
	TapeDriveSerialNumber(テープドライブのシリアル番号)
	TapeDriveType(テープドライブの種類)
	TapeDriveVendor(テープドライブのベンダ)
テープ ライブラリ	テープ ライブラリのファームウェア バージョン
	TapeLibraryScsiId(テープ ライブラリの SCSI ID)
	TapeLibrarySerialNumber(テープ ライブラリのシリアル番号)
	TapeLibrarySlotCount(テープ ライブラリのスロット数)
	TapeLibraryVendor(テープ ライブラリのベンダ)
	TapeLibraryDriveCount(テープ ライブラリのドライブ数)
	TapeLibraryModel(テープ ライブラリのモデル)

表 C-4. レポート用の FC およびイーサネット スイッチのインベントリ属性

コンポーネント	属性
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	DeviceDescription(デバイスの説明)
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム モデルの種類
ファームウェア	ファームウェアの名前
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)

表 C-5. レポート用の KVM のインベントリ属性

コンポーネント	属性
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	DeviceDescription(デバイスの説明)
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム モデルの種類
ファームウェア	ファームウェアの名前
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)

表 C-6. レポート用の DRAC のインベントリ属性

コンポーネント	属性
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	DeviceDescription(デバイスの説明)
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム モデルの種類
ファームウェア	ファームウェアの名前
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)

表 C-7. レポート用の CMC のインベントリ属性

コンポーネント	属性
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイスの資産タグ
	DeviceDescription(デバイスの説明)
	DeviceManufacturer(デバイスの製造元)
	デバイス名
	DeviceSerialNumber(デバイスのシリアル番号)
	デバイスのサービス タグ
	デバイス システム モデルの種類
ファームウェア	ファームウェアの名前
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)

表 C-8. レポート用のプリンタのインベントリ属性

コンポーネント	属性
プリンタ サプライ	PrinterSupplyIndex(プリンタ サプライのインデックス)
	PrinterSupplyDescription(プリンタ サプライの説明)
	PrinterSupplyType(プリンタ サプライの種類)
	PrinterSupplyLevel(プリンタ サプライ レベル)
	PrinterSupplyMaxLevel(プリンタ サプライの最大レベル)
プリンタの給紙トレイ	PrinterInputIndex(プリンタの給紙トレイのインデックス)
	PrinterInputName(プリンタの給紙の名前)
	PrinterInputVendorName(プリンタの販売業者名)
	PrinterInputModel(プリンタ給紙トレイのモデル)
	PrinterInputDescription(プリンタ給紙の説明)
	PrinterInputMaxCapacity(プリンタ給紙の最大容量)
プリンタの排紙トレイ	PrinterOutputIndex(プリンタ排紙のインデックス)
	PrinterOutputName(プリンタの排紙の名前)
	PrinterOutputVendorName(プリンタの販売業者名)
	PrinterOutputModel(プリンタ排紙トレイのモデル)
	PrinterOutputDescription(プリンタ排紙の説明)
	PrinterOutputMaxCapacity(プリンタ排紙の最大容量)
プリンタ カバー エントリ	PrinterCoverIndex(プリンタ カバーのインデックス)
	PrinterCoverDescription(プリンタ カバーの説明)
	PrinterCoverStatus(プリンタ カバーのステータス)
エージェント	エージェントの説明
	エージェントのグローバル ステータス
	エージェントの ID
	エージェントの製造元
	エージェントの名前
	エージェントのバージョン
連絡先	連絡先の情報
	ContactLocation(連絡先のロケーション)
	連絡先名
デバイス	デバイス ロケーション
	デバイス システム モデルの種類
ファームウェア	ファームウェアのシャーン インデックス
	ファームウェアのインデックス
	ファームウェアの名前
	ファームウェアのリリース日
	ファームウェアの種類
	ファームウェア バージョン
ネットワーク	NICIPAddress(NIC IP アドレス)
	NIC MAC アドレス
	NICDescription(NIC の説明)

表 C-9. 電源のインベントリの属性

コンポーネント	属性
電源の監視 (xx0x and xx1x Server 用)	ピーク アンペア数
	ピーク電力 (W)
	ピーク電力 (BTU/hr)
	ピーク アンペア (開始時刻)
	ピーク アンペア (時刻)
	ピーク電力 (開始時刻)

	ピーク電力 (時刻)
電力予算 (xx0x and xx1x Server 用)	ピーク ヘッドルーム (W)
	アイドル状態の電力 (W)
	最大潜在電力 (W)
	キャップ値 (W)
	ピーク ヘッドルーム (BTU/hr)
	アイドル状態の電力 (BTU/hr)
	最大潜在電力 (BTU/hr)
キャップ値 (BTU/hr)	
電力プロファイル	プロファイル設定

---

[目次のページに戻る](#)



[目次のページに戻る](#)

## Dell Management Console の

### セキュリティ

Dell™ Management Console Version 1.1 ユーザーズ ガイド

#### ● [ビルトイン セキュリティ機能](#)

## ビルトイン セキュリティ機能

Dell Management Console では次のポートを提供しています。

### ポート

[表B-1](#)には、標準オペレーティング システム サービスである Dell Management Console とほかのエージェント アプリケーションで使用されるポートが一覧表示されています。

Dell Management Console がファイアウォールを介してリモート デバイスに接続できるようにするには、ポートを正しく構成する必要があります。

[表B-1](#)で示されているシステム管理ソフトウェアのバージョンは、そのポートを使用するために必要な最低バージョンです。

表 B-1. Dell Management Console のポート

ポート	プロトコル	ポート タイプ	Dell Management Console のバージョン	最大暗号化レベル	方向	使用	構成可能
22	SSH	TCP	[1.x]	128-bit	なし	SSH クライアント	はい
						Server Administrator へのリモートソフトウェア アップデート- Linux オペレーティング システムをサポートしているシステム用	
						Linux システムのパフォーマンス監視	
23	Telnet	TCP	[1.x]	なし	入力/出力	Telnet から Linux デバイス	いいえ
25	SMTP	TCP	[1.x]	なし	入力/出力	Dell Client Manager Console からの電子メール警告アクション (オプション)	いいえ
67, 68, 69, 4011	PXE	UDP				再起動して DHCP は	
68	UDP	UDP	[1.x]	なし	入力/出力	Wake-on-LAN	はい
53, 80, 135, 137, 139, 150, 1433, 2500		TCP				Altiris Console: リモート コンピュータ使用のコンソール	
80	HTTP	TCP	[1.x]	なし	入力/出力	アプリケーションの起動- PowerConnect™ Console	いいえ
ICMP						ping	
135, 137, 139, 445		TCP/UDP				HTTP 以外の通信 (例: UNC を使用したクライアント パッケージのダウンロード)	

135	RPC/DCOM	TCP/UDP	[1.x]	なし	入 力/ 出 力	WMI/CIM 管理クエリ	いいえ
138		UDP				NS クライアントのインストール	
161	SNMP	UDP	[1.x]	なし	入 力/ 出 力	SNMP クエリ管理	いいえ
162	SNMP	UDP	[1.x]	なし	入 力/ 出 力	SNMP イベント受信およびトラップ転送	いいえ
389	LDAP	TCP	[1.x]	128-bit	入 力/ 出 力	IT Assistant ログオンのドメイン認証	
401-402		TCP/UDP			入 力/ 出 力	Deployment Solution	
443	専用/Altiris Agent, WSMAN	TCP	[1.x]	なし	入 力/ 出 力	EMC ストレージ検出およびイベントリ、Altiris Agent が一度インストール済み	いいえ
445		UDP				HTTP 以外の通信 (例: UNC を使用したクライアント パッケージのダウンロード)	
623	RMCP	UDP	[1.x]	なし	入 力/ 出 力	IPMI、WS-MAN、および ASF 管理	はい
664	RMCP	UDP			入 力/ 出 力	セキュア ASF 管理	はい
1010	PXE	TCP				Deployment Solution: PXE 構成サービスと通信する PXE 構成	
1011		TCP				Monitor Solution	
2070-2073, 1758-1759	PXE	UDP				Deployment Solution: PXE イメージの TFTP と MFTP 転送用の PXE	
3389	RDP	TCP	[1.x]	128 ビット SSL	入 力/ 出 力	アプリケーションの起動-リモート デスクトップから Windows ターミナル サービス	はい
3829, 4949, 4950, 4951		TCP				Altiris Deployment Solutions と PCT Real Time が PCTWiz と RTDestAgent 間の通信および RTDestAgen の検索に使用	
4952		TCP				接続切断の管理に使用される Deployment Solutions 通信	
6389	専用	TCP	[1.x]	なし	入 力/ 出 力	ホスト システム ( NaviCLI/NaviSecCLI または Navisphere Host Agent) とストレージ システム上の Navisphere Array Agent 間の通信を有効にします。	いいえ
8080						Deployment Solutions Web Console	
16992					出 力	AMT 管理 (セキュリティなし)	いいえ
16993					出 力	AMT 管理 (セキュリティあり)	いいえ
16994					出 力	AMT 管理リダイレクト サービス (セキュリティなし)	いいえ
16995					出 力	AMT 管理リダイレクト サービス (セキュリティあり)	いいえ
50120-50124						Task Server	
52028, 52029		TCP				NS クライアント マルチキャスト	
1024 - 65535	DCOM	TCP/UDP	不明	なし	入 力/ 出 力	WMI クエリ管理 (ランダム ポート)	OS - <a href="http://msdn.microsoft.com/enus/library/ms809327.aspx">msdn.microsoft.com/enus/library/ms809327.aspx</a>



[目次のページに戻る](#)

## Dell OpenManage ITAssistant の検出設定の移行

Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [IT Assistant 検出設定のインポート](#)
- [データベース移行のユーザー インターフェイス](#)
- [IT Assistant 検出設定の移行前の注意事項](#)

Dell™ OpenManage™ IT Assistant を使用したことがないか、検出範囲を Dell Management Console に移行しない場合は、このセクションをスキップしてください。

IT Assistant の既存のユーザーである場合は、このセクションを読み、検出範囲を Dell Management Console に移行する方法について確認してください。


Dell Management Console では、IT Assistant 8.0 以降の検出設定情報を移行できます。

---

### IT Assistant 検出設定のインポート

次の検出設定を IT Assistant データベースから Dell Management Console に移行できます。

- 1 除外範囲
- 1 包含範囲
- 1 包含範囲に関連付けられたプロトコル情報:
  - 1 SNMP: 再試行回数、タイムアウト、読み取りコミュニティ名

 **メモ:** DellManagement Console には書き込みコミュニティ名がないため、書き込みコミュニティ名は移行されません。

- 1 ICMP: 再試行回数とタイムアウト
- 1 Dell|EMC NaviCLI@: ユーザー名とパスワード
- 1 IPMI: 再試行回数、タイムアウト、ユーザー名、パスワードおよび KGkey
- 1 CIM: ドメイン名、ユーザー名およびパスワードドメイン名を入力しない場合は、[ローカル ホスト] が使用されます。
- 1 Dell™ PowerVault™ MD Storage Arrayプロトコルの有効化/無効化情報
- 1 検出スケジュール情報

---

### データベース移行のユーザー インターフェイス

データベース移行のリンクへは、[ホーム] → [Dell Management Console ポータル] をクリックすることでアクセスできます。[Quick Start] タブの [Dell Enterprise Management Quick Start] Web パーツで、[Dell OpenManage IT Assistant の検出設定の移行] をクリックします。

---

### IT Assistant 検出設定の移行前の注意事項

- 1 IT Assistant 8.0 以降からDell Management Console データベースに移行できるのは検出範囲のみです。
- 1 データベースの移行プロセスを開始した後は、移行をキャンセルしたり、中止したりできません。
- 1 リモートの IT Assistant データベースからデータを移行したり、データベースの名前付きインスタンスからデータを移行したりすることもできます。ローカル システムとリモート データベース間の接続が機能していることを確認してください。
- 1 検出範囲を移行する前に、検出タスクごとに使用されるスレッドの数を減らして、DellManagement Consoleシステムにかかる負荷を軽減することができます。デフォルト値の 40を変更するには、[設定] → [すべての設定] を選択します。右側のウィンドウで、[設定] → [検出とインベントリ] → [Network Discovery の設定] を選択し、デフォルト値を変更します。

移行後に Network Discovery の設定を変更する場合は、各検出タスクを選択して編集する必要があります。詳細については、「[検出のパフォーマンス](#)」を参照してください。

## リモート データベース

リモート データベースを指定するには、ローカル システムとリモート データベース間の接続が機能していることを確認してください。リモート データベース接続を有効にするには、「[SQL Server 2005 または 2008 Express へのリモート接続の有効化](#)」を参照してください。ITAssistant データベースのロケーションと認証モードを指定する必要があります。

- 1 Microsoft® Windows® 認証: ユーザー名とパスワードが ITAssistant と Dell Management Console で同じであることを確認してください。
- 1 混合/SQL 認証: ITAssistant データベースの管理者 SQL ログイン資格情報を指定します。指定された SQL ログイン資格情報は、有効であり、リモート データベースに対して適切なサーバー ロールおよびユーザー マッピングがある必要があります。

IT Assistant は、Windows 認証モードのみを使用してデータベースを作成します。SQL 認証を使用するには、認証モードを変更します。詳細については、「[SQL Server および Windows 認証の有効化](#)」を参照してください。

IT Assistant は、リモート データベースのデフォルトのインスタンスをサポートします。名前付きインスタンスで ITAssistant のデータベースを構成している場合は、サーバー名と一緒に名前付きインスタンスを指定してください (例: MyServer/NamedInstance)。

## SQL Server 2005 または 2008 Express へのリモート接続の有効化

デフォルトでは、SQL Server はリモート データベースに自動的に接続しません。接続を手動で有効にする必要があります。Microsoft Windows の ODBC Data Source Administrator ツールを使用して、リモート データベースの接続を確認してください。リモート接続を有効にしないリモート SQLServer に接続すると、エラーが表示されます。

このエラーを解決するには、次の手順に従います。

- 1 SQL Server 上で SQLServer および Windows 認証モードの両方を有効にします。
- 1 TCP/IP プロトコルを使用して、リモート接続を有効にします。

## SQL Server および Windows 認証の有効化

SQL Server および Windows 認証を有効にする方法

- 1 ローカル SQL Server 上で、Windows 認証ユーザー資格情報を使用し、SQL Server Management Studio Express を使用して、SQL Server にログインします。SQL Server への認証に Windows アカウントが使用されます。
- 2 **オブジェクト エクスプローラ**で、インスタンス名を右クリックし、[ **プロパティ** ] を選択します。
- 3 左側のウィンドウで、[ **セキュリティ** ] を選択し、サーバー認証を [ **SQL Server および Windows 認証モード** ] に変更します。
- 4 インスタンス名を右クリックし、[ **再起動** ] を選択して SQL Server サービスを再開し、変更を有効にします。

## リモート接続の有効化

リモート接続を有効にする方法

- 1 [ **SQL Server Surface Area Configuration** ] を開きます。
- 2 [ **Surface Area Configuration for Services and Connections** ] を選択します。
- 3 左側のウィンドウで、SQL Server インスタンス → [ **Database Engine** ] → [ **リモート接続** ] を展開します。
- 4 右側で、[ **ローカルおよびリモート接続** ] → [ **TCP/IP と名前付きパイプの両方を使用する** ] を選択します。
- 5 左側で、[ **SQL Server ブラウザ** ] → [ **サービス** ] を選択します。
- 6 右側で、起動タイプが [ **無効** ] である場合は、[ **自動** ] に変更し、[ **適用** ] をクリックします。
- 7 [ **開始** ] をクリックしてサービスを開始し、[ **OK** ] をクリックします。
- 8 SQL Server 認証モードを使用してリモートシステムから SQL Server にログインします。

## ITAssistant 8.x からの検出情報の移行

1. Dell Management Console をインストールします。
2. Dell Management Console を起動します。
3. **[ホーム]**→ **[Dell Management Console ポータル]** をクリックします。
4. **[クイック ガイド]** タブの **[Dell Enterprise Management Quick Start]** Web パーツで、**[Dell OpenManage IT Assistant の検出設定の移行]** をクリックします。

**[IT Assistant 検出設定の移行]** ページが表示されます。

5. **[検出設定の移行]** Web パーツで、**[移行ウィザードの起動]** をクリックします。
6. ウィザードの最初のページで、IT Assistant データベースへの接続に必要なパラメータを入力します。

ローカルまたはリモートで構成されている ITAssistant データベースを指定できます。

ITAssistant がデータベースの名前付きインスタンス上で構成されている場合は、その情報を **[データベース サーバー名]** で指定します。


例: MyITAssistant\MyNamedInstance。

必要な認証モードを選択します。

**[次へ]** をクリックします。

7. 2 番目のページには、前のウィンドウで入力した ITAssistant データベースから取得された検出範囲が表示されます。

**[包含範囲]** リストボックスに ITAssistant から取得された、有効なすべての包含範囲が表示されます。

 **メモ:** [包含範囲] 内でサブ範囲が無効になっている場合、そのサブ範囲は Dell Management Console に移行されません。

**[除外範囲]** リストボックスに ITAssistant から取得された、すべての除外範囲が表示されます。

**[包含範囲]** リストボックスから各包含範囲を選択し、その詳細 (プロトコルおよび関連付けられている設定) を表示します。

**[次へ]** をクリックします。

8. ウィザードの 3 番目のページには、ITAssistant の移行スケジュール情報が表示されます。

ただし、移行タスクを直ちに実行したい場合は、**[今すぐ実行]** を選択し、**[次へ]** をクリックします。

9. ウィザードの最後のページは、情報のみのウィンドウです。

**[完了]** をクリックして移行を開始します。

## Dell Management Console での移行されたデータの表示

Dell Management Console で移行されたデータを表示する方法

1. **[ホーム]** → **[検出およびインベントリ]** → **[Network Discovery]** をクリックします。
2. **[Network Discovery タスクの管理]** Web パーツの **[使用可能なタスク]** タブで、移行されたさまざまなスキャン グループ (検出タスク) を表示できます。

移行された検出タスクは、[IT Assistant の移行対象検出タスク - <包含範囲>] のように表示されます。

[実行タスク] タブでは、検出タスク ステータスを表示できます。

3. 移行された検出タスクのプロトコルを表示するには、[設定] → [すべての設定] → [監視と警告] → [資格情報の設定] → [資格情報管理] を選択します。

移行された検出タスクの接続プロファイルを表示するには、[設定] → [すべての設定] → [監視と警告] → [プロトコル管理] → [接続のプロファイル] → [接続プロファイルの管理] を選択します。

詳細については、「[検出タスクの実行](#)」および「[インベントリタスクの結果の表示](#)」を参照してください。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## 検出とインベントリ設定の構成


Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [検出ユーザー インタフェース](#)
- [検出設定を構成する前に](#)
- [接続プロファイルと資格情報の管理](#)
- [検出タスクの作成](#)
- [新規組織ビューと組織グループの作成](#)
- [インベントリの設定の構成](#)

Dell™ Management Console では検出、インベントリの収集、ユーザーへの警告、ドライバ、BIOSおよびファームウェアのアップデート、そして企業内の各システムの様々なタスクを実行することができます。管理対象システムには、サーバー、プリンタ、テープ デバイス、ストレージ デバイス、リモート アクセス カード搭載システム、Dell PowerConnect™ スイッチおよびラック集中システムで使用されるデジタル キーボード/ビデオ/マウス (KVMs) スイッチなどが含まれます。

このセクションでは、中小企業 (50 サーバーと 200 以上のクライアント システム、そして 10 スイッチ) のシステム管理者がどのように Dell Management Console の Discovery Solution と Inventory Solution を使用するかを説明します。

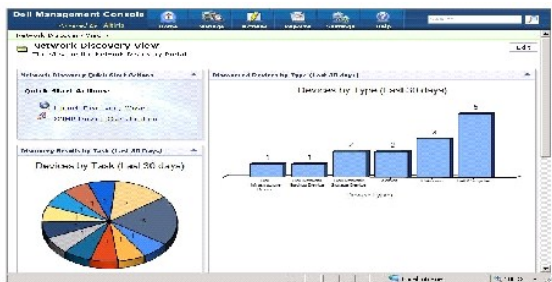
シナリオではネットワーク環境管理担当の管理者がどのように Dell Management Console を構成するかを説明します。

 **メモ:** これらのシナリオは、Dell Management Console の全能力を説明するものではありません。

## 検出ユーザー インタフェース

[検出] ポータルにアクセスする方法 [ホーム] → [検出とインベントリ] → [Network Discovery] をクリックします。

### 検出ユーザー インタフェースの概要



初めてネットワーク デバイスの検出の構成を扱う場合は、[Network Discovery Quick Start アクション]の Web パーツを使用することをお勧めします。

スクリーンの下部にある [Network Discovery タスク管理]の Web パーツには、利用可能な検出タスクおよび実行されたタスクが表示されます。

[タスク別の検出結果]の Web パーツには、タスクの実行およびタスクによって検出されたデバイス数が表示されます。

[検出済みデバイスの分類]の Web パーツには、検出された様々なデバイスが表示されます。(例: サーバー、プリンタ、テープ、スイッチなど)



## 検出設定を構成する前に

Dell Management Console を使用して検出を構成する前に、ネットワークに基づき基本的な意思決定を下す必要があります。特に次のことについて決断する必要があります。

- 1 検出するシステムのホスト名、IP アドレスまたは IP サブネット範囲。
- 1 デバイスと通信するために必要な資格情報。たとえば、もし Microsoft® Windows® システムを WMI プロトコルを使用して検出する場合、DellManagementConsole に対する Windows の資格情報を入力する必要があります。「[資格情報の管理](#)」を参照してください。
- 1 ネットワーク上のシステムとデバイスの管理に必要なシステム管理プロトコル (クイック レファレンス: [表 5.1](#))

プロトコルを管理するには、デバイスがサポートするシステム管理プロトコルに従い、接続プロファイルを作成する必要があります。詳細については、「[接続プロファイル](#)」を参照してください。

## 接続プロファイルと資格情報の管理

Credential Manager を使用して、様々なプロトコルを介した接続に使用される資格情報などの極秘データを暗号化し保存することができます。

接続プロファイルとは、論理セットとして構成および保存できるプロトコルのセットとこれらの対応する資格情報のことです。このセットは、定義されているプロトコルの使用の対照として Discovery、Inventory、および Monitoring Solutions によって使用されます。

Dell Management Console では、デバイスとの通信に接続プロファイルが使用されます。認証を必要とするデバイスを識別し、これらの資格情報のリストを準備しておく必要があります。そして、これらのデバイスの接続プロファイルを作成する必要があります。たとえば、ネットワーク上の 10 台のサーバーが別々の認証資格情報を持っている場合は、各システム用の接続プロファイルを作成しなければなりません。

## 資格情報の管理

Dell|EMC ストレージ デバイスをネットワークに追加し検出するには、Discovery Solution が Dell|EMC デバイスと通信するための資格情報を提供します。

- 1 Dell Management Console で、**[設定]**→**[すべての設定]** をクリックします。
- 2 左側のウィンドウの **[設定]**→**[監視と警告]**→**[資格情報の設定]** フォルダの下で、**[資格情報管理]** を選択します。
- 3 右側のウィンドウで **[資格情報の追加]** をクリックします。
- 4 **[資格情報の追加]** のダイアログ ボックスで、**資格情報タイプ**として **[EMC 資格情報]** を選択します。
- 5 資格情報の名前 (例: emc-cred) を入力します。

Dell|EMC デバイスのユーザー名とパスワードを入力し、**[OK]** をクリックします。

新しい資格情報は、**[資格情報管理]** ページに表示されます。

## 接続プロファイル

Dell Management Console では、デフォルトの接続プロファイルが提供されています。このプロファイルでは次のプロトコルが有効になっています。

- 1 HTTP
- 1 ICMP
- 1 SNMP V1 V2
- 1 SNMP トラップ送信者
- 1 WMI


テンプレートとして保存されているデフォルトの接続プロファイルを参照し、ネットワーク デバイスの検出に使用するプロトコルを含む新しい接続プロファイルを作成します。

## デフォルトの接続プロファイルの表示

デフォルトの接続プロファイルの表示方法

1. **【設定】**→ **【すべての設定】** をクリックします。
2. 左側のウィンドウで **【設定】** フォルダ→ **【監視と警告】**→ **【プロトコル管理】**→ **【接続プロファイル】**→ **【接続プロファイルの管理】** を選択します。

プロトコルを追加または削除するようにデフォルトの接続プロファイルを編集します。

 **メモ:** デフォルトの接続プロファイルが既に存在する場合でも、各プロトコル用に適切な資格情報を構成する必要があります。


## デフォルトの接続プロファイルの編集

デフォルトの接続プロファイルを編集するか、あるいは **【設定の追加】** をクリックして新しい接続プロファイルを追加することができます。

1. **【接続プロファイルの管理】** ページで **【デフォルトの接続プロファイル】** を選択し、**【編集】** (鉛筆のアイコン) をクリックします。

**【グループ設定の定義】** ページにデフォルト プロファイルで事前構成されているプロトコルが表示されます。-

2. **【グループ設定の定義】** ページで **オン** を選択し、IPMI を有効にします。
3. 上向き矢印をクリックしてデバイスの管理対象デバイスまたはグループの IPMI 資格情報を追加します。

 **メモ:** IPMI が正常に機能するには、管理対象デバイスの KGKey を入力する必要があります。デバイスの IPMI 資格情報プロファイルに KGKey を入力します。詳細については、[「資格情報の管理」](#)を参照してください。

4. ネットワーク デバイスは HTTP、ICMP、および SNMP Trap Sender を使用しないため、これらを無効にします。

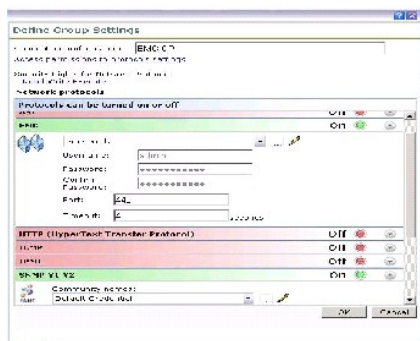
多数のプロトコルがあるとデバイスの検出速度が低下するため、ネットワークの検出に不要なプロトコルは無効にすることをおすすめします。

5. **【OK】** をクリックします。

## 新しい接続プロファイルの作成

ネットワークに Dell|EMC デバイスを追加する場合、デフォルトの接続プロファイルでは必要とされるシステム管理プロトコルが有効になっていないため、デフォルトの接続プロファイルを使用することはできません。EMC と SNMP が有効になっている新しい接続プロファイルを作成する必要があります。(各種デバイスで必要とされる接続プロファイルは、[表5-1](#) を参照してください。)

1. [「デフォルトの接続プロファイルの表示」](#)を参照してください。
2. **【接続プロファイルの管理】** ページで **【設定の追加】** をクリックします。
3. **【グループ設定の定義】** ウィンドウで EMC プロトコルをオンにし、下向きの矢印をクリックして EMC 資格情報を構成します。



4. 接続プロファイル名 (例: EMC\_SNMP) を入力します。
5. ドロップダウン リストから emc-cred を選択します ([資格情報の管理](#) を参照)。

Dell Management Console は emc-cred 情報を取り込んですべてのフィールドに投入します。

6. SNMP V1 V2 プロトコルを選択してオンにし、下向きの矢印をクリックして SNMP 資格情報を構成してから [OK] をクリックします。

新しい接続プロファイルは [\[接続プロファイルの管理\]](#) ページに表示されます。


表 5-1. 各種デバイスで必要とされるプロトコルと接続プロファイル

デバイス	サポートされているシステム管理プロトコル	接続プロファイル用のプロトコル
サポートされる Microsoft Windows オペレーティング システムを実行しているサーバー	SNMP、WMI、および IPMI	SNMP、WMI、または IPMI、あるいはこれらのコンビネーション
サポートされている Linux オペレーティング システムを実行しているサーバー	SNMP および IPMI	SNMP または IPMI、あるいはこれらのコンビネーション
Dell PowerVault™ ストレージ システム	MD アレイ	MD アレイ
Dell PowerConnect スイッチ	SNMP	SNMP
テープ	SNMP	SNMP
プリンタ	SNMP	SNMP
Dell EMC	SNMP と Navisphere® Secure CLI	SNMP および EMC
リモート アクセス コントローラ	SNMP	SNMP
Digital KVM	SNMP	SNMP
ライフサイクル コントローラを実行しているサーバー	Web Services for Management (WS-MAN)	WS-MAN
Dell EqualLogic	SNMP	SNMP


## 検出タスクの作成

1. [ホーム] → [検出とインベントリ] → [Network Discovery] をクリックします。
2. [Network Discovery のホーム] ページの [Network Discovery の QuickStart 操作] Web パーツで [検出ウィザードの起動] をクリックします。

[ネットワーク デバイスの検出] ページが表示されます。

 **メモ:** [Network Discovery のホーム] ページの [使用可能なタスク] タブで [新規] をクリックして、検出タスクを作成することもできます。

3. 「ステップ 1: デバイス検出方法の選択」で [対象ネットワークのスキャン] を選択し、[次へ] をクリックします。

 **メモ:** ARP を選択した場合は、SNMP 要求を許可するように構成されたルータの IP アドレスを入力します。

4. 「ステップ 2: ネットワーク IP 範囲の入力」で [包含] → [カスタム範囲] をクリックします。

カスタム範囲は、様々なサブネットを同時に定義するために使用されます。たとえば、サブネットマスクが 255.255.255.0 のカスタム範囲「10.94.\*.\*」では、10.94.1.1 から 10.94.255.254 までの IP アドレスをスキャンします。

カスタム範囲が広くなるとデバイスの検出に長時間かかるため、カスタム範囲の使用には注意します。

5. [カスタム範囲] ダイアログ ボックスで下記の情報を入力し、[次へ] をクリックします。

カスタム範囲: 10.94.168.\*

マスク: 255.255.255.0

- 「ステップ 3: **デバイス通信プロトコルの選択**」で**[デフォルトの接続プロファイル]**を選択します。このプロファイルでは HTTP、ICMP、SNMP、および WMI などのプロトコルが選択されています。
- IPMI プロトコルも含めるように **[デフォルトの接続プロファイル]**を編集し、**[次へ]**をクリックします。

[「デフォルトの接続プロファイルの編集」](#)を参照してください。

- 「ステップ 4: **タスク名の入力**」で**タスク名**として「Discover\_All」と入力し、**[次へ]**をクリックします。
- 「ステップ 5: **検出を実行する時期の選択**」でタスクのスケジュールを選択します。

要件に基づき、ネットワーク上のデバイスの検出をスケジュールします (例: 週に1回)。

スケジュールを週に1回実行するには、次の操作を行います。

**スケジュール:** 共有スケジュール

**共有スケジュールの選択:** 週単位

**[新規]**をクリックします。

- [新規共有スケジュールの作成]** ページで、スケジュールの名前と説明を入力します。


**[スケジュールの追加]** → **[予定開始時刻]** を選択し、0600 を検索タスクの開始時間として選択します。

**[繰り返しなし]** をクリックして **[繰り返しのスケジュール]**のスクリーンで**週と月曜日**を選択します。

**[OK]** をクリックします。

- [ネットワーク デバイスの検出]** ページで **[完了]** をクリックします。

「Discover\_All」タスクが **[サーバー タスク]** → **[ネットワーク タスク]** フォルダの下のタスク管理ポータルに表示されます。

 **メモ:** 別の認証資格情報を持つすべてのデバイスまたはデバイスのグループには、新しい接続プロファイルが必要です。各デバイスあるいはグループのデバイス用に別々の検出タスクを作成し、適切な接続プロファイルにマップする必要があります。

## 検出タスクの実行

検出タスクを作成した後、「Discover\_All」タスクを実行する場合は、次のステップに従います。

- [ホーム]** → **[検出とインベントリ]** → **[Network Discovery]** をクリックします。

**[Network Discovery ホーム]** ページが表示されます。

- [Network Discovery タスク管理]** の Web パーツで、**[使用可能なタスク]** のタブをクリックします。
- 「Discover\_All」タスクを選択し、**[今すぐ実行...]** をクリックします。

Dell OpenManage™ ITAssistant から移行された検出タスクも実行することができます。

検出タスクの移行に関する詳細は、[「ITAssistant 8.x からの検出情報の移行」](#)を参照してください。

デバイスの詳細を表示するには、ネットワークを検出した後にインベントリ タスクを作成し、実行する必要があります。詳細については、[「すべてのシステムのインベントリを収集するためのインベントリタ](#)

[スクの作成](#)を参照してください。

## 検出されたデバイスの表示

検出されたネットワーク デバイスを表示するには、次のステップに従います。

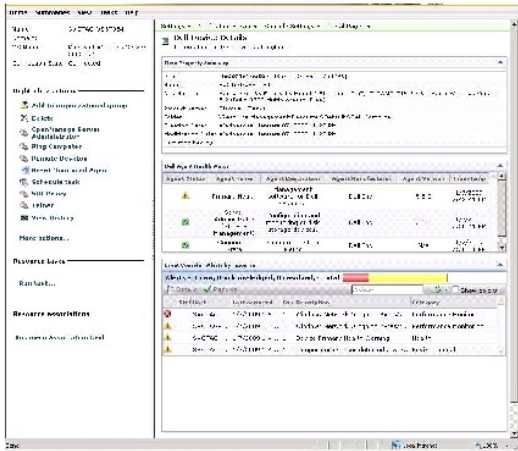
1. **【管理】** → **【すべてのデバイス】** をクリックします。
2. 左側のウィンドウで、サーバーを選択して検出されたシステムを表示します。

Dell OpenManage Server Administrator がインストールされているすべてのサーバーは、**リソース タイプ=Dell コンピュータ**として検出されます。

他のリソース タイプの詳細は、「[表4-1](#)」を参照してください。

3. システムを選択してダブルクリックし、詳細を表示します。

このシステムの **【リソース マネージャ】** ページが表示されます。



**メモ:** 検出されたデバイスのヘルスが標準の場合、プライマリヘルスマトリックが **【Dell Agentヘルスステータス】** の Web パーツに表示されるまで少し時間がかかります。ヘルスマトリックの詳細は、[表9-8](#)を参照してください。

## 注意事項

1. **【すべてのデバイス】** ツリーに表示されている仮想マシン、モジュラーシステム、またはクラスタを削除する必要がある場合は、先ずグループの下のデバイスを削除してからグループを削除します。検出範囲からもグループを削除します。そうしないと各検出サイクルの後にグループが表示されます。

## リソース マネージャ


**【リソース マネージャ】** ページには、スクリーン右側のウィンドウに2つの Web パーツがあります。

**【項目のプロパティの概要】** の Web パーツには、検出されたデバイスに関する全般情報が含まれています。

**【Dell Agentヘルスステータス】** の Web パーツには、デバイスに関連付けられているすべてのエージェントが表示されます。この Web パーツは、ServerAdministrator、Storage Management、および RemoteAccess Controller などの管理エージェントのステータスを提供します。この情報は、SNMP または WMI プロトコルを使用して取得されます。

エージェントヘルスステータスは、Monitor Solution が生成したイベントによって決定されます。詳細は「[監視と警告](#)」を参照してください。検出後、リソース マネージャには検出されたエージェントの

ステータスが表示されます。Monitor Solution が 1 つ以上の管理対象エージェントからの警告を発する場合、エージェントのステータスは重大、警告、または不明に変更されます。

 **メモ:** すべてのエージェントがすべてのデバイス上で利用可能であるとは限りません。たとえば、Storage Management Service Remote Access Controller がシステムにインストールされていない場合、これらのコンポーネントに関するエージェント情報は表示されません。エージェントがないということは、適切なソフトウェアがインストールされていないかハードウェアが適切に有効化されていないことを示します。

また、異なるデバイス タイプは異なるエージェントを表示します。

エージェントのステータスは、監視されているデバイスに対して受信したヘルス タイプの警告に直接関連しています。たとえば、プライマリ ヘルスに「警告」または「重大」が表示された場合、対応するヘルス警告が [Event Console] の Web パーツに表示されます。

Event Console はシステム、ソフトウェア、プリンタ、および他のデバイスを監視するための個別のツールを維持する必要性を削減します。Event Console は、SNMP トラップと他のステータス メッセージを収集し、これらを単一のロケーションで表示します。すべてのステータスメッセージは、Dell Management Console データベース内の影響を受けているリソースに各受信メッセージをリンクする共通のフォーマットに変換されます。これらのフォーマット済みのメッセージは「警告」と呼ばれます。

Event Console でトラップが FC スイッチ、イーサネット スイッチまたは EMC アレイから生成された場合、デバイスの IP アドレスが表示されます。しかしデバイスがすでに Dell Management Console で検出されていてもデバイスの名前は表示されません。

Event Console は、次にあげる方法で警告を処理できるルール ベースのトリガ システムも提供します。

- 1 特定の警告に応じた Task Server タスクを起動する。

一部のデバイスで検出の起動タスクが利用可能な場合、次が可能です。

- 1 警告データベースに特定の警告が保存されることを防ぐ。
- 1 別の管理システムに警告を転送する。

Event Console に関する詳細は、[ヘルプ] → [コンテキスト] から Symantec のマニュアルを参照してください。

[リソース マネージャ] スクリーンの左側でデバイスとデバイスの接続状態に関する基本情報を確認できます。接続情報には、デバイスがオンラインかどうかが表示されます。

[右クリック アクション] のセクションでは、デバイス上で実行できるアクションのセットが表示されます。このアクションのリストは状況感知型で、表示されるアクションは検査されているデバイスのタイプ(システム、デバイス、アウトオブバンドデバイス、プリンタなど)に依存します。

## 検出ログ

検出ログでは、検出タスクのステータスを確認することができます。ログは、検出の問題のトラブルシューティングを行う時に役立つデータを提供します。デフォルトでは、Dell Management Console はログ エントリを保存しません。

検出ログ記録を有効にするには、次のステップに従います。

 **メモ:** 多数のデバイスを検出する場合、検出ログを有効にすると Dell Management Console のパフォーマンスに影響を及ぼす可能性があります。

- 1 [設定] → [すべての設定] をクリックします。
- 2 左側のウィンドウで、[検出とインベントリ] フォルダ → [検出ログの設定] を選択します。
- 3 右側のウィンドウで、[設定の変更] をクリックします。
- 4 [検出ログ記録を有効にします] を選択し、検出ログの保存場所へのパスを入力して [設定の保存] をクリックします。
- 5 ブラウザ ウィンドウを閉じ、Altiris™ Object Host Service を再起動します。

## 検出のパフォーマンス

Dell Management Console の検出タスクのパフォーマンスを管理するには、検出タスクを作成する前に各検出タスクに必要なスレッド数を設定することができます。

1. **【設定】**→ **【すべての設定】** をクリックします。
2. **【設定】**→ **【検出とインベントリ】** → **【Network Discovery の設定】** をクリックします。
3. 右側のウィンドウで**検出タスク**ごとの最大のスレッド数を変更します。

この値は、作成したすべての検出タスクに適用されます。

検出タスクの作成後にデフォルトの値を変更するには、次のステップに従います。

1. **【ホーム】** → **【検出とインベントリ】** → **【Network Discovery】** をクリックします。

**【Network Discovery ホーム】** ページが表示されます。

2. **【Network Discovery タスクの管理】** Web パーツの**【使用可能なタスク】**タブの下で、スレッド数を変更するタスクを選択します。

**【編集】** ボタン(鉛筆のアイコン) をクリックします。


3. **【検出タスクの編集】** ウィンドウで、**【高度】** をクリックします。
4. **検出タスクごとの最大スレッド数**を変更して **【OK】** をクリックします。

## 警告開始検出

警告開始検出は、Dell Management Console によって管理されていないデバイスの警告またはトラップを介する検出を有効にします。

ネットワーク内の管理対象外のデバイスのトラップ送信先を Dell Management Console システムの IP アドレスで構成します。これらのデバイスがトラップを Dell Management Console システムに非同期に送信する場合、各トラップはトラップを送信するノードを検出する個々の検出プロセスを開始します。

この機能はデフォルトでは無効になっています。

 **メモ:** この機能を有効にする場合は注意してください。管理対象外のデバイスから多くの警告を受信すると、DellManagementConsole が反応しなくなる原因となる場合があります。

## 検出のトラブルシューティング

検出のトラブルシューティングを実行するには、下記のツールの 1 つまたはすべてを使用します。

- 1 Dell トラブルシューティング ツール
- 1 Network Discovery ログ
- 1 Altiris™ Log Viewer
- 1 その他のトラブルシューティング ツール

Dell トラブルシューティング ツールは、Dell Management Console のインストール可能なプログラムで入手できます。このツールを使用して、接続問題の原因を発見することができます。詳細については、次の場所で入手できる「Readme」を参照してください: <DMC DVD>\Tools\Troubleshoot\Readme.txt。

検出に関する問題のトラブルシューティングは、次の場所にある『Dell Management Console - Trouble shooting Guide』を参照してください。 [en.community.dell.com/groups](http://en.community.dell.com/groups)

## Network Discovery ログ

「[検出ログ](#)」を参照してください。

## Altiris Log Viewer

Altiris Log Viewer の表示するには、次のステップに従います。

1. Dell Management Console がインストールされているシステム上 **[スタート]** ボタンをクリックします。
2. **[プログラム]** → **[Altiris]** → **[Diagnostics]** → **[Altiris Log Viewer]** をクリックします。

Altiris Log Viewer が表示されます。

## その他のトラブルシューティング ツール

- 1 IPMI 接続ツール

(例: ipmish.exe, ipmitool.exe)

- 1 SNMP MIB Browser

(例: MG-SOFT MIB Browser)

- 1 ネットワーク プロトコル アナライザ

(例: Wireshark)

---

## 新規組織ビューと組織グループの作成


1. **[管理]** → **[組織ビューと組織グループ]** をクリックします。
2. 左側のウィンドウで、**[新規組織ビュー]** → **[新規]** → **[組織ビュー]** を右クリックします。
3. **[新規組織ビュー]** を右クリックし、**[新規]** → **[組織グループ]** をクリックします。

このグループにデバイスを追加し、グループに対する適切なロールを割り当てることができます。


---

## インベントリの設定の構成

Dell Management Console Inventory Solution ではさまざまなプロトコルを使用して、ネットワーク上のデバイスからインベントリ情報を収集することができます。

 **メモ:** Server Administrator がインストールされている Dell システムは、インベントリ タスクを有効化し、システムに関する具体的な詳細のレポートを返します。

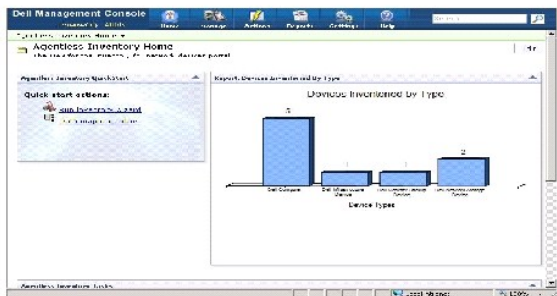
Dell Management Console ではまた、MIB をインポートして受信される SNMP トラップをフォーマットすることもできます。しかし、MIB をインポートし、新しいデバイスにエージェントレス インベントリを拡張するためデータ クラスにマップすることはできません。この機能には、Altiris Inventory Solution from Symantec のライセンスが必要です。

 **メモ:** Dell Management Console のコンテキストにおいてエージェント ベースとは、Altiris™ Agent がターゲット システムにインストールされていることを意味し、エージェントレスとは、Dell Systems Management Agent-Dell OpenManage Server Administrator がターゲット システムにインストールされていることを意味します。

[インベントリ] ポータルにアクセスする方法 **[ホーム]** → **[検出とインベントリ]** → **[エージェントレス インベントリ]** をクリックします。

## インベントリ ユーザー インタフェースの概要





初めてネットワーク デバイスのインベントリ情報の構成と表示を扱う場合は、**[エージェントレス インベントリの Quick Start]**の Web パーツを使用することをお勧めします。

スクリーンの下部にある **[エージェントレス インベントリ タスク]**の Web パーツには、利用可能なインベントリ タスクおよび実行されたタスクが表示されます。

## すべてのシステムのインベントリを収集するためのインベントリ タスクの作成

検出されたシステムのインベントリを収集し、情報をリソースマネージャに表示する方法

1. **[ホーム]** → **[検出とインベントリ]** → **[エージェントレス インベントリ]** をクリックします。

**[エージェントレス インベントリのホーム]** ページが表示されます。

2. **[エージェントレス インベントリの Quick Start]** Web パーツで **[インベントリ ウィザードの実行]** をクリックします。

**[エージェントレス インベントリ タスクの作成]** ページが表示されます。

3. 「ステップ 1: **インベントリするデバイスの選択**」でネットワーク上の Dell PowerEdge™ システムのみのインベントリを収集するには、**[デバイスの選択]** を選択し、「**グループ パッケージを選択する**」ドロップダウンメニューから「**サーバー**」を選択して**[次へ]** をクリックします。
4. 「ステップ 2: **インベントリ ネットワーク タスク名**」で、同種のタスク間で識別しやすいように、一意な名前「Dell Server Inventory Task」を入力して**[次へ]** をクリックします。
5. 「ステップ 3: **スケジュール**」で、このタスクの作成後にスケジュールを実行するように **[今すぐ]** を選択し、**[完了]** をクリックします。

このタスクを後で実行するように日時を指定し、定期タスクに指定することもできます。

エージェントレス インベントリ タスクが作成され、**[エージェントレス インベントリ タスク]** セクションの下の **[エージェントレス インベントリのホーム]** ページに表示されます。

## MIB のインポート

MIB (Management Information Base) を使用してインベントリ機能を拡張することができます。

MIB のインポートを実行する方法

1. Dell Management Console で、**[設定]** → **[すべての設定]** → **[監視と警告]** → **[SNMP MIB インポート ブラウザ]** → **[MIB ブラウザ]** を選択します。
2. 右上のウィンドウで**[MIB ファイルのインポート]** を選択し、必要な **MIB ファイル** を参照し選択して **[適用]** を選択します。
3. MIB ファイルは次のロケーションから入手できます: iso → org → dod → internet → private → enterprises。

## カスタム組織グループ内の選択されたデバイスのインベントリを収集するためのインベントリ タスクの作成

複数の組織グループを作成した後、「[新規組織ビューと組織グループの作成](#)」を参照して Dell|EMC デバイスのみのインベントリを生成できます。

1. **[ホーム]** → **[検出とインベントリ]** → **[エージェントレス インベントリ]** をクリックして **[エージェントレス インベントリのホーム]** ページを表示します。
2. **[エージェントレス インベントリの Quick Start]** Web パーツで **[インベントリ ウィザードの実行]** をクリックします。

**[エージェントレス インベントリ タスクの作成]** ページが表示されます。

3. 「ステップ 1: **インベントリするデバイスの選択**」で、たとえばネットワーク上の Dell|EMC デバイスのみのインベントリを収集するには、**[デバイスの選択]** を選択し、「**グループ パッケージを選択する**」ドロップダウンメニューから「**すべてのデバイス**」を選択します。
4. Dell|EMC デバイス以外のすべてのデバイスをクリアし、**[次へ]** をクリックします。
5. 「ステップ 2: **インベントリ ネットワーク タスク名**」で、同種のタスク間で識別しやすいように、一意な名前「Dell Server Inventory Task」を入力して **[次へ]** をクリックします。
6. 「ステップ 3: **スケジュール**」で、このタスクの作成後にスケジュールを実行するように **[今すぐ]** を選択し、**[完了]** をクリックします。このタスクを後で実行するように日時を指定し、定期タスクに指定することもできます。

## タスクの進行状況と詳細の表示

移行タスクのステータスを表示するには、次のステップに従います。

1. **[ホーム]** → **[検出とインベントリ]** → **[エージェントレス インベントリ]** をクリックして **[エージェントレス インベントリのホーム]** ページを表示します。
2. **[エージェントレス インベントリのタスク]** の Web パーツの下で **[タスクの実行]** タブを選択します。

タスクのステータスと進行状況が表示されます。

3. **[エージェントレス インベントリのタスク]** の Web パーツの下で **[使用可能なタスク]** タブを選択します。

すべての使用可能なインベントリ タスクが表示されます。

4. タスクの詳細を表示するには、タスク インスタンスをダブルクリックします。

タスクの詳細が新規のウィンドウに表示されます。

## インベントリ タスクの結果の表示

1. **[管理]** → **[すべてのデバイス]** をクリックします。
2. 左側のウィンドウで、**[すべてのデバイス]** ツリーを展開し、「**サーバー**」を選択します。

検出されたシステムは、右側のウィンドウにリソース タイプが「**Dell コンピュータ**」として表示されます。

3. インベントリの詳細を表示するシステム名をダブルクリックします。
4. **[リソース マネージャのホーム]** ページで、**[概要]** → **[ハードウェアの概要]** をクリックします。

システムのインベントリ情報が表示されます。ハードウェアの概要を表示するには、ターゲット システムに **Server Administrator** をインストールし、**Dell コンピュータ** としてシステムを分類します。

---

[目次のページに戻る](#)



[目次のページに戻る](#)

## ハードウェア構成タスク

Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [ハードウェア構成タスクについて](#)
- [ハードウェア構成タスクのユーザーインターフェイスの概要](#)

Dell™ Management Console には、ハードウェア構成タスクのセットが用意されており、これを使用してサーバーのハードウェア設定を迅速に構成できます。これらのタスクにより、Dell PowerEdge™ システム上で共通の BIOS 設定および共通の Baseboard Management Controller (BMC) 設定を構成できます。

## ハードウェア構成タスクについて

ハードウェア構成タスクでは、システム BIOS タスクと同様の機能が提供されます。**ハードウェア構成タスクの [高度]** ウィンドウで設定を変更した場合、タスクを正常に実行するには**管理者**パスワードを再入力する必要があります。

高度な設定およびハードウェア構成パラメータに関する詳細は、『Dell Management Console オンライン ヘルプ』を参照してください。

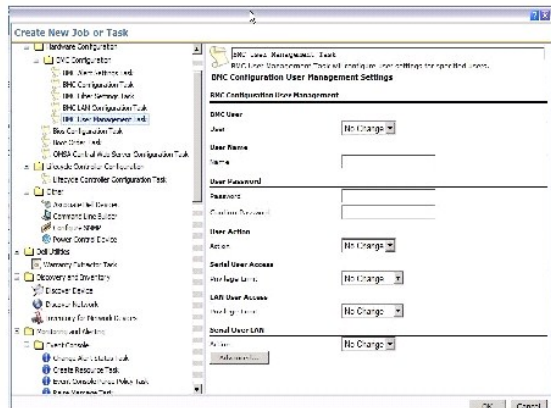
ハードウェア構成タスクを使用して、次の設定を構成できます。

- 1 BIOS 構成タスク: フロントパネル LCD の設定、メモリ冗長性設定、キーボード Numlock の設定、ネットワーク インターフェイス コントローラ (NIC) の設定およびシステムセキュリティの設定を構成できます。
- 1 BMC の構成: このタスクには 5 つのサブタスクがあります。
  - 1 BMC 警告設定タスク: プラットフォーム イベントの警告ポリシーと警告送信先を構成するにはこのタスクを実行します。
  - 1 BMC の構成タスク: LAN チャネル アクセス、シリアル構成パラメータおよびターミナル モード設定などの共通の BMC パラメータを構成するにはこのタスクを実行します。
  - 1 BMC フィルタ設定タスク: プラットフォーム イベント フィルタ (PEF) の設定を構成するにはこのタスクを実行します。温度プローブ エラーなどの指定された PEF イベントに対し、サーバーの電源オフや再起動などの適切なアクションを構成できます。
  - 1 BMC LAN 構成タスク: Dell PowerEdge システム上で LAN およびシリアル オーバー LAN (SOL) のパラメータを構成するにはこのタスクを実行します。
  - 1 BMC ユーザー管理タスク: 指定されたユーザーのユーザー設定を構成するにはこのタスクを実行します。
- 1 ブート順序タスク: 管理対象システムのプライマリ デバイスのブート シーケンスを変更するにはこのタスクを実行します。
- 1 Central Web Service の構成タスク: Central Web Service URL の起動ポイントを、Dell OpenManage™ Server Administrator がインストールされている管理対象システム上に構成するにはこのタスクを実行します。
- 1 ライフサイクル コントローラの構成タスク: ライフサイクル コントローラの設定を構成するにはこのタスクを実行します。
- 1 サーバー タスク (ヘルス モニタ電子メール タスク): 既に選択されているデバイスのヘルス ステータスに関する電子メール警告を送信するにはこのタスクを使用します。
- 1 新規タスクの作成

## ハードウェア構成タスクのユーザーインターフェイスの概要

[ジョブとタスク] ポータル ページにアクセスする方法 **[管理]** → **[ジョブとタスク]** をクリックします。

**[ハードウェア構成]** フォルダは、**[Dell タスク]** フォルダの下に表示されます。



## ハードウェア構成タスクの作成

ハードウェア構成タスクを作成する場合は、「[ジョブとタスク モジュールの使用](#)」を参照してください。

タスクは、[[ジョブおよびタスクのステータス](#)] Webパーツの Dell Management Console ポータル ページから表示できます。タスクの [[出力のプロパティ](#)]を表示するには、タスクをダブルクリックします。

詳細については、[オンライン ヘルプ](#)を参照してください。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

# Dell Management Console のインストール、アンインストール、およびアップグレード

## Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [インストール要件](#)
- [Dell Management Console のアンインストール](#)
- [Dell Management Console の最新バージョンへのアップグレード](#)
- [トラブルシューティング](#)

Dell™ Management Console は、Symantec™ モジュラー アーキテクチャを使用して、ユーザーのニーズに最も適合するソリューションを提供します。Dell Management Console は、Symantec インフラストラクチャ上にビルドされます。その主要テクノロジーは、タスクの完了、ソフトウェア展開、ネットワーク上のデバイスの検出およびインベントリにおいて活用されます。

Symantec Installation Manager (SIM) は DellManagement Console のインストーラです。SIM インストーラは管理ステーション上に SIM をインストールします。SIM では Dell Management Console をインストール オプションとして提供しています。

---


## インストール要件

推奨されるハードウェア構成については、「[推奨される最小のハードウェア構成](#)」を参照してください。

Dell Management Console をインストールする管理ステーションは、次のソフトウェア必須条件を含める必要があります。

## Symantec Installation Manager の必須条件

Dell Management Console をインストールする前に、管理ステーションに Microsoft® .NET Framework 3.5 (*Dell Management Console* DVD に収録) をインストールする必要があります。

 **メモ:** この必須条件が管理ステーションにインストールされていない場合、SIMインストーラ(DellManagement Console DVD に収録) は、この必須条件をインストールしてから Dell Management Console をインストールします。

## インストール適合性のための必須条件

- 1 Microsoft Windows Server® 2003 32 ビット版 (Enterprise または Standard)
- 1 Microsoft ASP .NET Framework
- 1 500 台までの管理システム: SQL Express 2005 Express
  
- 500 台以上の管理対象システム: Microsoft SQL Express 2008、SQL Server 2005 または SQL Server 2008 (64 ビット リモートのみ)
- 1 8 GB 以上のディスク空き容量 (10 GB のディスク空き領域を推奨)
- 1 Internet Information Services 6.0
- 1 Microsoft Internet Explorer® バージョン 7.0 または 8.0

インストールの必須条件に関する詳細は、『*Dell Management Console Version 1.1 のサポート情報マトリックス*』を参照してください。

## 注意事項

- 1 管理ステーションを Windows DomainController として構成しないでください。
- 1 ターミナルサービスを使用して Dell Management Console をインストールする場合は、コンソール セッションを使用してインストールしてください (例:mstsc/console)。
- 1 管理ステーションで、HTTPS(HyperText Transfer Protocol over Secure Socket Layer) をインストール、構成、有効にすることを強くお勧めします。

- 1 このリリースの Dell Management Console にアップグレードする場合は、SIM を使用してください。最新のアップデートを取得するには、SIM がインターネットに接続されている必要があります。SIM を起動すると、すべての重要なアップデートがリストされ、推奨されるアップデートは **【アップデート】** セクションにリストされます。Dell Management Console を選択してください。

## Dell Management Console のインストール

Dell Management Console とほかのユーティリティは、*Dell Management Console DVD* からインストールするか、Dell Web サイト [dell.com/openmanage](http://dell.com/openmanage) からダウンロードしてインストールできます。インストーラから Dell Management Console の依存関係をインストールすることもできます。

1. *Dell Management Console DVD* を DVD ドライブに挿入します。インストール プログラムが自動的に起動しない場合は、DVD のルート フォルダに移動し、**setup.exe** をダブルクリックします。

**[Dell Management Console]** ダイアログ ボックスが表示されます。

2. ようこそ画面で、**[Dell Management Console のインストール]** を選択します。


ポート数を増やすためマシンを再起動させることを促すメッセージが表示されます。**[はい]** を選択します。

システムが再起動したらインストーラを実行します。インストーラは、Microsoft .NET Framework がシステムに存在するかどうかをスキャンします。.NET が存在しない場合、.NET Framework のインストールを求められます。

依存関係がすべて存在する場合は、**[Symantec Installation Manager セットアップ]** ダイアログ ボックスが表示されます。

3. **[次へ]** をクリックします。
4. エンド ユーザー使用許諾契約書に同意して、**[次へ]** をクリックします。
5. **[送信先フォルダ]** ダイアログ ボックスで、Dell Management Console をインストールするフォルダを参照し、**[インストールの開始]** をクリックします。
6. インストールが完了したら、「**Symantec Installation Manager を自動的にインストールする**」を選択して **[完了]** をクリックします。

Symantec Installation Manager が自動的に起動されます。

 **メモ:** ホット フィックス、パッチ、付加価値プラグイン ソリューションの試用版をダウンロードするには、インターネット アクセスが必要です。


7. **[Symantec Installation Manager]** メイン ダイアログ ボックスで、**[新製品のインストール]** を選択します。
8. **[新製品のインストール]** ダイアログ ボックスで、**[Dell Management Console]** を選択し、**[次へ]** をクリックします。

様々なフィルタを選択し **[利用可能なすべてのバージョンを表示する]** を選択し、ほかのコンポーネントを表示してインストールすることができます。

9. **[オプションのインストール]** ダイアログ ボックスでインストールしたい利用可能な機能を選択して **[次へ]** をクリックします。
10. エンド ユーザー使用許諾契約書に同意して、**[次へ]** をクリックします。

**[インストール適合性チェック]** ダイアログ ボックスに依存関係と推奨事項が表示されます。

11. 存在しない依存関係がある場合は、この要件をインストールします。


 **メモ:** .Net 証明書および SQL Maximum Memory 構成のインストール適合性を確認します。

**[インストール適合性の再チェック]** をクリックし、**[次へ]** をクリックします。

12. **[Dell Management Console の構成]** ダイアログ ボックスで、ローカルの管理者資格情報を入力します。

電子メール情報を構成済みの場合は、テスト電子メールを送信して構成を確認できます。

13. **[次へ]** をクリックします。
14. **[データベースの構成]** ダイアログ ボックスで、Symantec Management Console で使用する Microsoft SQL Server の詳細を入力し、**[次へ]** をクリックします。

 **メモ:** SQL Server 2005 で DellOpenManage ITAssistant を使用していた場合は、管理対象デバイスの数によっては、同じデータベースを DellManagementConsole で使用できます。詳細については「[推奨される最小のハードウェア構成](#)」を参照してください。

15. **【インストールの詳細の確認】** ダイアログ ボックスで **【インストールの開始】** をクリックします。

Dell Management Console がインストールされます。

**【製品ライセンス】** ダイアログ ボックスが表示されます。

16. **【製品ライセンス】** ダイアログ ボックスで、**【次へ】** をクリックします。

**【インストール完了】** ダイアログ ボックスが表示されます。

17. **【インストール完了】** ダイアログ ボックスで、**【完了】** をクリックします。

Dell Management Console DVD を使用して、その他の Dell ユーティリティをインストールできます。

Dell Management Console を Dell Client Manager にインストールする方法については、『[Symantec Management Platform インストール ガイド](#)』を参照してください。

## インストール後の注意事項

1. Dell Management Console をインストールした後、オペレーティングシステムや Symantec Management Console のパスワードを変更する場合は、必ずオペレーティングシステムのパスワードを変更する前に Symantec Management Console のパスワードを変更します。

ただし、Notification Server パスワードを変更する前にオペレーティング システム パスワードを変更した場合は、次のコマンドを使用して Notification Server パスワードを変更します。

```
aexconfig /svcid user:<ユーザー名 (ドメイン、コンピュータ\ユーザー)> password:<パスワード>
```

 **メモ:** aexconfig コマンドは、Altiris/Notification server/bin フォルダで入手できます。

1. Dell Management Console をインストールした後、システムホスト名を変更して DellManagementConsole を起動した場合はサーバー例外が表示されます。

この問題のトラブルシューティングの詳細については、『[Dell Management Console オンライン ヘルプ](#)』の **Symantec Management Server のエラー**に関するセクションを参照してください。

---

## Dell Management Console のアンインストール

Dell Management Console をアンインストールするには、次の操作を行います。

1. **【プログラムの追加と削除】** に進み、Symantec プラットフォームおよびソリューション ウィザードを実行します。
2. **【Symantec プラットフォームおよびソリューション】** コンポーネントを選択し、**【アンインストール】** をクリックします。

Dell Management Console がアンインストールされます。

Dell Management Console DVD から Dell Management Console をアンインストールすることもできます。

1. *Dell Management Console* DVD を挿入します。
2. **【Dell Management Console】** ダイアログ ボックスで、**【Dell ManagementConsole のインストール】** を選択します。
3. **【製品のインストール】** ダイアログ ボックスが表示されるまで、インストールウィザードを続行します。
4. **【Dell Management Console】** オプションを選択し、**【アンインストール】** をクリックします。



Dell Management Console がアンインストールされます。

 **メモ:** Dell Management Console をアンインストールしても、DellManagement Console データベースはアンインストールされません。

---

## Dell Management Console の最新バージョンへのアップグレード

Dell Management Console DVD を使用して、前のバージョンの Dell Management Console からアップグレードすることができます。

[このリリースの Dell Management Console にアップグレードする場合は、SIM を使用してください。最新のアップデートを取得するには、SIM がインターネットに接続されている必要があります。SIM を起動すると、すべての重要なアップデートがリストされ、推奨されるアップデートは「アップデート」セクションにリストされます。Dell Management Console を選択してください。](#)

 **メモ:** Dell Management Console のアップグレード中、Dell Management Console の構成およびデータベースの構成のスクリーンは表示されません。

SIM の起動後、重大なアップデートをインストールするように指示される場合があります。Dell Management Console のアップグレードを続行する前に、すべてのアップデートをインストールすることをお勧めします。

Dell Management Console 1.1 は、Symantec Management Platform (SMP) SP3 に基づいています。そのため、最新バージョンの Server Management Suite および Dell Client Manager を Dell Management Console Version 1.1 DVD からインストールする前 (またはインストール中) に Dell Management Console 1.1 にアップグレードすることをお勧めします。

---

## トラブルシューティング

トラブルシューティングについては、オンライン ヘルプを参照してください。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## はじめに


### Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [このリリースの新しい機能](#)
- [Dell Management Console のクイックガイド](#)
- [必要になる可能性があるその他のマニュアル](#)

Dell™ Management Console は、一対多数システム管理アプリケーションで、拡張された検出機能、インベントリ機能、監視機能、パッチ アップデート機能、レポート機能を提供します。

Dell Management Console は、基本的なハードウェア管理用のスケーラブルなモジュラー コンソールに加え、資産、セキュリティ、整合性などの高度な機能も提供する Web ベースのグラフィック ユーザー インターフェイス (GUI) です。Dell Management Console をネットワーク環境の管理ステーションにインストールできます。

Dell Management Console は、Dell サポート Web サイト (support.dell.com) からインストールできる無料のソフトウェアですが、Dell Web サイト ([dell.com/openmanage/register](http://dell.com/openmanage/register)) で登録して無料の恒久ライセンスを取得する必要があります。登録すると、30日の試用期限が切れた後も Dell Management Console を引き続き使用できます。Dell Management Console は、Symantec Server Management Suite など、さまざまな Symantec™ プラグインもサポートします。

 **メモ:** Symantec Inc. が Altiris Inc. を買収したため、このドキュメントでは Altiris™ と Symantec への参照が含まれています。

## このリリースの新しい機能

このリリースでは次の機能を利用できます。

- 1 電源監視: デバイスの標準的なセットの電力消費量を監視できます。
- 1 ライフサイクル コントローラ有効パッチ: Lifecycle Controller Version 1.3 および Integrated Dell Remote Access Controller (iDRAC) version 6 が搭載されたサーバーのパッチ アップデートを実行できます。
- 1 ヘルス モニタ電子メール タスク: 事前に選択したデバイスのヘルスのステータスに関する警告を特定のユーザーに電子メールで送信するように、Dell Management Console を構成できます。
- 1 Dell EqualLogic デバイスのインベントリ情報を収集できます。詳細は、support.dell.com/manuals で『Dell EqualLogic マニュアル』を参照してください。

以前リリースされた Dell Management Console からこのリリースにアップグレードするには、『Dell Management Console Version 1.1 のサポート情報マトリックス』を参照してください。

## Dell Management Console のクイック ガイド

Dell Management Console のインストールとセットアップのプロセス

1. Dell Management Console のインストールの計画: 次の要件に基づいてインストールを計画します。
  - 1 ネットワーク サイズ
    - 1 管理するネットワーク デバイス、およびネットワーク デバイスとの通信に必要なプロトコル (Simple Network Management Protocol (SNMP)、Windows® Management Interface (WMI)、Web Services for Management (WS-MAN)、または Intelligent Platform Management Interface (IPMI) プロトコルなど)。デバイスおよび必要なプロトコルに関する詳細は、[表5-1](#)を参照してください。
    - 1 監視する属性。たとえば、デバイスのヘルスのみを管理、あるいはヘルスとパフォーマンスを管理できます。
    - 1 複数のサイトへの階層化ソフトウェア展開。詳細については、[\[ヘルプ\] → \[マニュアル ライブラリ\]](#)、または [\[ヘルプ\] → \[コンテキスト\]](#) で Symantec のマニュアルを参照してください。

詳細については、『[Dell Management Console のインストールの計画](#)』を参照してください。

2. Dell Management Console のインストール: Dell Management Console は Dell Management Console DVD または Dell Web サイト ([dell.com/openmanage](http://dell.com/openmanage)) から入手できます。Dell Management Console のインストールの詳細については、『[Dell Management Console のインストール、アンインストール、およびアップグレード](#)』を参照してください。
3. Dell Management Console の構成の準備: Dell Management Console の構成、およびネットワーク デバイスを計画することは最も重要です。次の詳細の構成を計画します。
  - 1 検出タスク。たとえば、『含める範囲』と『除外する範囲』(IP アドレス、サブネット、ホスト名、およびカスタム範囲など) を定義します。

- 1 ネットワーク上のデバイスの種類 (Dell および Dell 以外)
  - 1 デバイスのセキュリティ
  - 1 接続プロファイルと資格情報。詳細については、「[接続プロファイルと資格情報の管理](#)」を参照してください。
4. Dell Management Console を次の順序で構成します。
- e. 検出タスク: 検出するネットワーク デバイスのグループを定義します。
  - f. エージェントの展開: Altiris Agent を展開し、Dell OpenManage™ Agent と Dell OpenManage Server Administrator (OMSA) をターゲット サーバーに展開します。
  - g. インベントリ: メモリ、プロセッサ、電源、組み込みデバイス、ソフトウェアおよびファームウェアのバージョンのインベントリ情報を収集します。詳細については、「[インベントリの設定の構成](#)」を参照してください。
  - h. ネットワーク デバイスの編成: 組織または地理的な場所に基づいてネットワーク デバイスを編成できます。
  - i. ステータス ポーリングの設定: 検出されたすべてのデバイスの電源および接続のヘルス チェックを実行します。この機能は、デバイスが正常に動作している、異常な状態である、または電源が OFF になっているのいずれかを判定します。詳細については、「[監視と警告](#)」を参照してください。
  - j. イベント管理および警告: プロトコルを構成します。
  - k. Management Information Base (MIB): Dell 以外のデバイスがネットワークにある場合は、これらのデバイスから受信したトラップを認識するための適切な MIB をインポートします。詳細については、「[MIB のインポート](#)」を参照してください。
  - l. パフォーマンスとヘルス モニタリング: ネットワークのリアルタイム ヘルスおよびパフォーマンスを監視します。
  - m. パッチ管理: Altiris Agent または LC 有効パッチ アップデートを使用して 1 つのシステムまたはシステムのグループに一度にアップデートを展開します。
  - n. タスク: システムのグループを構成します。
  - o. レポート: レポート結果を Dell Management Console で表示する方法を選択し、レポートのデフォルトのビューを設定します。

## Dell Management Console のインストールの計画

このセクションでは、Dell Management Console のインストールを計画する際に生じる可能性のある疑問点について回答しています。

### Dell Management Console をインストールするための基本的なハードウェア要件は何ですか？

特定の Dell Management Console の展開およびネットワーク環境によっては、プロセッサ速度、メモリの容量、およびハードウェアの空き容量についての推奨より上の構成にすることが適切な場合があります。

### 推奨される最小のハードウェア構成

- 1 Microsoft® Windows Server® 2003 R2 SP2 (32 ビット版) (Standard Edition または Enterprise Edition)
- 1 物理プロセッサ: 2
- 1 RAM: 4 GB
- 1 DVD ドライブ
- 1 Microsoft .NET Framework Version 3.5 または 3.5 SP1
- 1 Windows Internet Information Services Version 6.0
- 1 Microsoft SQL Express 2005 または SQL Express 2008、SQL Server 2005 または SQL Server 2008 (64 ビット リモート)
- 1 (推奨) 大規模環境の場合は、リモート データベース、および 8GB 以上の利用可能なメモリ

詳細については、「[DellTechCenter.com](#)」を参照してください。

Dell OpenManage IT Assistant 用に Microsoft SQL Server 2005 を既にインストールしています。Dell Management Console に移行してこのデータベースを動作させたいのですが、他のデータベースをインストールすべきでしょうか？

一般に、管理するシステムの数、および管理対象システムから受け取る警告の数に応じて、Dell Management Console で使用するデータベースが決まります。500 台以下のデバイスを管理する場合は、SQL Express 2005 または SQL Server 2005 (32 ビット版) のいずれかを使用できます。

インストールまたは有効にする必要があるシステム管理プロトコルは何ですか？

一般に、監視するシステムで規定されているプロトコル、およびシステムでサポートされている各エージェントプロトコルを選択します。監視するシステムに SNMP (Simple Network Management Protocol)、WMI (Windows® Management Interface)、WS-MAN (Web Services for Management) または IPMI (Intelligent Platform Management Interface) プロトコルを使用するエージェントがある場合は、これらのプロトコルを DellManagement Console で構成します。

Dell Management Console では、**接続プロファイル**を構成して、必要な数のプロトコルを含めることができます。Dell ManagementConsoleは、**接続プロファイル**で定義したプロトコルを使用してネットワーク上のデバイスに接続します。

**サブネット上で複数のシステム管理プロトコルを使用している場合は、管理対象システムの IPアドレスをどのように構成すればよいですか？**

可能な場合は、同じシステム管理プロトコルを使用しているシステムを隣接するサブネット内にまとめて構成します。この方法を使用すると、Dell Management Console の検出範囲を作成する際に管理が容易になります。

**監視ネットワークのパフォーマンスは、監視対象の属性によって決まりますか？**

はい。監視するデバイスの属性によって必要なリソースが決まります。たとえば、システムのヘルスのみを監視する場合は、推奨される最小のハードウェア構成で十分です。しかし、構成は監視するシステムの数に依存します。

システムのヘルスとパフォーマンスを監視するには、推奨より上の構成をお勧めします。「[推奨される最小のハードウェア構成](#)」を参照してください。

**世界各地に、複数の階層を持つネットワークを保有し、そこで管理システムを使用しています。これは、Dell Management Console のインストール方法にどのような影響を与えますか？**

世界の各地に管理ステーションがある場合は、DellManagement Console のインストール方法に影響及ぼします。詳細については、階層化インフラストラクチャに関する Symantec のマニュアルを参照してください。Symantec のマニュアルは、[\[ヘルプ\]](#) → [\[マニュアル ライブラリ\]](#) で参照できます。

## Dell Management Console の構成の計画

Dell Management Console をインストールした後、このアプリケーションの構成を計画する必要があります。

**ネットワークに Dell および Dell 以外のデバイスがあります。これらのデバイスを個別に構成する必要がありますか？**

はい、監視するすべての Dell 以外のデバイスに適した MIBをインポートする必要があります。Dell 以外のデバイス用の MIB をインポートすると、これらのデバイスの SNMP警告を受け取ることができます。

**Dell ManagementConsole を使用するために構成するセキュリティ オプションは何ですか？**

[\[ヘルプ\]](#) → [\[マニュアル ライブラリ\]](#) で、ロールベースのセキュリティに関する Symantec のマニュアルを参照してください。

**Dell OpenManage IT Assistant からの移行を行います。検出範囲を Dell ManagementConsole に移行する方法を教えてください。**

検出設定を IT Assistantから移行する方法については、「[IT Assistant 検出設定のインポート](#)」を参照してください。

**使用する機能に必要な特殊な構成はありますか？**

要件に合わせて任意のまたはすべての機能を構成できます。各機能が正しく機能するように管理対象のデバイスに展開する必要があるエージェントについては、「[表 1-1](#)」を参照してください。

**表 1-1. エージェントでサポートされている機能**

機能	エージェントなし	Dell OpenManage Server Administrator	Altiris Agent
検出	IPMI、WMI、または SNMP を使用して検出	リソース マネージャの詳細なハードウェア概要が必要	不要
インベントリ	IPMI、WMI、または SNMP を使用した基本インベントリ	リソース マネージャの詳細なハードウェア概要が必要	不要
ヘルスの監視	IPMI* を使用した Out-of-Band ヘルス モニタリング	エージェント ベースが必要 SNMP を介したヘルス モニタリング	不要
イベントと警告	基本的な IPMI プラットフォーム イベントトラップ (PET) のみ	包括的なハードウェア イベントに必要	不要
ハードウェア構成タスク	NA	必須	不要
DellAgent (Server Administrator) の展開	NA	NA	必須
アップデート (ファームウェア/ドライバ/BIOS) 管理	NA	NA	必須
オペレーティング システム パフォーマンスの監視	WMI/IPMI* 経由でエージェントレスで Windows を監視	IPMI* が有効になっていない、または利用できない場合に必要	Linux 上で実行しているシステムに必要

\* IPMI は、Dell PowerEdge™ x8xx 以降のサーバーで利用できます。

DellManagement Console で管理対象デバイスを管理するように管理対象デバイスを有効にするにはどうすればよいですか？

SNMP および WMI プロトコルを使用している Dell PowerEdge™ システムの場合、管理を最も簡単にできるようにするには、DellOpenManage™ Server Administratorを管理対象システムにインストールする必要があります。

Dell Management Console でプロトコルと資格情報が正しく設定されている場合は、サーバー以外のその他のデバイスを管理できます。たとえば、ネットワークプリンタを管理する場合は、SNMP が有効化され、Dell Management Console の接続プロファイルの設定でコミュニティ文字列が定義されている必要があります。詳細については、「[接続プロファイルと資格情報の管理](#)」を参照してください。

## 必要になる可能性があるその他のマニュアル

次のマニュアルにアクセスして参照できます。

- Symantec のマニュアルは、[\[ヘルプ\]](#) → [\[マニュアル ライブラリ\]](#) で参照できます。
  - Symantec のマニュアルには Notification Server 7.0 のマニュアルが含まれています。
- オンライン ヘルプは、[\[ヘルプ\]](#) → [\[コンテキスト\]](#) で参照できます。
- 詳細については、Dell サポート Web サイト [support.dell.com/manuals](http://support.dell.com/manuals) で、『Dell Management Console のサポート情報マトリックス』を参照してください。
- このマニュアルで使用されている用語に関する情報は、Dell サポート Web サイトの「用語集」を参照してください。
- Dell EqualLogic の詳細は、Dell サポート Web サイト ([support.dell.com/manuals](http://support.dell.com/manuals)) で『Dell EqualLogic マニュアル』を参照してください。
- その他のマニュアルは、Dell Tech Center ([delltechcenter.com/page/Dell+Management+Console](http://delltechcenter.com/page/Dell+Management+Console)) および ([en.community.dell.com/groups/](http://en.community.dell.com/groups/)) で利用できません。
- Navisphere CLI の最新ソフトウェアとユーザー マニュアルは、[powerlink.emc.com](http://powerlink.emc.com) を参照してください。

[目次のページに戻る](#)


[目次のページに戻る](#)

## 監視と警告

### Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [監視について](#)
- [監視と警告モジュールのユーザー インターフェイス](#)
- [依存関係](#)
- [Monitoring and Alerting Solution のライセンスの制限](#)
- [パフォーマンス モニタ](#)
- [監視ポリシーの有効化](#)
- [メトリックスの変更](#)
- [パフォーマンス ビューア](#)
- [ヘルス モニタリング](#)
- [OnDemand モニタリング](#)
- [クライアント アップデート自動化ポリシー](#)
- [異なるしきい値を持つ各種デバイスを監視するためのポリシーの複製](#)
- [サーバー監視警告の管理](#)

Dell™ Management Console は、ネットワーク上の管理対象デバイスと通信を行い、ヘルスおよびパフォーマンス データを収集します。監視と警告モジュールは、システムのリアルタイムのヘルス、パフォーマンスおよび電力消費量を監視するための主要インターフェイスです。この機能は、SNMP (Simple Network Management Protocol)、CIM (Common Information Model)、および IPMI (Intelligent Platform Management Interface)などのさまざまなプロトコルを使用して、管理対象デバイスと通信を行います。

 **メモ:** Dell Management Console で監視と警告を構成する場合、新しい構成がアクティブになるまで追跡を開始できません。


#### Dell™ OpenManage™ Storage Management の関連メモ

- 1 サーバーに接続されたストレージのアームウェアが古い場合、Dell Management Console のストレージ コントローラ コンポーネントのステータスで [警告] ステータスが表示されます。ストレージ コントローラ コンポーネントのステータスの詳細は「OpenManage Server Administrator」を参照してください。
- 1 ストレージ コントローラ コンポーネントで仮想ディスクが削除たか物理ディスクが削除された場合、Monitor Agent が再起動されたときやデバイス セッションが更新されたときのみ Dell Management Console で変更が反映されます。(デフォルトでは、デバイス セッションは 1 時間に 1 回更新されます。)
- 1 MIB (Management Information Base) はコンポーネントとロールアップ ステータスをサポートします。コンポーネントのステータスは、子要素のロールアップ ステータスに依存しない要素のステータスです。ロールアップ ステータスは要素とその子にとって最悪のケースのステータスです。OpenManage Storage Management と Dell Management Console には異なるインターフェイスと、これらのステータスを表示するための必須条件があります。
  - 1 OpenManage Storage Management のユーザー インターフェイスにはロールアップ ステータスのみが表示されます。これは、考えられる問題を判断するために完全な階層をドリルダウンすることなく、非正常な状態を判断するために特に必要です。
  - 1 Dell Management Console にはコンポーネント ステータスが表示されます。Dell Management Console ではフラット ビューでデバイスを監視します。ここではすべての非正常な状態のコンポーネントを一度に表示できます。コンポーネントが故障していると推測される恐れがあるため、要素のコンポーネント ステータスを上げることは極力避けてください。ステータスの変化はロールアップ ステータスが原因の可能性があります。そのため、Dell Management Console と OpenManage Server Administrator ユーザー インターフェイスのストレージ ドリルダウン ステータスはいつも一致するとは限りません。
- 1 異なる OpenManage バージョンでサポートされているカウンタの違いによるエラーを避けるため、ハードウェアでサポートされる最新の OpenManage バージョンを使用してください。
- 1 すべてのインスタンスにおいて、単一カウンタは単一の警告を共有し、別のインスタンスが非正常の状態になったときに新しい警告を生成しません。たとえば、温度プローブが 4 つありその内の 1 つが [警告] の状態にあるため警告を受信したとします。ほかの温度プローブが [警告] の状態になったとしても新しい警告は生成されません。
- 1 プローブ インスタンスの命名は、OpenManage Server Administrator ユーザー インターフェイスと Dell Management Console ユーザー インターフェイスとは異なる可能性があります。

## 監視について

Monitor Solution を使用すると、監視ポリシーで定義されているエージェントベースまたはエージェントレスのインターフェイスを通じて、検出されたデバイスをリアルタイムで監視できます。

 **メモ:** Dell Management Console のコンテキストでは、エージェントベースとは、Altiris™ Agent がターゲット システムにインストールされていることを意味し、エージェントレスとは、Dell のシステム管理エージェントである Dell OpenManage™ Server Administrator がターゲット システムにインストールされていることを意味します。

 **メモ:** Symantec Inc. は Altiris® Inc. を買収しました。このドキュメントでは、Altiris と Symantec への参照が混用されていることがあります。

ポリシーは、ルールのセット、およびこれらのルールを実行するターゲット グループを定義します。ルールは、監視するデータと警告を発する条件、または処置を取る条件を定義します。メトリックスは、監視するデータ、およびデータを取得するポーリング間隔を定義します。Dell ポリシーでは、メトリックス、ルールおよびポリシーを定義して、Dell ハードウェアのヘルスおよびパフォーマンスを監視できるようにします。

**メモ:** 詳細については、Monitor Solution™ に関する Symantec™ のユーザー ガイドを参照してください。

表 9-1. Dell ポリシーの説明

Dell ポリシー	説明	エージェントベース/エージェントレス	サポート範囲	デフォルトの動作	デフォルトのポーリング間隔
デバイスのプライマリヘルス	プライマリ デバイスヘルスを監視します (Dell OpenManage™ Server Administrator が Dell Server のこの情報を提供します。他のすべてのデバイスについては、埋め込みエージェントがこの情報を提供します)。	エージェントレス	すべての Dell デバイス	有効	1 時間
デバイス エージェントヘルス - Dell Remote Access Controller インバンド-	Dell Remote Access Controller (DRAC) インバンドのヘルスを監視します。	エージェントレス	DRAC を装備した Dell Server	有効	1 時間
デバイス エージェントヘルス - Dell OpenManage Storage Management	Dell OpenManage Storage Management のヘルスを監視します。	エージェントレス	Storage Management がインストールされている Dell Server	有効	1 時間
デバイスの接続状態	デバイスの接続状態を監視します。	エージェントレス	すべての Dell デバイス	有効	1 時間
Microsoft® Windows® のパフォーマンスの監視	Windows パフォーマンス カウンタを監視します。	エージェントレス	サポートされている Windows オペレーティング システムがインストールされている Dell Server	無効	2 分
Linux のパフォーマンス監視	Linux パフォーマンス カウンタを監視します。	エージェントベース	サポートされている Linux オペレーティング システムがインストールされている Dell Server	無効	2 分
電源監視	Dell Server の監視	エージェントレス	Dell OpenManage™ Server Administrator がインストールされている Dell Server	無効	1 時間

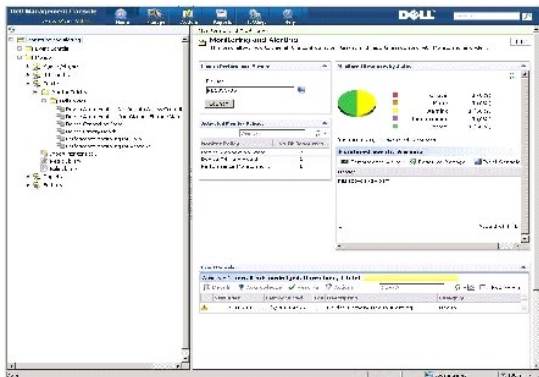
**メモ:** デフォルトでは、すべてのヘルス ポリシーは有効になっていますが、パフォーマンスおよび電源ポリシーはユーザーが有効にする必要があります。履歴およびリアルタイムビューでは、有効になっているポリシーのみが表示されます。

**メモ:** 監視のポーリング時間は、メトリックス ベースで定義されます。ただし、ポリシーのすべてのメトリックスのデフォルト ポーリング時間は同じです。

## 監視と警告モジュールのユーザー インターフェイス

[ホーム] → [監視と警告] をクリックして、監視と警告モジュールにアクセスします。

### 監視と警告モジュールのユーザー インターフェイスの概要



左側のウィンドウに、[監視と警告] ツリーが表示されます。このツリーから、[メトリック ライブラリ]、[ルール ライブラリ]、[レポート]、および [設定] ポリシーにアクセスできます。

右側のウィンドウに、ユーザー インターフェイスの Web パーツが表示されます。このウィンドウでは、次のタスクを行うことができます。

- 1 パフォーマンス ビューアの起動。
- 1 アクティブ化されているポリシーの表示。
- 1 ステータス別のリソースの監視。
- 1 Event Console の表示。受信した最新の警告が表示されます。

## 依存関係

Monitoring and Alerting Solution は、さまざまな要因に依存しています。[表9-2](#) では、これらの要因を詳細に説明しています。

表 9-2. Monitoring Solution の依存関係

依存関係	説明
Device Agent	ヘルスマニタリングでは、プロトコル経由でデータを提供するために監視対象デバイスにエージェントが必要です。たとえば、Dell Server では、サーバーを監視してそのプライマリヘルスステータスを取得するには Server Administrator がインストールされている必要があります。同様に、プリンタのヘルスを監視するには、プリンタに SNMP をサポートする埋め込みエージェントが必要です。
プロトコルのサポート	Dell モニタ メトリクスは、 <i>Smart Metrics</i> (スマート メトリクス) であり、プロトコル依存関係があります。このメトリクスは、プロトコルまたはインターフェイスである。SNMP、WMI、WS-MAN、IPMI、NaviCli、Symbol、および Linux コマンドのうちの1つまたは複数からのサポートを必要とします。「 <a href="#">接続プロファイルと資格情報の管理</a> 」を参照してください。
Discovery Solution	監視するデバイスは、検出され、Dell デバイスとして分類されている必要があります。Discovery Solution は、エージェントバージョンおよび製造元のデータを収集します。このデータはリソース マネージャビューでエージェントヘルスを表示するときに使用されます。  <b>メモ:</b> デバイスは、検出で使用されたプロトコルのみによって監視できます。  <b>メモ:</b> デバイスを監視するには、デバイスが Dell デバイスとして分類されている必要があります (例: Dell コンピュータ、Dell プリンタ)。
Event Solution	Event Console には、Dell Management Console で受け取ったすべての SNMP トラップと監視の警告が表示されます。[ステータス、グループ別の管理対象リソース ビュー] および [リソース マネージャヘルス ビュー] などのさまざまな Web パーツでは、監視警告を使用してデバイスのヘルスを測定します。さらに、SNMP トラップは、「 <a href="#">OnDemand モニタリング</a> 」機能も推進します。
Reporting Solution	Reporting Solution は、Dell モニタベース レポートを提供します。
Dell Management Console のホーム ページ	このホーム ページには、デバイスヘルスステータスを表示する主要インターフェイスであるグループヘルスビューがあります。
Dell ライセンス	Dell ライセンスはデフォルトのライセンスであり、Dell デバイスを監視するために必要です。Dell ライセンスでは、既存のポリシーを制限付きでカスタマイズすることもできます。ただし、新しいポリシーを作成することはできません。
無制限ライセンス	無制限ライセンスはフルライセンスです。このライセンスでは、既存の監視ポリシーの完全な変更、およびユーザー定義ポリシーの作成を行うことができます。このプラグインは、Symantecから購入できます。
Altiris Agent for Linux	Linux パフォーマンスの監視に必要です。
Linux Monitor Agent	Linux パフォーマンスの監視に必要です。

## Monitoring and Alerting Solution のライセンスの制限

Dell Management Console には、Monitoring and Alerting Solution で使用できる機能に影響を及ぼす制限付きライセンスがあります。このライセンスを使用すると、Dell デバイスのみでポリシーを実行したり、ポリシーの限られた部分を変更したりできます。

ただし、無制限ライセンスや追加の監視パックを購入すると、Dell ポリシーで設定されているすべての機能を利用できます。

### 制限付き Dell ライセンス

このライセンスで実行できないタスク:

- 1 メトリクスの作成。
- 1 ルールの作成。
- 1 メトリクスの複製。
- 1 次の例外を除く、メトリクスまたはルールの変更。

メトリクスで実行できる操作:



- 1 メトリック ポーリング間隔の変更。
- 1 メトリック タイムアウトの変更。
- 1 メトリックスの有効化あるいは無効化。

ルールで実行できるタスク:

- 1 ルールの条件の変更。
- 1 ルール値のタイプの変更。
- 1 ルール値の変更。
- 1 ルールの繰り返し回数の変更。
- 1 ルールのオーバータイム値の変更。
- 1 ルールの状態属性の変更。
- 1 ルールのアクション属性の変更。
- 1 ルール、バック、およびカテゴリの有効化または無効化。
- 1 ルールの複製。

ポリシーで実行できるタスク:

- 1 ポリシー ターゲットの変更。
- 1 ポリシーからのルールの追加または削除。
- 1 ポリシーの複製。

## パフォーマンス モニタ

パフォーマンス モニタリングを使用すると、Microsoft Windows および Linuxオペレーティング システムでサポートされている標準的なセットのパフォーマンス カウンタを監視できます。

### パフォーマンス モニタリングの依存関係

表 9-3. パフォーマンス モニタリングの依存関係

Dell ポリシー	エージェント/ エージェント レス	サポート範囲	デフォルト の動作	依存関係
Windows のパフォーマンス監視	エージェント レス	サポートされている Windows オペレーティング システムがインストールされている Dell Server	無効	WMI プロトコル、Windows2003 以降
Linux のパフォーマンス監視	Altiris Agent	サポートされている Linux オペレーティング システムがインストールされている Dell Server	無効	glibc 2.2 以降、systat、LinuxAgent および MonitorAgent  <b>メモ:</b> Monitor Solution の詳細は、Symantec のユーザーズ ガイドを参照してください。

### Linux パフォーマンス モニタリング用の Systat のインストール

次のコマンドを入力して、このライブラリの rpm が Linux Server に既に存在しているかどうかを確認します。

```
rpm -qa | grep systat
```

rpm が存在する場合は、次のコマンドを実行してライブラリをインストールします。


rpm -i <パッケージ名>

Linux Server にライブラリまたは rpm が存在しない場合、次のサイトからダウンロードします。

pagesperso-orange.fr/sebastien.godard/

Linux オペレーティング システム メディアにも rpm が収録されています。

rpm を Linux Server にダウンロードし、前述の手順に従ってインストールします。

 **メモ:** sysstat ソースをコンパイルしないことを強くお勧めします。

## パフォーマンスのメトリクス

パフォーマンス メトリクスは、Windows および Linux オペレーティング システムと同じタイプのカウンタに基づいています。

表 9-4. パフォーマンスのメトリクス

メトリック (合計数 = 単一 + 複 合)	説明
<b>CPU</b>	
使用率、 カーネル 使用時間	プロセスのスレッドが特権モードでコードを実行するときに費した経過時間の割合をパーセントで表示します。Windowsのシステムサービスは、呼び出されると、システム専用データへアクセスするためにしばしば特権モードで実行されます。これらのデータは、ユーザー モードで実行されているスレッドがアクセスできないように保護されます。システムの呼び出しは、明示的に、またはページ フォールトや割り込みのように暗示的に行われる場合があります。以前のオペレーティング システムとは異なり、Windows では、ユーザー モードおよび特権モードの伝統的な保護に加え、プロセス境界を使用してサブシステムを保護します。アプリケーションに代わってWindowsが行う処理には、プロセス内の特権時間に加え、別のサブシステム プロセス内で現れるものもあります。
使用率、 プロセス 使用時間	プロセスが非アイドルのスレッドを実行するために費やす経過時間の割合をパーセントで表示します。この値は、サンプル期間において、アイドル状態のスレッドがアクティブである期間を計測し、その時間をサンプル期間から引いて算出します (各プロセスには、実行するスレッドがほかにない場合にサイクルを消費するアイドル状態のスレッドがあります)。このカウンタは、プロセスの処理状況の主要インジケータです。
使用率、 ユーザ使 用時間	プロセスがユーザー モードで費やす経過時間の割合をパーセントで表示します。ユーザー モードは、アプリケーション、環境サブシステム、必須のサブシステム用に設計された制限付きの処理モードです。  また、特権モードはオペレーティング システム コンポーネント用に設計され、ハードウェアおよびすべてのメモリに直接アクセスできます。オペレーティング システムは、オペレーティング システム サービスにアクセスするために、アプリケーション スレッドを特権モードに切り替えます。このカウンタは、サンプル時間の割合として平均ビジー時間を表示します。
<b>論理ディスク</b>	
論理ディ スクの空 き領域	選択した論理ディスクドライブの使用可能な空き領域の合計の割合をパーセントで表示します。
論理ディ スクイン ディスク アウト/秒	ディスク上の読み書き操作の比率。
<b>メモリ</b>	
使用率、 ページフ ァイル使 用状態	Memory\Committed Bytes の Memory\Commit Limit に対する比率です。コミットされたメモリとは、ディスクへの書き込みのためにページング ファイルに領域が予約されている物理メモリです。Commit Limit は、ページング ファイルのサイズによって決まります。ページングファイルが拡張されると、Commit Limit も増え、この比率は低くなります。このカウンタは平均値ではなく現在の値のみをパーセントで表示します。
利用可能 なメモリ	システム上で実行中のプロセスで利用可能な物理メモリのサイズをメガバイト数で表示します (Memory\Available Bytes ではバイト数で示されます)。ゼロメモリ、空きメモリ、およびスタンバイメモリの容量の合計です。空きメモリは、使用可能なメモリです。ゼロメモリは、以前のプロセスが使用したデータを以降のプロセスが参照しないようにゼロで埋められたメモリのページです。スタンバイメモリは、ディスクへのルート上にあるプロセスのワーキング セット (物理メモリ) から削除されているが、再呼び出しが可能なメモリです。このカウンタは、平均値ではなく最新の観測値のみを表示します。
ページイ ン、ページ アウト/秒	ハード ページ フォールトを解決するためにディスクから読み取られた、またはディスクに書き込まれたページの数です。このカウンタは、システム全体の遅延を引き起こすフォールトの主要インジケータです。Memory\Pages Input/sec および Memory\Pages Output/sec の合計です。ページの数がカウントされるので、そのままの値で Memory\Page Faults/sec などのページ カウントと比較することができます。(通常、アプリケーションが要求する) ファイル システム内および非キャッシュのマップされたメモリ ファイル内のフォールトを解決するために取得されたページを含みます。
<b>ネットワーク</b>	
受信バイ ト数/秒	各ネットワーク アダプタ上で受信されるバイトの比率です。これには、フレーム文字も含まれます。Network Interface\Bytes Received/sec は、Network Interface\Bytes Total/sec の一部です。
受信バケ ット数/秒	ネットワーク インターフェイス上で受信されるパケットの比率。
送信バイ ト数/秒	各ネットワーク アダプタ上で送信されるバイトの比率です。これには、フレーム文字も含まれます。Network Interface\Bytes Sent/sec は、Network Interface\Bytes Total/sec の一部です。
送信バケ	ネットワーク インターフェイス上で送信されるパケットの比率。

ト数/秒	
<b>物理ディスク</b>	
平均アクセス時間	ディスクの平均転送時間 (秒単位)。
物理ディスク イン、ディスクアウト/秒	ディスク上の読み書き操作の比率。
<b>システム</b>	
コンテキスト スイッチ/秒	コンピュータ上のすべてのプロセッサがあるスレッドから他のスレッドに切り替わる場合における組み合わせの比率です。コンテキストの切り替えは、実行スレッドが任意のプロセッサを解放する、優先度の高いスレッドによって割り込まれる、または Executive サービスやサブシステム サービスを使用するためにユーザー モードと特権 (カーネル) モードが切り替わる時に発生します。これは、すべてのプロセッサ上で実行中のすべてのスレッドの Thread\Context Switches/sec の合計値で、切り替えの回数で計測されます。システムおよびスレッド オブジェクトにはコンテキスト スイッチ カウンタがあります。このカウンタは、最新の 2 つのサンプルで観測した値の差をサンプル期間で割った値を表示します。
プロセッサ キュー長	プロセッサ キューにあるスレッドの数です。ディスク カウンタとは異なり、このカウンタは実行準備ができていないスレッドのみをカウントし、実行中のスレッドはカウントしません。プロセッサが複数あるコンピュータでもプロセッサ時間のキューは 1 つです。そのため、コンピュータにプロセッサが複数ある場合は、負荷を処理しているプロセッサの数でこの値を割る必要があります。負荷にもよりますが、通常は、プロセッサごとに 1 つの持続されているプロセッサ キューに対してスレッドが 10 未満であれば、許容されます。
<b>メモ:</b> これらの定義は Windows のパフォーマンス モニタリング カウンタのもので、Linux のパフォーマンス モニタリング カウンタの定義は若干異なる場合もあります。	

## パフォーマンス モニタリングのしきい値

すべてのパフォーマンス カウンタには、デフォルトの警告しきい値および重大なしきい値があります。これらのしきい値を超えると、デバイス ロールアップ ヘルスに影響を及ぼす警告が生成されます。- デバイス ヘルスの変化は、**グループヘルスビュー** (Del Management Console ポータル ページ) で表示できます。

表 9-5. パフォーマンス モニタリングのしきい値

メトリック (合計カウント (シンプル+コンパウンド))	単位	警告しきい値	重大なしきい値	範囲
<b>CPU</b>				
利用率、カーネル使用時間	%	70	80	0-100
利用率、プロセッサ使用時間	%	70	80	0-100
利用率、ユーザ使用時間	%	70	80	0-100
<b>論理ディスク</b>				
<b>メモ:</b> これらのカウンタは、サポートされている Linux オペレーティングシステムを実行しているサーバーでは利用できません。				
論理ディスクの空き領域	%	20	10	0-100
論理ディスク イン、ディスクアウト/秒	/秒	5	10	任意
<b>メモリ</b>				
利用率、ページファイル使用状態	%	90	95	0-100
利用可能なメモリ	MB	50	20	任意
ページ イン、ページアウト/秒	/秒	15	20	任意
<b>ネットワーク</b>				
受信バイト数/秒	バイト/秒	1250000	1875000	任意
受信パケット数/秒	パケット/秒	1250	1875	任意
送信バイト数/秒	バイト/秒	1250000	1875000	任意
送信パケット数/秒	パケット/秒	1250	1875	任意
<b>物理ディスク</b>				
平均アクセス時間	秒	1	2	任意
物理ディスク イン、ディスクアウト/秒	/秒	5	10	任意
<b>システム</b>				
コンテキスト スイッチ/秒	/秒	100000	200000	任意
<b>メモ:</b> コンテキスト スイッチは、サーバーごとに異なる可能性があります。これらの値は、状況に応じて判断して、設定してください。				
プロセッサ キュー長		4	8	任意

## 監視ポリシーの有効化

1. [監視と警告] ポータル ページの左側のウィンドウで、**[監視] → [ポリシー] → [監視ポリシー] → [Dell ポリシー]** を選択し、変更するポリシーを選択します。
  - 1 DRAC がインストールされているサーバーのエージェントヘルスを監視するには、**[デバイス エージェントヘルス - Dell Remote Access Controller - インバンド]** を選択します。
  - 1 OpenManage Storage Management デバイスのエージェントヘルスを監視するには、**[デバイス エージェントヘルス - OpenManage Storage Management]** を選

択します。

1. Linux システム パフォーマンスの監視を有効にするには、[Linux のパフォーマンス監視] を選択します。
  1. Windows システム パフォーマンスの監視を有効にするには、[Windows のパフォーマンス監視] を選択します。
  1. デバイスのヘルスを監視するには、[デバイスのプライマリヘルス] を選択します。
  1. 電力消費量の監視を有効にするには、[電源監視] を選択します。
2. [オン/オフ] ドロップダウンをクリックし、[オン] を選択します。
  3. [変更を保存する] をクリックします。
  4. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。「[クライアントポリシーアップデートの強制](#)」を参照してください。

## ポーリング設定の変更

1. [監視と警告] ポータル ページの左側のウィンドウで、[監視] → [ポリシー] → [メトリック ライブラリ] を選択します。
2. 間隔を変更するメトリックを選択し、鉛筆アイコンをクリックして編集します。
3. [ポーリング間隔] にミリ秒単位の時間を入力し、[OK] をクリックします。
4. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。詳細については「[クライアントポリシーアップデートの強制](#)」を参照してください。

## ルールへのタスクの追加

1. [監視と警告] ポータル ページの左側のウィンドウで、[監視] → [ポリシー] → [ルール ライブラリ] を選択します。
2. タスクを追加するルールを選択します。たとえば、[デバイスのプライマリヘルス - 重大] を選択し、鉛筆のアイコンをクリックして編集します。
3. ルールの編集ダイアログ ボックスの [アクション] セクションの [タスク] で、黄色の星印をクリックして新しいタスクを追加します。
4. 追加するタスクを選択します。たとえば、[電子メールの送信] を選択します。
5. 右側のウィンドウで、タスクと一緒に保存する適切な詳細を入力し、[OK] をクリックします。
6. このルールの一部として [タスク] リストにタスクが表示されることを確認します。
7. [ルールの編集] ダイアログ ボックスで、[OK] をクリックします。
8. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。詳細については「[クライアントポリシーアップデートの強制](#)」を参照してください。

## メトリックスの変更

メトリックスは変更できます。

メトリックの編集方法

1. [監視と警告] の Web ポータル ページで、[監視] → [ポリシー] → [エージェントレスのメトリックスの編集] を選択します。
2. [エージェントレスのメトリックス] で編集するメトリックスを選択し、鉛筆のアイコンをクリックします。
3. ポーリング間隔とタイムアウトに必要なアップデートを行ったら、[OK] をクリックします。



**メモ:** 複数のメトリックスを選択してポーリング間隔とタイムアウトをアップデートできます。

4. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。「[クライアントポリシーアップデートの強制](#)」を参照してください。

メトリック ルールの編集方法

1. [監視と警告] ポータル ページ、[監視] → [ポリシー] → [ルール ライブラリ] を選択します。
2. [エージェントレスのメトリックス] で編集するメトリックスを選択し、鉛筆のアイコンをクリックします。
3. メトリックスとアクションに必要なアップデートを行ったら、[OK] をクリックします。
4. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。「[クライアントポリシーアップデートの強制](#)」を参照してください。

## スマート メトリックの編集方法

1. [監視と警告] の Web ポータル ページで、[監視]→[ポリシー]→[メトリック ライブラリ] を選択します。
2. [エージェントレスのメトリックス] で編集するメトリックスを選択し、鉛筆のアイコンをクリックします。
3. メトリックス値とスマートキー値に必要なアップデートを行ったら、[OK] をクリックします。
4. クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。「[クライアント ポリシー アップデートの強制](#)」を参照してください。

## パフォーマンス ビューア

パフォーマンス ビューアは、パフォーマンス カウンタやその他の監視されているデータを表示するためのリアルタイム インターフェイスを提供します。リアルタイムでこのデータを表示するには、[アクション] → [監視] → [リアルタイム...]を選択し、デバイスを選択します。履歴データを表示するには、[アクション] → [監視] → [履歴...] をクリックし、デバイスを選択します。

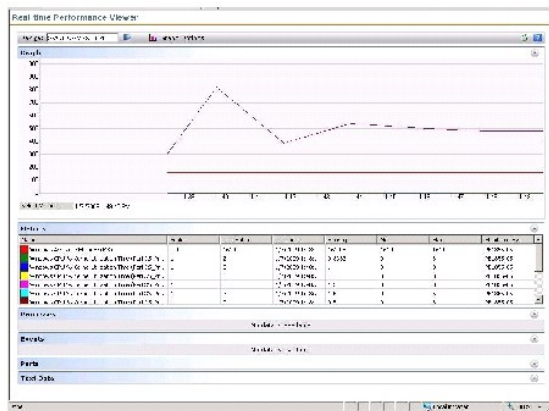
このインターフェイスの起動と表示の詳細については、[ヘルプ] → [マニュアル ライブラリ] で Symantec のマニュアルを参照してください。

### Dell™ OpenManage™ Server Administrator のメモ

1. パフォーマンス ビューアで利用できる機能は OpenManage Server Administrator で利用できる機能とは異なります。
1. パフォーマンス ビューア グラフを起動したとき、デバイス プライマリ ヘルス ステータスとデバイス接続状態がある OpenManage Server Administrator メトリックスに対し、そしてほかの OpenManage Server Administrator に対してもまた値が 99 に設定され起動されます。

### Dell™ OpenManage™ Storage Management のメモ

1. サーバーがストレージに接続され、すでに作成された仮想ディスクが 2 つあり、そしてサーバーが Dell Management Console で検出されている場合、ストレージ仮想ディスク コンポーネントの 2 つのプロンプがパフォーマンス ビューアで表示されます。OpenManage Server Administrator を使用して別の仮想ディスクが作成された場合、監視サービスを再起動したときかデバイスが再検出されたときのみに Dell Management Console に変更が表示されます。



## ヘルス モニタリング

ヘルス モニタリングは、検出されたすべての Dell デバイスのヘルスおよび接続状態を監視するための共通のインターフェイスを提供します。ヘルス モニタリングには、プライマリ デバイス ヘルス、エージェント ヘルス、およびデバイス接続状態が含まれます。デバイスのヘルスは、Symantec Notification Server® に送信され、Dell Management Console ホーム ページのロールアップ ビューに表示されます。また、デバイスのリソースマネージャ ポータル ページでは、ドリルダウン ビューからデバイス ヘルスも表示できます。

パフォーマンス ビューアでデバイス ヘルスを表示すると、メトリックスの Web パーツに数値が表示されます。表9-6 では、これらの値について説明しています。

表 9-6. 最後の値の説明

値	状態
0	標準
10	不明
20	情報
30	警告
40	メジャー
50	重大
99	切断
1	電源オフ

**メモ:** ほとんどの場合、デバイスが電源オフの間にアウト オフ バンド インターフェイスからデバイス ステータスを取得できる Dell Remote Access Controllers (DRAC) などのデバイスを除き、「切断状態」と「電源オフ状態」を区別することはできません。

すべてのヘルス モニタリング ポリシーはエージェントレス (デバイスへの AltirisAgent のインストールが不要) であり、デフォルトで有効に設定されています。

ルールは、ヘルス状態が変化したときに警告をトリガするために定義されます。

## ヘルス モニタリングの依存関係

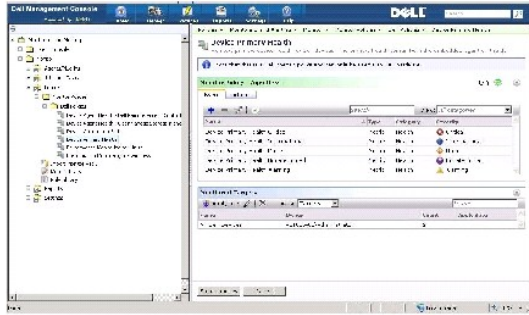
表 9-7. ヘルス モニタリングの依存関係

依存関係	説明
Dell OpenManage Server Administrator	DellServer ヘルスを管理するには、Server Administrator が必要です。Server Administrator をインストール中に、Storage Management および Dell Remote Access Controller をインストールすることもできます。
SNMP	SNMP は、ほとんどのネットワーク デバイスの監視に利用できる唯一のプロトコルです。
Navisphere® CLI (NaviCLI)	EMC® デバイスのヘルスを監視するには、NaviCLI が必要です。  Navisphere CLI の最新ソフトウェアとユーザー マニュアルは、powerlink.emc.com を参照してください。
シンボル	DellPowerVault™ MD 3000 アレイのヘルスを監視するには、Symbol が必要です。
WMI、IPMI	これらのプロトコルは、SNMP に加えてサーバー ヘルスを取得するためにオプションで使用できます。

## ヘルス ポリシー

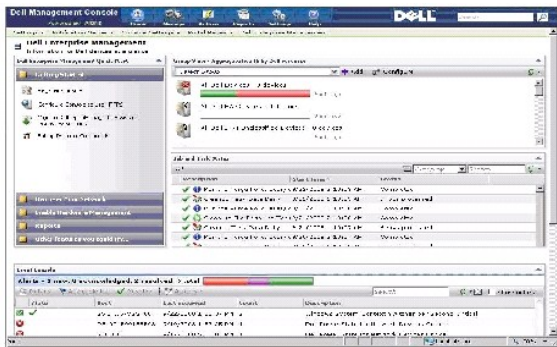
表 9-8. ヘルス ポリシー

ヘルス ポリシー	説明
デバイスのプライマリ ヘルス	デバイスの全体的ヘルス
デバイスの接続状態	デバイスがネットワークに接続されているかどうか
エージェント ヘルス - Storage Management	ソフトウェア ストレージ コンポーネントのヘルス
エージェント ヘルス - DRAC	リモート アクセス コントローラのヘルス



## グループ ビュー

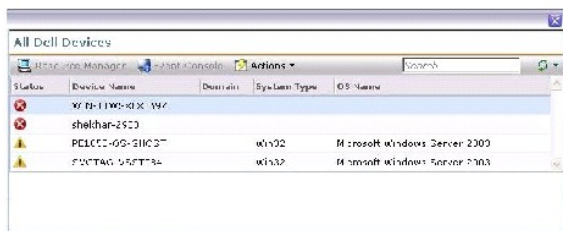
**グループ ビュー**は、デバイス ヘルスを表示する主要インターフェイスです。デバイスヘルスはハードウェアヘルスの最悪のケースのロールアップであり、パフォーマンス モニタリングでの警告条件に該当します。



この**グループ ビュー**は、Dell ヘルス監視ポリシーで収集されたヘルス値に基づいており、デバイスのヘルス状態に変化が生じるたびにリアルタイムで更新されます。この Web パーツの右上隅にある更新コントロールを使用して、更新間隔を指定できます。また、**[更新]** をクリックしてヘルス ステータス ビューをアップデートすることもできます。

この Web パーツは、デバイス クラスごとに棒グラフ表示でロールアップ ヘルスを表示する複数の定義済みのグループで構成され、さらにすべての Dell デバイスのヘルスをロールアップするサマリグループも表示します。また、ユーザー独自のカスタム グループを追加したり、既存のグループをこのビューから削除したりすることもできます。

デバイス グループのタイトルまたはデバイス グループ棒グラフのセクションをクリックすると、新しいウィンドウが開き、デバイスの完全なリスト、または特定の状態にそれぞれ一致しているデバイスが表示されます。このウィンドウには、グループのロールアップ状態に対する特定の要因とその他の詳細が表示されます。



**[リソース マネージャ]** を表示するには、**[すべての Dell デバイス]** ウィンドウでデバイスをクリックします。

## ヘルス モニタリングのリソース マネージャ ビュー





## 注意事項

- 1 Dell Management Console では、デバイスを検出および監視する際に同じプロトコルを使用します。たとえば、SNMP を含まないカスタム接続プロファイルを使用した場合、リソース マネージャおよびパフォーマンス ビューアで、次のようなパフォーマンス メトリックスおよび一部のヘルス メトリックスが表示されません。
  - デバイス エージェント ヘルス - OpenManage Storage Management
  - デバイス エージェント ヘルス - Dell Remote Access Controller IB (イン バンド)

## OnDemand モニタリング


OnDemand モニタリングを使用すると、SNMP 警告を受信したときに Notification Server でメトリックスのセットを簡単に収集できます。

この機能は、ヘルスに影響を与える可能性がある SNMP トラップを受信した時点で、デバイス ヘルスをポーリングするために使用されます。この機能により、ヘルスをアップデートするために次のポーリング間隔を待機することなく、ハードウェア ヘルスが変化した時点でデバイス ヘルスを正確かつ効果的に更新できます。

この機能を適切に機能させるには、Dell Management Console システムの IP アドレスを管理対象システムの SNMP サービス構成で SNMP トラップの宛先に入力します。

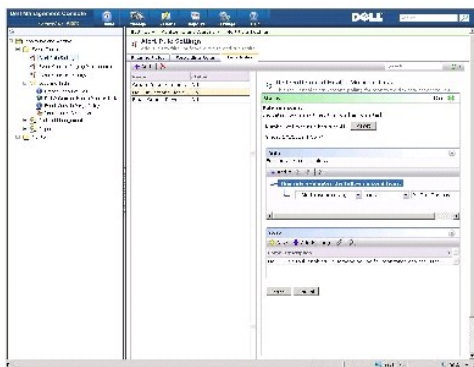
その他のデバイス タイプの場合は、デバイスのマニュアルで、トラップを Dell Management Console システムに転送する構成手順を参照してください。

OnDemand 機能はデフォルトで有効に設定されています。

 **メモ:** この機能は、デバイスからの SNMP トラップに依存しているため、デバイスが SNMP 管理用に構成されている必要があります。

OnDemand タスクと警告ルールは、**【監視と警告】** ポータル ページで確認できます。OnDemand 警告ルールでは、OnDemand タスクをトリガするのに必要な条件を定義し、この機能を有効にするかどうかを制御します。このルールは、左側のウィンドウの **【監視と警告】** → **【Event Console】** → **【警告ルールの設定】** に表示されます。右側のウィンドウの **【タスク ルール】** タブで、**【Dell OnDemand ヘルス監視タスク】** を選択します。


OnDemand タスクにより、OnDemand アラートがトリガされた場合に、どのメトリックスをポーリングするかが定義されます。このタスクは、警告ルール内でタスクをダブルクリックするか、左側のウィンドウで **【監視と警告】** → **【Event Console】** → **【ジョブとタスク】** → **【DellOnDemand ヘルス監視タスク】** を直接選択すると表示されます。



## 特定のデバイスへの OnDemand ポーリングの強制

1. **【管理】** → **【すべてのデバイス】** をクリックします。
2. 右側のウィンドウで、OnDemand ポーリングを強制するデバイスを右クリックし、**【プロパティ】** を選択します。
3. **【プロパティ】** ページで、[GUID] の値をコピーします。
4. **【ホーム】** → **【監視と警告】** をクリックします。
5. **【監視と警告】** ポータル ページで、**【Event Console】** → **【ジョブとタスク】** → **【Dell OnDemand ヘルス監視タスク】** をクリックします。
6. 右側のウィンドウの **【タスクのステータス】** Web パーツで、**【新規スケジュール】** をクリックします。

7. **【新規スケジュール】** ダイアログ ボックスでは、ポーリングをすぐに実行するか、後で実行するかをスケジュールできます。
8. **【監視されているリソース】** セクションで、ステップ 3 でコピーした Guid の値を貼り付けます。


 **メモ:** Guidに、スペースなどの余分な文字が含まれていないことを確認してください。

9. **【スケジュール】** をクリックします。

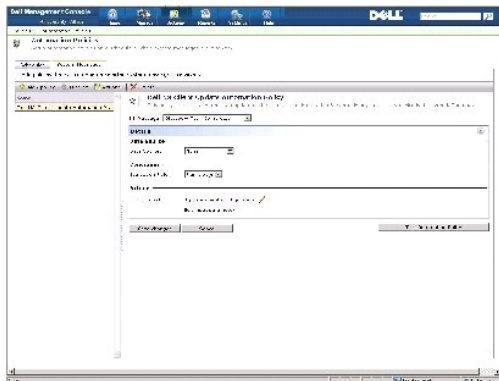
タスクが実行されると、ヘルス ビュー内でヘルス アップデートを確認できます。

## クライアント アップデート自動化ポリシー

新しいデバイスが検出されたり、監視ポリシー、メトリック、またはルールが更新されたりしたときは、クライアント ポリシーのアップデートが必要です。この機能を使用すると、新しいデバイスを検出するたびにクライアント ポリシーを自動的にアップデートできます。自動アップデートにより、Monitor Agent が再起動され、そのエージェントへのオープン接続が終了します。ただし、このポリシーでは Remote Monitoring Agent のアップデートの間に現在の監視プロセスへの瞬間的な割り込みが発生します。それでも、クライアント アップデートを手動で強制したり ([「クライアント ポリシー アップデートの強制」](#)を参照)、ポリシー、ルール、またはメトリックの変更後、次回ポーリングしたクライアントのアップデートを待機したりする必要があります。

 **メモ:** この機能は、エージェントレスの監視のみに適用されます。

この機能を定義するタスクを確認するには、**【管理】** → **【自動化ポリシー】** をクリックします。**【自動化ポリシー】** ページの **【システム メッセージ】** タブで、**【Dell NS クライアント アップデート自動化ポリシー】** を選択します。




## クライアント ポリシー アップデートの強制

クライアント ポリシー アップデートは、デフォルトで 1 時間ごとに発生します。

1. Notification Server の Windows ツールバーで、**【AltirisAgent】** アイコンを右クリックし、**【Altiris Agent 設定】** をクリックします。
2. **【Altiris Agent】** ダイアログ ボックスで、**【送信】** をクリックし、次に **【アップデート】** をクリックします。
3. **【構成】** セクションで、**【要求時間】**と**【変更時間】**が一致していること、またはアップデート後に**【変更時間】**が最新になっていることを確認します。

これは、構成が変更されたが、変更を監視するためにエージェントのリセットが必要であることを示します。

Monitor Agent のリセットには、数分以上かかることがあります (監視するデバイスの数が増えるほど、必要な時間が増えます)。リセットした後、メトリックスはデータが取得されると**パフォーマンス ビュー**で利用できます。

 **メモ:** 同じデバイスのすべてのメトリックスが同時に取得されないことがあります。また、使用する接続プロファイルによっては表示されるメトリックスが変わることもあります。接続プロファイルの詳細については、[「新しい接続プロファイルの作成」](#)および[「デフォルトの接続プロファイルの編集」](#)を参照してください。

## 異なるしきい値を持つ各種デバイスを監視するためのポリシーの複製

この手順は、デバイスの 2 つ以上のグループを異なるしきい値に対して同時に評価するポリシーまたはポリシーのサブセットを作成する場合にのみ必要です。

メトリックスとルールはグローバルに定義されます。つまり、これらの値に対して変更を行うと、メトリックまたはルールのすべての参照に影響を及ぼすということです。

あるデバイスまたはデバイスのグループに対して固有の変更を実行し、同時に別のデバイスのグループで元の値を維持する場合は、メトリックまたはルールを複製し、元のメトリックまたはルールではなく複製を参照する新しいポリシーを作成します。

### ルールの複製

1. **【監視と警告】** ポータル ページの左側のウィンドウで、**【監視】** → **【ポリシー】** → **【ルール ライブラリ】** を選択します。
2. 変更するルールを右クリックし、**【複製】** アイコンを選択します。

ルールが複製されます。


3. 複製したルールを選択します。
4. 変更するプロパティを変更して、**【保存】** をクリックします。
5. 変更するすべてのルールでステップ 1 ~ 4 を繰り返します。

### 元のポリシーの複製

1. **【監視と警告】** ポータル ページの左側のウィンドウで、複製するポリシーを選択します。
2. ポリシーを右クリックし、**【複製】** を選択します。

ポリシーが複製されます。

3. 複製したポリシーを選択します。
4. ポリシー内のすべての既存のルールを選択し、**-** ボタンを使用して削除します。
5. **+** ボタンを使用して、すべての新しいルールをポリシーに追加します。
6. 新しいポリシー名を入力し、**【適用対象】** ドロップ ダウンをクリックして、ポリシーの新しいターゲットを選択します。

 **メモ:** 元のポリシーと重ならないターゲットを選択していることを確認してください。そうでない場合、同じデバイス上でメトリックを 2 度監視することで帯域幅が失われる可能性があります。

7. **【オン/オフ】** ドロップ ダウンをクリックし、**【オン】** を選択します。
8. **【変更を保存する】** をクリックします。

クライアント ポリシーの強制アップデートを実行 (またはデフォルトのポリシー アップデート期間を待機) して、変更を有効にします。詳細については「[クライアント ポリシー アップデートの強制](#)」を参照してください。

## サーバー監視警告の管理

Dell Management Console を構成し、事前に選択したデバイスのヘルスのステータスに関する警告を特定のユーザーに電子メールで送信することができます。

電子メールを送信するスケジュールを設定することもできます。定義済みコレクション内のデバイスのヘルス ステータスの変更がタスクによって監視されているヘルス ステータスと一致する場合、次にタスクの実行がスケジュールされている時に指定されたユーザーに電子メールが送信されます。

タスクの作成および警告の送信の必須条件として、SMTP Server を追加し構成する必要があります。詳細は、[ヘルス モニタ電子メール タスクのスケジュール設定](#)を参照してください。

## ヘルス モニタ電子メール タスクの表示

ヘルス モニタ タスクのリストを表示する方法: [Dell Management Console] の **ポータル** ページで、[Dell Enterprise Management Quick Start] → [Quick Start] → [ヘルス モニタ電子メール タスク] を選択します。

## ヘルス モニタ電子メール警告の受信

警告を受信するには、SMTP Server を構成しヘルス モニタ電子メール タスクを作成および構成してからヘルス モニタ電子メール タスクのスケジュールを設定する必要があります。

ヘルス モニタ電子メール タスクの完了レポートが表示され、選択したユーザーに電子メールが送信されます。

ヘルス モニタレポートには、参照可能なデバイスが一覧表示されます。レポートでは、デバイスをクリックしリソース マネージャ ページを表示できます。

## SMTP Server の構成

SMTP Server を構成する手順

1. [Dell Management Console] で、**[設定]** → **[すべての設定]** → [Notification Server] → **[Notification Server の設定]** を選択します。
2. [Notification Server の設定] ページの **[電子メール]** タブで次を行います。
  - a. SMTP Server の **設定** 情報を入力します。
  - b. **デフォルトの電子メール アドレス** 情報を入力します。
  - c. **[テスト電子メールの送信]** をクリックして設定をテストします。
3. **[OK]** をクリックします。

## ヘルス モニタ電子メール タスクの作成

サーバーのヘルスに関する警告を受信するには、ヘルス モニタ電子メール タスクを構成します。

Dell Management Console で、次のいずれかの操作を行います。

- a. [Dell Management Console] ポータル ページで次の操作を行います。
  - i. [Dell Enterprise Management Quick Start] Web パーツで、**[Quick Start]** → **[新規ヘルス モニタ電子メール タスク]** を選択します。
  - ii. **[電子メール情報]** Web パーツで、警告中にユーザーに送信する電子メール情報を入力します。警告の条件を変更することができます。警告条件を変更するには、『Dell Management Console オンライン ヘルプ』を参照してください。
- b. **[ジョブとタスク]** ポータル ページで次の操作を行います。
  - i. Quick Start の **[ジョブとタスク]** Web パーツで **[新規ジョブまたはタスクの作成]** を選択します。
  - ii. **[新規ジョブまたはタスクの作成]** ページで、**[サーバー タスク ヘルス モニタ電子メール タスク]** を選択します。
  - iii. **[サーバー タスク ヘルス モニタ電子メール タスク]** ページで、電子メール情報を入力します。警告の条件を変更することができます。警告条件を変更するには、『Dell Management Console オンライン ヘルプ』を参照してください。

## ヘルス モニタ電子メール タスクのスケジュール設定

選択した Dell デバイス上で、ヘルス モニタ電子メール タスクを実行するスケジュールを設定することができます。**[タスクとジョブのポータル]** ページから警告タスクをスケジュールすることもできます。

ヘルス モニタ電子メール タスクのスケジュールを設定する手順

1. [Dell Management Console] ポータル ページで [Quick Start] → [ヘルス モニタ電子メール タスク] を選択します。
2. [ヘルス モニタ電子メール タスク] ページで電子メール タスクを選択します。
3. [タスクのステータス] で、[新規スケジュール] をクリックします。
4. タスクをスケジュールするには、[今すぐ] をクリックします。タスクを特定の頻度、指定の日時にスケジュールするには [スケジュール] を選択して詳細を入力します。
5. ヘルス モニタ電子メール タスクの電子メール条件を構成する時に入力パラメータを入力するフィールドを選択した場合は、これらのフィールドが利用可能になります。有効なフィールドに受信者の電子メール情報を入力します。
6. [スケジュール] をクリックします。
7. ヘルス モニタ レポートを表示するには、完了したスケジュールをクリックします。
8. レポートでデバイスをクリックするとリソース マネージャ ページを表示できます。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## 電源監視

### Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [電源監視の依存関係](#)
- [電源監視のメトリックス](#)
- [電源監視のしきい値](#)
- [電源監視の管理](#)
- [グループ メトリックス](#)

電源監視を使用すると、Dell Server の標準的なセットの電力消費量のカウンタを監視できますが、サーバーが電源監視をサポートしている必要があります。

電源監視では、次の機能を提供します。

- 1 Dell OpenManage が収集したメトリックスからデータを受信する。
- 1 電力消費量の傾向およびデバイスのデータをグラフ形式で表示する。
- 1 SNMP と WMI プロトコルを介してデータにアクセスする。
- 1 電源監視は、yx0x と yx1x サーバーおよび OpenManage Server Administrator version 5.3 以降がある次の x9xx サーバーのみでサポートされています。
  - 1 1950 MLK111
  - 1 2950 MLK111

サポートされているサーバーに関する詳細は、『Dell Management Console Version 1.1 のサポート情報マトリックス』を参照してください。

yxxx というサーバーの名前の形式では、「y」は R あるいは T などのアルファベットを示し、「x」は数字を示しています。

- 1 電源装置あたりのアンペア数は「A」、エネルギー消費は「KWh」など単一プローブの測定値を記録する。
- 1 総電源量といった総測定値を記録する。
- 1 リアルタイムの電力消費量データや電力消費量データの履歴などのグラフを表示する。
- 1 さまざまな電力消費量メトリックスのレポートを生成する。

### Dell™ OpenManage™ Server Administrator の関連メモ

- 1 一部の累積ステータスでは、OpenManage Server Administrator のステータスと Dell Management Console で表示されたステータスが異なる場合があります。
- 1 Dell Management Console では、累積したヘルスは常に最悪のケースの累積であるため、デバイスの重大なステータスはグループ表示であるグローバルヘルスに換え、重大なステータスを円グラフで監視します。

例えば、電源の 1 つがサーバーから削除されたとします。OpenManage Server Administrator では全体的なヘルス ステータスが警告として表示され、電源冗長性ステータスもまた警告として表示され、電源は「重大」として表示されます。正しいイベント (OpenManage Server Administrator ステータスと一致) は、リソース マネージャの中でも警告として表示されます。しかし Dell Management Console のサーバーヘルスステータスでは、**監視されているリソース (ステータス別)** の円グラフで「重大 (赤)」として表示されます。

### 電源監視の関連メモ

- 1 現在パフォーマンス ビューアでは、1 台のサーバーのみのリアルタイム電力消費量を提供していますが、複数のサーバーの電力消費量を見るにはレポートを表示する必要があります。
- 1 500 を超えるノードを管理する場合、電源監視は使用できません。500 ノード以下の場合、次の Dell Management Console 管理ステーションのシステム要件を満たしている必要があります。
  - 1 サポートされているオペレーティング システム (例: Microsoft® Windows Server® 2003 R2 SP2 (32 ビット) Standard または Enterprise Edition)
  - 1 物理プロセッサ: 2
  - 1 RAM: 4 GB
  - 1 DVD ドライブ
  - 1 Microsoft .NET Framework Version 3.5 または 3.5 SP1
  - 1 Windows Internet Information Services Version 6.0
  - 1 Microsoft SQL Express 2005 または SQL Express 2008、SQL Server 2005 または SQL Server 2008 (64 ビットリモート)

- 1 大規模環境の場合は、リモート データベース、および 8GB 以上の利用可能なメモリ
- 1 WMI プロトコルを使用して検出したデバイスのインベントリを収集する場合、[ハードウェアの概要] ページにある [電源情報] 表の電源タイプには値がありません。

## 電源監視の依存関係

電源監視の依存関係は次のとおりです。

表 10-1. 電源監視の依存関係

Dell ポリシー	エージェント/ エージェントレス	サポート範囲	デフォルトの動作	依存関係
電源監視	エージェントレス	サポートされている電源監視が有効になっている Dell サーバー	無効	SNMP および WMI プロトコル

## 電源監視のメトリクス

次にあげる Dell Servers による電力消費量のメトリクスを監視できます。


 **メモ:** 利用不可あるいは初期化中のメトリクスを表示するには、[利用不可あるいは初期化中のメトリクスの表示 (Show unavailable/initializing metrics)] チェック ボックスを選択します。監視対象に選択した数値のメトリクスは、[グラフとメトリクス] で使用でき、選択したテキスト メトリクスは [テキスト データ] で使用できます。このオプションを選択すると、Monitor Agent が収集しているほかのメトリクスを表示できますが、データが取得されるまでこれらのメトリクスを選択してグラフ表示することはできません。

表 10-2. 電源監視のメトリクス

メトリック	説明
<b>エージェントレス数値メトリクス</b>	
Dell の電源: 電源装置あたりのアンペア数 (Amps)	電源装置のアンペア数を監視する場合に選択します。
Dell の電源: エネルギー消費量 (KWh)	エネルギー消費量をキロワット時で監視する場合に選択します。
Dell の電源: エネルギー消費量 (BTU/hr)	エネルギー消費量を発熱量で監視する場合に選択します。
Dell の電源: エネルギー消費量 (Watts)	エネルギー消費量をワットで監視する場合に選択します。
Dell の電源: 瞬時ヘッドルーム (BTU/hr)	利用可能な瞬時ヘッドルームを発熱量で監視する場合に選択します。
Dell の電源: 瞬時ヘッドルーム (Watts)	利用可能な瞬時ヘッドルームをワットで監視する場合に選択します。
Dell の電源: 電力消費量 (BTU/hr)	電力消費量を発熱量で監視する場合に選択します。
Dell の電源: 電力消費量 (Watts)	電力消費量をワットで監視する場合に選択します。
<b>エージェントレス テキスト メトリクス</b>	
Dell の電源: エネルギー消費 (開始時間)	エネルギー消費の開始時間のテキスト データを表示する場合に選択します。

## 電源監視のしきい値

電力消費量は、使用しているハードウェアに固有のもので、1 つのシステムでは重大な消費量であっても、ほかのシステムでは範囲内である場合があります。便利なように、電源メトリクスで警告をトリガするルールが定義されています。しかしハードウェアとの密接な結び付きのため、これらのルールがトリガされたのを表示するには監視されているハードウェア固有の適切なしきい値を定義する必要があります。(デフォルトの設定では真のハードウェア値よりはるかに上に設定されています。)

## 電源監視の管理

電力消費の監視を使用するには、電源監視ポリシーを有効にします ([監視ポリシーの有効化](#)を参照)。

電源監視がアクティブ化されたことを確認した後、利用可能な電力消費量のメトリクスを使用してデバイスの電力消費量を監視することができます。次のいずれかを実行できます。

- 1 リアルタイム データを表示する ([電源監視メトリクスの管理](#)を参照)。

- 履歴データを表示する ([アクション] → [監視] → [履歴]) をクリックし、デバイスを選択。
- さまざまな電力消費量メトリックスのレポートを表示する (レポートを参照)。

電力消費量監視メトリックスのルールとアクションを変更することができます (メトリックスの変更を参照)。

## 電源監視メトリックスの管理

エージェントレス数値メトリックスとテキスト メトリックスのリストから必要なメトリックスを選択し、デバイスの電力消費量を監視することができます。さまざまなメトリックスのルールとアクションの定義を変更することができます。

デバイスの電力消費量を表示する方法

- 次のいずれかを実行してください。
  - Dell Management Console で [アクション] → [監視] → [リアルタイム] を選択します。
  - [監視と警告] ポータル ページの [パフォーマンス ビューアの起動] でデバイス アイコンをクリックしてデバイスを選択し、[起動] をクリックします。
  - [監視と警告] ポータル ページの [監視されているリソース (ステータス別)] でデバイスを選択し、[パフォーマンス ビューア] をクリックします。

[リアルタイム パフォーマンス ビューア] ページと [登録済みのメトリックス] ページが表示されます。

- [登録済みのメトリックス] ページに必要なメトリックスを選択し、[OK] をクリックします。詳細については、[電源監視のメトリックス](#) を参照してください。

## グループ メトリックス

この機能は Dell Management Console の今後のバージョンで利用可能になります。グループ メトリックスでは、効率的なデータ収集を可能にするインターフェイスを提供します。効率的にデータを収集することで、スマート メトリック レポートで表示された同じグループと比較する場合にレポートの計算がより速くなります。このインターフェイスでは、グループ レベルでのしきい値の作成も可能です。すべてのグループ メトリックスは、指定したグループの値の合計を計算します。グループ メトリックスは、常に 1 つのターゲットしか所有できません。そしてこのターゲットは、ポリシー ターゲットと同じかポリシー ターゲット内に含まれている必要があります。この両方は、[電源監視サポートのあるすべてのデバイス](#) グループのデフォルトとなり、検出時に自動的に決定されます。

表 10-3. グループ メトリックス

メトリックス	説明
Dell の電源: グループのエネルギー消費量 (KWh)	グループのエネルギー消費量を監視することができます。
Dell の電源: グループの瞬時ヘッドルーム (BTU/hr)	グループの利用可能な瞬時ヘッドルームを発熱量で監視することができます。
Dell の電源: グループの瞬時ヘッドルーム (W)	グループの利用可能な瞬時ヘッドルームをワットで監視することができます。
Dell の電源: グループの電力消費量 (BTU/hr)	グループが消費する電力を発熱量で監視することができます。
Dell の電源: グループの電力消費量 (W)	グループが消費する電力をワットで監視することができます。

## グループ メトリック レポートの表示

グループ メトリック データは、リアルタイムあるいは履歴ビューアでは表示できません。このデータは、グループ メトリック レポートでのみ表示することができます。

グループ メトリックスの表示方法 Dell Management Console で [レポート] → [すべてのレポート] → [グループ メトリック レポート] を選択します。

## グループ メトリックスの管理

事前定義されたグループ メトリックスは、電源監視ポリシーの一部です。これらのメトリックスは、スマート メトリックスと同じなため、キーが 1 つ違うだけで同じ方法で変更され、グループ メトリックスのターゲットを指定できます。同様に、グループ メトリックスの監視に使用されるルールは、スマート メトリックスのルールと同じ方法で変更できます。メトリックスの監視とルールの詳細は、[電源監視の管理](#) を参照してください。



---

[目次のページに戻る](#)

[目次のページに戻る](#)

# Dell Patch Management Solution

## Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [Dell Patch Management Solution について](#)
- [Altiris Agent 有効パッチ管理の必須条件](#)
- [ライフサイクル コントローラ有効パッチ管理の必須条件](#)
- [Patch Management Solution のユーザー インターフェイス](#)
- [DUP とシステムのバンドル](#)
- [DUP カタログのインポート](#)
- [Dell Inventory Collector ツール](#)
- [\[Dell ベンダ構成\] ページ](#)
- [Dell アップデート パッケージのダウンロード](#)
- [パッチ アップデートがサポートされている Linux Dell Server の検出](#)
- [パッチ アップデートがサポートされている Windows Dell Server の検出](#)
- [パッチ アップデートがサポートされているライフサイクル コントローラ有効 Dell Server の検出](#)
- [Dell Patch Management レポートへのアクセス](#)
- [整合性評価タスク](#)
- [Dell ハードウェア アップデートの管理](#)
- [DUP のステー징と配布](#)
- [ロールアウト ジョブ](#)
- [ロールバック レポート](#)
- [Patch Management Solution のトラブルシューティング](#)

Dell Patch Management Solution により、操作環境をスキャンして、サポートされている Dell™ PowerEdge™ システムが、BIOS 用、ドライバ用、ファームウェア用の Dell アップデート パッケージ (DUP) を受取するためのパッチの最低要件を満たしているかどうかを判断できます。またソリューションは DUP のダウンロードと配布を自動化します。

Dell Management Console は、ライフサイクル コントローラが搭載されているサーバーのパッチのアップデートをサポートします。最小のサポートされているライフサイクル コントローラ、およびパッチ アップデートに必要な Integrated Dell Remote Access Controller (iDRAC) ファームウェアの詳細は、『Dell Management Console のサポート情報マトリックス』を参照してください。

ライフサイクル コントローラが搭載されているサーバーでは、Symantec Management Agent (旧称 Altiris Agent) はパッチ サーバー アップデートを実行する必要はありません。

ライフサイクル コントローラ有効パッチ サーバー アップデートでは、BIOS、ファームウェア、またはその両方の既存バージョンの情報、オペレーティング システム ドライバ バック、32 ビット診断および Unified Server Configurator (USC) などのアプリケーション Dell アップデート パッケージ (APAC DUP) の情報を収集し、Dell Server 内の様々なハードウェア コンポーネントに最新のアップデートを適用することができます。必要なアップデートのスケジュールを設定し配備することもできます。

システムでアップデートが必要な場合は、*Dell Server Updates DVD* を使用するか、適切な DUP を Dell サポート Web サイト <ftp.dell.com> からダウンロードします。

### Dell Patch Management の関連メモ

- 1 ステージングと配布 (デフォルトの接続プロファイルあり) 中に Windows ターゲットとして選択されたサーバーでは、優先度で「ライフサイクル コントローラを使用してアップデートを適用する」が選択されている場合、ロールアウトジョブに失敗します。この問題を解決するには、ライフサイクル コントローラ ベースのアップデートにはライフサイクル コントローラ ベースのターゲットを使用します。
- 1 ステージングと配布 (適切な接続プロファイルあり) 中にライフサイクル コントローラ有効ターゲットとして選択されたサーバーでは、優先度で「Altiris Agent を使用してアップデートを適用する」が選択されている場合、ロールアウトジョブに失敗します。この問題を解決するには、Altiris Agent ベースのアップデートにはステージングと配布ウィザードで Windows ターゲットを使用します。
- 1 アップグレード後にバンドルを再度ステージングする必要があります。Dell Management Console version 1.1 へアップグレードすると、ステージングされたバンドルが削除されます。ステージングされたバンドルを取得するには、ステージング タスクを再度実行する必要があります。

### ステージング タスクを実行する方法

1. Dell Management Console で **[管理]** → **[ジョブとタスク]** → **[システム ジョブとタスク]** → **[ソフトウェア]** → **[Patch Management for Dell Servers]** → **[サーバー]** → **[ソフトウェア アップデート パッケージのダウンロード]** を選択します。

2. アップグレードする前にバンドルのステージングに使用するステージング タスクを選択し、ステージング タスクを右クリックして **[今すぐ開始]** を選択します。バンドルの再ステージング タスクが開始されます。

- 1 サーバーが Altiris Agent とライフサイクル コントローラ有効パッチ アップデートを同時にサポートするには、サーバーとサーバーの iDRAC を SNMP または WMI、そして WS-MAN プロトコルを含む接続プロファイルを使用して検出します。サーバーを検出する前に、サーバーに OpenManage Server Administrator をインストールする必要があります。

サーバーの検出後、Altiris Agent とライフサイクル コントローラ有効パッチの必須条件を完了します。

---

## Dell Patch Management Solution について

Dell Patch Management Solution で提供されるサポートは次のとおりです。

- 1 各アップデートおよびシステム アップデート セットのアップデートのサポート。

利便性と効率性を高めるには、バンドル ロールアウト ジョブを作成することをお勧めします。バンドル ロールアウト ジョブでは、単一の DUPとは対照的に、ソフトウェア アップデート セット全体 (バンドル) を配布します。

- 1 ライフサイクル コントローラが装備されているサーバー上のロールバック アップデートのサポート。以前のアップデートにのみロールバックできます。
  - 1 サポートされている Microsoft® Windows® および Linux オペレーティング システムを実行している Dell PowerEdge(TM) システムのサポート。
  - 1 オペレーティング システムに依存しないライフサイクル コントローラ有効パッチ アップデートを有する Dell PowerEdge システムのサポート。
  - 1 Dell システムを検出およびアップデートを受信するために必要なレベルまで Dell Server をアップデートするための単一サーバー ジョブのサポート。
- 

## Altiris Agent 有効パッチ管理の必須条件

あらかじめ次を完了しておく必要があります。


- 1 管理対象システムに Altiris Agent をインストールする。
  - 1 [ftp.dell.com](http://ftp.dell.com) または Dell™ Server アップデート ユーティリティから DUP カタログをインポートする。
  - 1 Inventory Collector をダウンロードする。
  - 1 クイックガイドの Web パーツの構成セクションで示されているように、整合性評価を実行する。
- 

## ライフサイクル コントローラ有効パッチ管理の必須条件

適用可能な DUP は、ライフサイクル コントローラがサポートしている BIOS、ファームウェア アップデートおよびアプリケーション Dell アップデート パッケージ (APAC DUP) に制限されます。APAC DUP には OS ドライブ パック、32 ビット診断、Unified Server Configurator (USC) が含まれています。

あらかじめ次を完了しておく必要があります。

- 1 サポートされているサーバーには、iDRAC6 Enterprise および USC の必要なファームウェアのバージョンが必要です。詳細については、『Dell Management Console のサポート情報 マトリックス』を参照してください。現在のバージョンの iDRAC にアップグレードする場合は、iDRAC を再検出する必要があります。

 **メモ:** iDRAC6 は構成されている必要があります。自動検出は Dell Management Console ではサポートされていません。

- 1 接続プロファイルで WS-MAN プロトコルを構成する。
  - 1 ライフサイクル コントローラ有効サーバーの iDRAC 6 は、DNS Server に登録する必要があります。Dell Management Console Server と iDRAC6 とのネットワーク通信には、ホスト名を使用できなければなりません。たとえば、Dell Management Console Server と iDRAC6 には、それぞれのホスト名を使用して Ping できる必要があります。
  - 1 WS-MAN 接続プロファイルを使用して iDRAC 6 Enterprise を検出する。検出されたデバイスは、Dell Server として分類されている必要があります。
  - 1 エージェントレス インベントリを使用して検出されたデバイスの情報を収集する。
  - 1 DUP カタログをダウンロードする。
  - 1 ライフサイクル コントローラ有効サーバーの整合性評価の実行
-

# Patch Management Solution のユーザー インターフェイス


Patch Management Solution のユーザー インターフェイス (UI) にアクセスする方法 [\[ホーム\]](#) → [\[Patch Management for Dell Servers のホーム\]](#) を選択します。

## Patch Management のクイックガイド

**[クイック ガイド]** Web パーツには、次の共通の構成および Patch Management プロセスの項目へのリンクがあります。

### 構成

- 1 **Proxy の構成** ([\[Notification Server の設定\]](#) ページをクリックすると表示されます。)
- 1 **アップデート カタログのダウンロード** ([\[DUP カタログのインポート\]](#) ページをクリックすると表示されます。)
- 1 **Inventory Collector のダウンロード** ([\[Dell Inventory Collector のインポート\]](#) ページをクリックすると表示されます。)

 **メモ:** [\[Dell Inventory Collector のインポート\]](#) ページは、Altiris Agent 有効パッチ アップデートにのみ必要です。

- 1 **ソリューションのグローバル設定** ([\[Dell ベンダ構成\]](#) ページをクリックすると表示されます。)
- 1 **Altiris Agent のインストール** ([\[Altiris Agent のインストール\]](#) ページをクリックすると表示されます。)

 **メモ:** [\[Altiris Agent のインストール\]](#) ページは、Altiris Agent 有効パッチ アップデートにのみ必要です。

### パッチ処理

- 1 **整合性チェックの実行対象**
  - 1 **Windows Server** ([\[パッチ適用可能な Windows Dell Server ジョブの判断\]](#) ページをクリックすると表示されます。)
  - 1 **Linux Server** ([\[パッチ適用可能な Linux Dell Server ジョブの判断\]](#) ページをクリックすると表示されます。)
  - 1 **ライフサイクル コントローラ有効サーバー** ([\[ライフサイクル コントローラ有効サーバーの整合性評価タスク\]](#) ページをクリックすると表示されます。ライフサイクル コントローラ有効パッチに必要です。)
- 1 **適用可能なアップデートの確認 (コンピュータ別)** ([\[ハードウェア アップデートの整合性レポート\]](#) ページをクリックすると表示されます。)
- 1 **アップデートの管理** ([\[Dell ハードウェア アップデートの管理\]](#) ページをクリックすると表示されます。)

**[サポートされているサーバーの識別]** Web パーツには、次の情報を含んだレポートが表示されます。

- 1 **[自動アップデートをサポートするサーバーを識別]** セクションには、次のレポートが含まれています。
  - 1 **スキャン対象コンピュータ:** このレポートは、整合性チェックの完了時に生成されます。このレポートは、Dell Management Console によって検出されたサーバー (ライフサイクル コントローラが装備あるいは Symantec Management Agent がインストールされているサーバー) を一覧表示した [\[Dell 自動パッチ サポートに対し評価されたコンピュータ\]](#) ページへのリンクを提供します。この一覧にはアップデートをサポートするサーバーが含まれています。
  - 1 **サポートされているサーバー:** このレポートは、整合性チェックの完了時に生成されます。このレポートは、Altiris Agent、ライフサイクル コントローラ有効パッチ アップデート、あるいはその両方をサポートするサーバーの一覧を含む [\[Dell 自動パッチ サポートに対し評価されたコンピュータ\]](#) ページへのリンクを提供します。
- 1 **[識別スキャンのスケジュール設定または開始]** セクションでは、サポートされているオペレーティング システム、サーバー モデルおよび Altiris Agent を有する Dell システムを検出することができます。管理対象システム上に Altiris Agent がインストールされていない場合は、[\[Altiris Agent のインストール\]](#) をクリックしてタスクを完了できます。

**[サポートされているサーバーのインベントリの収集]** Web パーツには、インベントリが正常に実行された Dell システムのリストを含むレポートが表示されます。一覧表示された Dell システムは、アップデートの受信準備ができていないか、必須条件を満たしていないか、インベントリが返されなかったかのいずれかです。インベントリ スキャンをスケジュールまたは開始するには次を行います。

- 1 パッチ アップデートがサポートされている Windows オペレーティング がインストールされている Dell Server を判断するには、[\[Windows 整合性評価タスク\]](#) をクリックします。
- 1 パッチ アップデートがサポートされている Linux オペレーティング がインストールされている Dell Server を判断するには、[\[Linux 整合性評価タスク\]](#) をクリックします。
- 1 パッチ アップデートがサポートされている ライフサイクル コントローラ有効 Dell サーバーを判断するには、[\[ライフサイクル コントローラ有効サーバーの整合性評価タスク\]](#) をクリックします。

**[アップデートの受信準備が整ったサーバーのアップデート整合性の確認]** Web パーツでは、サポートされている Dell システムの整合性を表示し、アップデートを配布します。円グラフには、最新のサーバー、1 つまたは複数の推奨アップデートが欠落しているサーバー、1 つまたは複数のオプションのアップデートがあるサーバー、1 つまたは複数の緊急アップデートが欠落しているサーバーがリストされます。円グラフのセクションをクリックすると、適用可能なアップデートが配布されます。

Altiris Agent およびライフサイクル コントローラ有効パッチ アップデートの **[アップデート タスクのステータスの確認]** Web パーツには、Altiris Agent 有効パッチの各アップデートおよびパ

ドル アップデートのステータス、そしてライフサイクル コントローラ有効サーバーのロールアウト ジョブのステータスが表示されます。


## DUP とシステムのバンドル

Dell アップデート パッケージ (DUP) は、Dell システムの BIOS、ドライバおよびファームウェアなどのシステム コンポーネントをアップデートします。DUP のコレクションは、Dell システム アップデート セットとして、バンドルでリリースされています。

Patch Management Solution のインターフェイスでは、システム アップデート セットはバンドルとして表示されます。Dell システムに個々の DUP を配布するのではなく、システム アップデート セットを配布することを推奨します。DUP は、DUP ロールアウト ジョブの作成で使用され、システム アップデート セットは、バンドル ロールアウト ジョブの作成で使用されます。

Altiris Agent 有効パッチ アップデートを使用してシステム コンポーネントをアップデートするには、Symantec Management Agent がインストールされている必要があります。ライフサイクル コントローラ有効アップデートにはエージェントは必要ありませんが、システム コンポーネント アップデートを完了するにはライフサイクル コントローラが必要です。

ライフサイクル コントローラ有効パッチでは、Altiris Agent 有効パッチ管理がサポートするすべてのアップデートがサポートされるわけではないので、バンドル アップデートを行うには Altiris Agent 有効パッチが推奨されます。

 **メモ:** デフォルトでは、Dell Management Console はライフサイクル コントローラ有効パッチ アップデートより Altiris Agent 有効パッチ アップデートを優先します。

Altiris Agent を使用してサーバーをアップデートするには、次を行います。

1. 接続プロファイルを作成し構成する。
2. Altiris Agent 有効パッチ アップデートを必要とする Dell システムを検出する。
3. **[Proxy の構成]** でネットワーク接続あるいはインターネット設定を構成する。
4. **[DUP カタログのインポート]** で DUP カタログをインポートする。

このリリースの Dell Management Console にアップグレードする場合は、DUP カタログを再度インポートする必要があります。

5. **[Inventory Collector のダウンロード]** で提供される URL から[Dell Inventory Collector ツール] をダウンロードする。
6. **[ソリューションのグローバル設定]** でベンダ情報を構成する。ftp.dell.com またはサーバー アップデート ユーティリティから DUP カタログをインポートすることができます。
7. **[Altiris Agent のインストール]** でエージェントをインストールする。
8. 整合性チェックで Windows、Linux またはその両方の整合性を確認する。システムのインベントリ情報は、整合性チェック中に収集されます。
9. レポートを使用してデータを表示し、**[ハードウェア アップデートの整合性]** レポートから Altiris Agent 有効パッチ アップデートを開始するか、**[アップデートの管理]** で Altiris Agent 有効パッチ アップデートを実行する。レポートを表示するには、**[最新の適用可能なアップデートの確認 (コンピュータ別)]** をクリックします。

アップデートまたはバンドルのロールアウトにライフサイクル コントローラを使用してサーバーをアップデートするには、次を行います。

1. WS-MAN プロトコルを使用して接続プロファイルを作成し構成する。
2. ライフサイクル コントローラ有効パッチ アップデートを必要とする Dell システムを検出する。(WS-MAN 接続プロファイルを使用して iDRAC 6 Enterprise を検出します。検出されたデバイスは、Dell コンピュータとして分類されている必要があります。エージェントレス インベントリを使用して検出されたデバイスの情報を収集します。)
3. **[Proxy の構成]** でネットワーク接続あるいはインターネット設定を構成する。
4. **[DUP カタログのインポート]** で DUP カタログをインポートする。
5. これらのシステムに対しエージェントレス インベントリを実行し、システムのインベントリ情報を収集する。
6. ライフサイクル コントローラ有効サーバーの整合性評価タスクを実行する。
7. レポートを使用してデータを表示し、**[ハードウェア アップデートの整合性]** レポートからライフサイクル コントローラ有効パッチ アップデートを開始するか、**[アップデートの管理]** でライフサイクル コントローラ有効パッチ アップデートを実行する。レポートを表示するには、**[最新の適用可能なアップデートの確認 (コンピュータ別)]** をクリックします。

ライフサイクル コントローラを使用してアップデートされたサーバーにロールバックを使用するには、次を行います。

1. レポートを表示するには、次のいずれかを行います。
  1. **[レポート]** → **[すべてのレポート]** → **[ソフトウェア]** → **[Patch Management for Dell Servers]** → **[ハードウェア アップデートの整合性]** を選択する。
  1. **[Patch Management for Dell Servers のホーム]** ポータル ページの**クイック ガイド** Web パーツで **[適用可能なアップデートの確認 (コンピュータ別)]** をクリックする。
2. **[ロールバックに利用可能なアップデート]** レポートのデータを表示します。

3. 「ステージングと配布」ウィザードを使用してライフサイクル コントローラ有効パッチ ロールバックを実行する。

---

## DUP カタログのインポート

[**DUP カタログのインポート**] ページを使用してダウンロード可能な Dell ソフトウェア管理パッケージを取得します。

Altiris Agent またはライフサイクル コントローラ有効パッチ アップデートの整合性評価を実行し、管理対象システムに適用可能な DUP を判断します。

評価に基づき、適用可能な DUP はステージングまたはステージングと配布のアクションを選択した場合にのみ Dell Management Console にダウンロードされます。最新の推奨される DUP を取得するには、カタログをダウンロードしなければなりません。

DUP カタログのインポート タスクを使用して、カタログのダウンロードを自動化することができます。Dell がリリースした最新の DUP を取得できるよう、このタスクを実行するスケジュールを指定します。

## Dell アップデート カタログのダウンロード

[**Dell ハードウェア アップデートの管理**] ページに DUP カタログのインポート タスクを設定するために、必要なソフトウェア管理リソースをダウンロードできます。

Dell アップデート カタログをダウンロードするには:

1. [**ホーム**] メニューで [**Patch Management for Dell Servers のホーム**] をクリックします。
2. [**クイックガイド**] Web パーツの [**構成**] の下の [**アップデート カタログのダウンロード**] をクリックします。
3. 右側のウィンドウで、次のいずれかを選択します。
  - **Dell サイト**
  - **ローカル ストレージ** (DUP をローカルで保存している場合)
  - [**変更された場合のみ**] は、デフォルトで選択されます。アップデートされたファイルのみがダウンロードされるので、不要なダウンロードは回避されます。
4. [**変更を保存する**] をクリックします。
5. [**新規スケジュール**] をクリックして、タスクのスケジュールを指定します。[**タスクのスケジュール**] ダイアログ ボックスでタスクを実行するスケジュールを指定するか、[**今すぐ**] を選択してタスクをすぐに実行します。

---

## Dell Inventory Collector ツール

Dell インベントリ コレクタ ツールを使用して、現在のオペレーティングシステムおよびハードウェア ファームウェアに関する情報を収集することができます。Dell Inventory Collector タスクは、Altiris Agent 有効パッチ アップデートにのみ必要です。

このツールでは、Dellシステムがアップデートを受信できるかどうかを判定します。Dell では、Windows オペレーティング システム搭載 Dell Server 用と Linux オペレーティング システム搭載 Dell Server 用のそれぞれのツールを提供しています。これらのツールは 3 ヶ月ごとにアップデートされ、公開されている Symantec ダウンロード ポータルから .cab ファイルとしてダウンロードすることができます。しかし、Dell Inventory Collector タスクにより、各ツールを自動的にダウンロードできます。

Dell Inventory Collector をダウンロードする手順

1. [**ホーム**] メニューから [**Patch Management for Dell Server のホーム**] をクリックします。
2. [**クイックガイド**] Web パーツの [**構成**] の下の [**Inventory Collector のダウンロード**] をクリックします。
3. 右側のウィンドウで、次のいずれかを選択します。
  - **Web URL:** Dell Inventory ツールを [solutionsam.com/imports/7\\_0/Patch/Dell/dellinvtool\\_windows.cab](https://solutionsam.com/imports/7_0/Patch/Dell/dellinvtool_windows.cab) あるいは [solutionsam.com/imports/7\\_0/Patch/Dell/dellinvtool\\_linux.cab](https://solutionsam.com/imports/7_0/Patch/Dell/dellinvtool_linux.cab) からダウンロードする
  - **ローカル ストレージ** (.cab ファイルがローカルで利用可能な場合)
4. [**変更を保存する**] をクリックします。

5. **[新規スケジュール]** をクリックして、タスクのスケジュールを指定します。**[タスクのスケジュール]** ダイアログ ボックスでタスクを実行するスケジュールを指定するか、**[今すぐ]** を選択してタスクをすぐに実行します。

## [Dell ベンダ構成] ページ

DUP アップデートのユーザー設定オプションでは、ライフサイクル コントローラ有効パッチ アップデートより Altiris Agent 有効パッチ アップデートが優先されています。

1. **[ホーム]** メニューで **[Patch Management for Dell Servers のホーム]** をクリックします。
2. **[クイックガイド]** Web パーツの **[構成]** の下の **[ソリューションのグローバル設定]** をクリックします。
3. 右側のウィンドウの **[Dell ベンダ構成]** ページで変更を行います。
4. **[適用]** をクリックします。

DUP の配布方法を設定するには、このページを構成します。これらの設定の一部は、**[ロールアウト ジョブ]** ウィザード内のデフォルト値として使用されます。ダウンロードされたすべての新しい DUP には、これらの設定がデフォルトで適用されます。設定を変更すると、既存のソフトウェア アップデート タスクとパッケージは、これらのデフォルト値を使用してアップデートされません。その場合は、**[ソフトウェア アップデートの管理]** ページからパッケージを再作成することで、アップデートを強制できます。

### [全般] タブのオプション

オプション	説明
DUP のダウンロード検証	すべての DUP が Dell に認定されていることを確認します。このオプションはデフォルトで選択されています。
DUP のダウンロードロケーション	Dell FTP サイトはデフォルトで選択されているため、DUP はこの Web サイトから直接ダウンロードされます。DUP を他の場所からダウンロードする場合は、 <b>[ローカルストレージ]</b> をクリックし、フィールドでロケーションを指定します。
DUP アップデートのユーザー設定	デフォルトでは、ユーザー設定は「 <b>Altiris Agent を使用してアップデートを適用する</b> 」に設定されています。ライフサイクル コントローラをユーザー設定として設定するには、「 <b>ライフサイクル コントローラを使用してアップデートを適用する</b> 」を選択します。 <b>メモ:</b> Altiris Agent とライフサイクル コントローラの両方を使用してサーバーをアップデートできる場合は、ユーザー設定に基づいてアップデートされます。
DUP の配布オプション	Windows オペレーティング システム、Linux オペレーティング システム、あるいはライフサイクル コントローラ用の配布される DUP を受信するには、ターゲットサーバーを指定します。

### [高度] タブのオプション

オプション	説明
パッケージのデフォルト	ソフトウェア アップデート パッケージを削除する頻度を指定できます。
パッケージの配布	Package Server の <b>配布を許可する</b> 。デフォルトで選択されています。Package Server がすべてのソフトウェア アップデート パッケージを処理します。詳細については、Symantec Management Platform のマニュアルを参照してください。 <b>Package Server 上の別のダウンロード先を使用する</b> 。パッケージをダウンロードする Package Server 上の別のロケーションを指定してから、Windows オペレーティング システムおよび Linux オペレーティング システムを実行している Dell システムのロケーションを入力します。 <b>クライアント上の別のダウンロード先を使用する</b> 。パッケージをクライアントシステムにダウンロードするための別のロケーションを指定してから、Windows オペレーティング システムおよび Linux オペレーティング システムを実行しているシステムのロケーションを入力します。

### [プログラム] タブのオプション

オプション	説明
プログラムのデフォルト	<b>実行の権限</b> ：プログラムを <b>[システム アカウント]</b> 、 <b>[ログインしたユーザー]</b> アカウント、 <b>[指定ユーザー]</b> アカウントのいずれかで実行するかどうかを指定します。 <b>指定ユーザー</b> を選択する場合は、フィールドでユーザードメインを指定します。このオプションは、Windowsを実行しているシステムにのみ適用されます。 <b>プログラムの実行条件</b> ：プログラムを実行できる条件を指定します。オプションには、 <b>[ユーザーがログオンしている場合のみ]</b> 、 <b>[ユーザーのログオンに関係なく]</b> および <b>[ユーザーがログオンしていない場合のみ]</b> があります。このオプションは、Windows を実行しているシステムにのみ適用されます。 <b>最小接続速度</b> ：デフォルトでは「 <b>エージェントの設定を使用する</b> 」が選択されていますが、別の速度も指定できます。 <b>次の時間後に終了</b> ：ソフトウェア アップデート タスクを終了するまでの時間を指定します。
エージェントイベント	管理対象システムから Dell Management Console システムに、関連のイベントを送信する場合に選択できます。

## Dell アップデート パッケージのダウンロード

ftp.dell.com またはサーバー アップデート ユーティリティから DUP カタログをインポートすることができます。DUP のダウンロード ロケーションは、[\[Dell ベンダ構成\] ページ](#)で構成できます。

---

## パッチ アップデートがサポートされている Linux Dell Server の検出

Linux オペレーティングシステムを実行している、サポートされているすべての Dell システムのうち、DUP の受信準備が整っているシステムをすべて検出できます。

Linux オペレーティング システムを実行し、パッチ アップデートがサポートされている Dell システム を検出する手順

1. **[ホーム]** メニューから **[Patch Management for Dell Server のホーム]** をクリックします。
  2. **[クイックガイド]** Web パーツの **[整合性チェックの実行対象]** の下の **[Linux Server]** をクリックします。
  3. **[パッチ適用可能な Linux Dell Server ジョブの判断]** ページで **[クイック実行]** をクリックしジョブをすぐ実行するサーバーを選択するか、**[スケジュール]** をクリックしジョブを定期的  
に実行するようにスケジュールを指定します。
- 

## パッチ アップデートがサポートされている Windows Dell Server の検出

Windows オペレーティングシステムを実行している Dell システムのうち、DUP の受信準備が整っているシステムを検出できます。

Windows オペレーティング システムを実行し、パッチ アップデートがサポートされている Dell システム を検出する手順

1. **[ホーム]** メニューから **[Patch Management for Dell Server のホーム]** をクリックします。
  2. **[クイックガイド]** Web パーツの **[整合性チェックの実行対象]** の下の **[Windows Server]** をクリックします。
  3. **[パッチ適用可能な Windows Dell Server ジョブの判断]** ページで **[クイック実行]** をクリックしジョブをすぐ実行するサーバーを選択するか、**[スケジュール]** をクリックしジョブを定  
期的に実行するようにスケジュールを指定します。
- 

## パッチ アップデートがサポートされているライフサイクル コントローラ有効 Dell Server の検出

ライフサイクル コントローラ有効パッチ アップデートをサポートしている Dell Server を検出することができます。

ライフサイクル コントローラが装備され、パッチ アップデートがサポートされている Dell Server を検出する手順

1. **[ホーム]** メニューから **[Patch Management for Dell Server のホーム]** をクリックします。
  2. Dell Management Console でデバイス検出ウィザードを使用して Dell Server を検出します。
  3. ライフサイクル コントローラを含む検出済みサーバーで、エージェントレス インベントリ ウィザードを使用してインベントリを収集します。
  4. **[クイックガイド]** Web パーツの **[整合性チェックの実行対象]** の下の **[ライフサイクル コントローラ有効サーバー]** をクリックします。
  5. **[ライフサイクル コントローラ有効サーバーの整合性評価タスク]** ページで、ライフサイクル コントローラ有効パッチを実行するサーバーを選択し、**[新規スケジュール]** をクリックして定  
期的にジョブを実行するスケジュールを指定します。デフォルトでは、このタスクにはライフサイクル コントローラが装備されているすべての Dell Server が選択されています。
- 

## Dell Patch Management レポートへのアクセス

レポートを使用して Altiris Agent およびライフサイクル コントローラ有効パッチ管理のデータを表示および管理できます。

Dell Patch Management レポートにアクセスする手順

1. **[レポート]** メニューで、**[すべてのレポート]** をクリックします。



2. 左側のウィンドウで、[レポート] → [ソフトウェア] → [Patch Management for Dell Servers] をクリックします。
3. 必要なレポートを含むフォルダを選択します。

たとえば、[Dell Server パッチ適用のインベントリ] レポート、[ハードウェア アップデートの整合性] レポート、[アップデート インストールの結果] レポートなどです。

## 整合性評価タスク

ライフサイクル コントローラ有効サーバーの整合性評価タスクでは、アップデート カタログからの利用可能なアップデートとサーバーに現在インストールされているアップデートを比較し、ターゲット サーバーの各種コンポーネントに対する適用可能なアップデートを判断します。このタスクは、インベントリによって収集された情報とアップデート カタログ内の情報に依存します。その結果、ターゲット サーバーに対しインベントリ タスクを実行し、カタログをダウンロードすることは、整合性評価タスクの必須条件になっています。

整合性評価タスクは、[クイック ガイド] Web パーツのリンクをクリックし、スケジュールとターゲット サーバーの情報を選択してスケジュールを設定することができます。整合性評価タスクが正常に実行された後、ユーザーは様々なハードウェア 整合性レポートを表示することができます。このレポートには、サーバー内の各種コンポーネント アップデートのインストール済みバージョンと利用可能なバージョンが表示されます。

## Dell ハードウェア アップデートの管理

[Dell ハードウェア アップデートの管理] ページでは、すべてのシステム アップデート セットを表示できます。DUP カタログ ファイル (.cab) は、「DUP カタログのインポート」タスクで ftp.dell.com または Dell Server Updates DVD からダウンロードできます。システム アップデート セットをステージングすると、関連付けられた DUP が Dell Management Console システムにダウンロードされます。システム アップデート セットの DUP がすべてダウンロードされると、バンドル ロールアウト ジョブで DUP を配布する準備が整います。[Dell ハードウェア アップデートの管理] ページでは、[ステージングと配布] タスクを作成できます。「[ステージングと配布ウィザード](#)」を参照してください。

[Dell ハードウェア アップデートの管理] ページで利用可能なオプション

オプション	説明
バンドルの管理 アップデートの管理	DUP (バンドルの管理) のバンドルの配布、または個々の DUP (アップデートの管理) の配布を選択できます。
フィルタ基準	システム モデルまたは名前によってフィルタできます。
OS タイプ	Windows、Linux またはすべてのオペレーティングシステム タイプでフィルタできます。
グループ	組織グループ内で検索できます。
アップデート	デフォルトではすべてのアップデート、あるいは適切なアップデートのみを表示することができます。
重要度	アップデートをフィルタする重要度レベルを選択できます。
すべてのバンドルのステージングと配布	リストされたすべてのバンドルをステージングおよび配布できます。
選択されたバンドルのステージングと配布	選択されたバンドルのみをステージングおよび配布できます。
選択されたバンドルの管理	1 つのバンドルを開き、1 つの DUP に対するロールアウト ジョブを作成します。
バンドル名	システム アップデート セットまたはバンドルの名前。
リリースの日付	バンドルがリリースされた日付。
重要度	バンドルの重要度レベル (例: 緊急)。
カレンダー	開始 (From) および終了 (To) の日付を指定すると、指定した日付の間にリリースされたバンドルを表示できます。
コンピュータ数	影響を受ける Dell システムの数。
アップデート数	バンドル内の DUP の数。
ダウンロード回数	関連するバンドルに対してダウンロードされた DUP の数。

## DUP のステージングと配布

バンドルのステージングと配布は、バンドルがリストされている [Dell ハードウェア アップデートの管理] ページから行えます。バンドルをステージングすると、関連付けられたすべての DUP が、Dell Web サイト ftp.dell.com から Dell Management Console システムにダウンロードされ、配布を選択することで選択したシステムにバンドルを展開してアップデートできます。DUPはローカルストレージからもダウンロードできます (例: Dell Server Updates DVD)。

DUP は、Dell システムのタイプ、オペレーティング システム、重要度およびグループでフィルタできます。

表示されているすべての DUP をステージングおよび配布するには:

1. **[ホーム]** メニューから **[Patch Management for Dell Server のホーム]** をクリックします。
2. **[クイックガイド]** Web パーツで **[アップデートの管理]** をクリックします。
3. 右側のウィンドウで、アップデートを適用するデバイスを選択し、次のいずれかを行います。
  1. **「すべてのアップデートのステージングと配布」**を選択する: すべてのサーバーに対しすべての適用可能なバンドルがステージングされ、サーバーの要件に基づいて個々の DUP がサーバーにプッシュされインストールされます。
  1. **「選択したアップデートのステージングと配布」**を選択する: 選択されたバンドルのみがステージングされ、サーバーの要件に基づいて個々の DUP がサーバーにプッシュされインストールされます。
  1. **「選択したアップデートを管理する」**を選択する: バンドルから選択された DUP のみがステージングされ、選択された DUP がサーバーにプッシュされインストールされます。

## ステージングと配布ウィザード

**[ステージングと配布]** ウィザードで、ロールアウト ジョブを作成します。ロールアウト ジョブにより、Dell アップデート パッケージ (DUP) を管理対象システムに配布します。このウィザードでは、適用可能なシステム上のみ DUP をインストールするために、ターゲットを自動的にフィルタします。

Altiris Agent およびライフサイクル コントローラ有効パッチの両方をサポートする Windows Server の場合に備え、1 つのターゲットのみでアップデートされるサーバーを選択します。たとえば、Windows Server に対し Altiris Agent 有効パッチ アップデートを使用して DUP またはバンドルを適用する場合は、サーバーを Windows ターゲットのみに追加する必要があります。

アップデートのオプションは、選択したターゲットに基づいています。

1. **Windows ターゲット** オプションは、レポートで Windows DUP またはバンドルが選択された場合に利用できます。
1. **Linux ターゲット** オプションは、レポートで Linux DUP またはバンドルが選択された場合に利用できます。
1. **ライフサイクル コントローラ有効ターゲット** オプションは、レポートで Windows DUP かバンドルあるいはその両方、またはアップデートのロールバックが選択された場合に利用できません。

### ステージングと配布ウィザードのオプション

オプション	説明
<b>再起動オプション</b>	<b>今すぐ再起動する:</b> DUP をインストールした後、すぐに再起動する場合に選択します。  ライフサイクル コントローラ有効サーバーでは、「今すぐ再起動する」のオプションが有効になっていない場合、サーバーを再起動した時にのみサーバーがアップデートされます。  <b>再起動しない:</b> DUP をインストールした後に再起動しない場合に選択します。
<b>インストール オプション</b>	<b>サイレント:</b> サイレント インストールを実行する場合に選択します。  <b>サイレント、ダウングレードを許可:</b> 廃止になった DUP をインストールする場合に選択します。
<b>ライフサイクル コントローラ有効サーバーの接続プロファイルの選択</b>	<b>接続プロファイル:</b> 既存のプロファイルを選択および編集する場合に選択します。  <b>新規:</b> 新しい接続プロファイルを作成する場合に選択します。  これは、ライフサイクル コントローラを基にしたアップデートのみに必要です。選択した WS-MAN 接続プロファイルは、アップデートするサーバーの検出に使用したものとは異なる可能性があります。ライフサイクル コントローラを基にしたパッチを実行するため、パッチに使用した WS-MAN 接続プロファイルにはターゲット サーバーの iDRAC での管理者権限が必要です。
<b>スケジュール</b>	<b>今すぐ:</b> DUP をすぐにインストールする場合に選択します。  <b>スケジュール:</b> DUP のインストールをスケジュールする場合に選択します。
Windows ターゲット	ロールアウト ジョブを適用するターゲットを選択する場合に選択します。ロールアウト ジョブから DUP を受信するのは、ターゲット内の適用可能なコンピュータだけです。
<b>ライフサイクル コントローラ有効ターゲット</b>	ロールアウト ジョブを適用するターゲットを選択する場合に選択します。適切なターゲットのみがロールアウト ジョブから DUP を受信します。
Linux ターゲット	ロールアウト ジョブを適用するターゲットを選択する場合に選択します。ロールアウト ジョブから DUP を受信するのは、ターゲット内の適用可能なコンピュータだけです。
<b>バンドル リストの配布</b>	ロールアウト ジョブによって配布される DUP バンドルのリスト。
<b>作成</b>	ウィザードを完了して、[ステージングと配布] ジョブを作成します。

## ロールアウト ジョブ

ロールアウト ジョブには、Dell アップデート パッケージを管理対象システムに配布するための一連のタスクが含まれています。

次のロールアウト ジョブを表示できます。

- 1 DUP ロールアウト ジョブ

単一の DUP が含まれている DUP ロールアウト ジョブは、**[ジョブとタスク] → [システム ジョブとタスク] → [ソフトウェア] → [Patch Management for Dell Servers] → [ロールアウト ジョブ] → [DUP]** フォルダに保存されます。

- 1 バンドル ロールアウト ジョブ

システム アップデート セットにすべての DUP が含まれている DUP ロールアウト ジョブは、**[ジョブとタスク] → [システム ジョブとタスク] → [ソフトウェア] → [Patch Management for Dell Servers] → [ロールアウト ジョブ] → [バンドル]** フォルダに保存されます。

ロールアウト ジョブは、サーバー コンポーネントを新しいバージョンにアップデートするだけです。現在ターゲット サーバー上にインストールされているものより古いアップデートでロールアウト ジョブを実行すると、そのジョブは失敗します。ダウングレードを強制するオプションは別にあります。

## ロールアウト ジョブの作成


ロールアウト ジョブは、管理対象システムにアップデートをインストールするために作成されます。

DUP ロールアウト ジョブを作成するには:

1. **[管理]** → **[ソフトウェア]** をクリックします。
2. 左側のウィンドウで、**[ソフトウェア]** → **[Dell ハードウェア アップデートの管理]** をクリックします。
3. 右側のウィンドウで、バンドルを選択します。
4. **[選択したアップデートの管理]** をクリックします。

選択したバンドル内のすべての DUP が表示されます。

5. 配布するアップデートを右クリックし、**[選択したアップデートのステージングと配布]** をクリックします。

 **メモ:** 複数の DUP を選択すると、ライフサイクル コントローラを使用してアップデートが実行された時に単一のロールアウト ジョブが作成されます。

6. DUP ロールアウト ジョブを作成したら、**[ジョブとタスク] → [システム ジョブとタスク] → [ソフトウェア] → Patch Management for Dell Servers → [ロールアウト ジョブ] → [DUP]** フォルダに移動して、DUP ロールアウト ジョブのステータスを表示します。

バンドル ロールアウト ジョブを作成する手順

1. **[管理]** → **[ソフトウェア]** をクリックします。
2. 左側のウィンドウで、**[ソフトウェア]** → **[Dell ハードウェア アップデートの管理]** をクリックします。
3. 右側のウィンドウで、テーブル内のバンドルを選択します。
4. **[選択したアップデートのステージングと配布]** をクリックします。
5. [ステージングと配布] タスクが、**[ジョブとタスク] → [システム ジョブとタスク] → [ソフトウェア] → [Patch Management for Dell Servers] → [サーバー] フォルダの [ステージングと配布]** ジョブに表示されます。このジョブは読み取り専用で、ロールアウト ジョブの進行状況の確認に使用します。[ステージングと配布] タスクが完了した後に、ロールアウト ジョブが作成されます。
6. バンドル ロールアウト ジョブを作成したら、**[ジョブとタスク] → [システム ジョブとタスク] → [ソフトウェア] → Patch Management for Dell Servers → [ロールアウト ジョブ] → [バンドル]** フォルダに移動して、バンドル ロールアウト ジョブのステータスを表示します。

## ロールアウト ジョブのステータスの表示

**[アップデートのステージングと配布]** ジョブでは、DUP を処理し、個々の DUP または バンドル アップデートのアップデートに対し、ロールアウト ジョブを作成します。

ロールアウト ジョブのステータスを表示する方法

1. Dell Management Console で、次のいずれかの操作を行います。
  1. **【管理】** → **【ジョブとタスク】** をクリックします。
  1. **Patch Management for Dell Servers のホーム** をクリックします。**【アップデート タスクのステータスの確認】** Web パーツにロールアウト ジョブのステータスが表示されます。

ロールアウト ジョブのステータスを表示する方法: **【ジョブとタスク】** → **【システム ジョブとタスク】** → **【ソフトウェア】** → **【Patch Management for Dell Servers】** → **【ロールアウト ジョブ】** → **【DUP】** または **【バンドル】** を選択します。

## ライフサイクル コントローラ有効ロールアウト ジョブ

ライフサイクル コントローラ有効ロールアウト ジョブは、すべてのライフサイクル コントローラ有効パッチ タスクで構成される Altiris ジョブ インフラストラクチャに基づいたジョブです。複数のアップデートの適用に、単一のロールアウト ジョブを実行することができます。

たとえば、N 個のアップデートが適用される場合、ロールアウト ジョブには以下が含まれます。

1. N 個のライフサイクル コントローラ有効アップデートの送信タスク
1. 1 つのライフサイクル コントローラ有効アップデートの実行タスク
1. N 個のライフサイクル コントローラ有効ステータス ポーリング タスク

ライフサイクル コントローラ有効ロールアウト ジョブは、管理対象システムに1 つ以上の DUP を適用するよう選択した時に **【ハードウェア アップデートの整合性】** レポートの 1 つ通して作成されます。各ジョブ内の各タスクには固有の機能があります。**【アップデートの送信】** タスクは、Dell Management Console からターゲット上のライフサイクル コントローラに DUP をダウンロードします。**【アップデートの実行】** タスクは、ライフサイクル コントローラを起動し特定の DUP のアプリケーションを開始します。**【ステータス ポーリング】** タスクは、DUP アプリケーションのステータス (DUP アプリケーションが正常に完了したかどうか) を確認します。ステータス メッセージは、アップデート後に表示されます。

---

## ロールバック レポート

ロールバック レポートには、以前インストールされた BIOS のバージョンまたはライフサイクル コントローラ有効サーバーで利用可能なファームウェアのアップデートが一覧表示されます。BIOS とファームウェアのみをロールバックできます。

ロールバックできない項目は次のとおりです。

1. Universal Server Configurator (USC)
1. Dell Diagnostics アプリケーション
1. オペレーティング システム (OS) インストール用のドライバ

### ロールバック レポートの表示

1. レポートを表示するには、次のいずれかを行います。
  1. **【レポート】** → **【すべてのレポート】** → **【ソフトウェア】** → **【Patch Management for Dell Servers】** → **【ハードウェア アップデートの整合性】** を選択する。
  1. **【Patch Management for Dell Servers のホーム】** ポータル ページの**クイック ガイド** Web パーツで **【適用可能なアップデートの確認 (コンピュータ別)】** をクリックする。
2. **【ロールバックに利用可能なアップデート】** レポートのデータを表示します。

ロールバック レポートでは、以下を行うことができます。

1. 以前インストールされた BIOS またはファームウェアにロールバックする方法: システムに適用するロールバック アップデートを選択し、**【選択したアップデートのロールバック】** をクリックします。
1. すべてのロールバック アップデートを適用する方法: **【すべてのアップデートのロールバック】** をクリックします。
1. ロールバック アップデートのバージョンと現在システムにインストールされているバージョンを比較するには、**【インストール済みのバージョン】** と **【利用可能なバージョン】** フィールド内のバージョンを比較します。
  1. サーバー: ロールバック アップデートを適用できるサーバーの名前が表示されます。
  1. デバイス: ロールバック アップデートを適用できるサーバー上のデバイスの名前が表示されます。

- 1 タイプ: コンポーネント タイプ (BIOS またはファームウェア) が表示されます。

## Patch Management Solution のトラブルシューティング

トラブルシューティングに役立てるため、レポートおよび実行インスタンスの詳細でエラー コードが生成されます。

### Dell アップデート パッケージの終了コード

アップデート パッケージを実行すると、終了コードが生成されます。これらのコードは、[Dell アップデートの実行の詳細] レポートに表示されます。終了コードは、アップデート パッケージの実行結果を判断および分析する場合に役立ちます。

表 11-1. DUP の終了コード

値	メッセージ	説明
0	SUCCESSFUL	アップデートに成功しました。
1	失敗	アップデート プロセス中にエラーが発生し、アップデートが失敗しました。
2	REBOOT REQUIRED	アップデートを適用するためにシステムを再起動します。
3	DEP_SOFT_ERROR	考えられる理由は次のとおりです。 <ul style="list-style-type: none"><li>1 同じバージョンのソフトウェアをアップデートしようとした。</li><li>1 前のバージョンのソフトウェアにダウングレードしようとした。</li></ul>
4	DEP_HARD_ERROR	要求されている必須条件のソフトウェアがシステム上で見つかりませんでした。
5	QUAL_HARD_ERROR	アップデート パッケージが適用できません。  考えられる理由は次のとおりです。 <ul style="list-style-type: none"><li>1 アップデート パッケージがオペレーティング システムをサポートしていない</li><li>1 アップデート パッケージとシステム内で見つかったデバイスとの互換性がない</li></ul>
6	REBOOTING_SYSTEM	システムの再起動

### Windows Dell Server 検出タスクの失敗エラー コード

これらのエラー コードは、Windows DellServer 検出タスクが失敗した場合に表示されます。コードは、タスクの実行インスタンスの詳細に表示されます。

表 11-2. Windows Dell Server 検出タスクの失敗エラー コード

値	メッセージ	説明
10	Err_OK_IsDellServer	実行に成功しました。システムは DellServer です。
11	Err_OK_IsNotDellServer	実行に成功しました。システムはDell Server ではありません。
12	Err_OK_IsNotSupportedDellServer	実行に成功しました。システムは Dell コンピュータですが、サポート可能な DellServer でないか、サポート可能なオペレーティングシステムがありません。
-20	Err_EndofScript	Err_EndofScript は現在使用されていません。
-21	Err_FileNotFound	サーバー リスト ファイル (DellServers.ini) が見つかりませんでした。
-22	Err_FailedStringSearch	現在使用されていません。
-24	Err_InvalidCmdArgument	コマンドラインの引数が間違っています。空白、"/model"または "/omsa" である必要があります。
-25	Err_CantAccessWMI	WMI クエリを実行できませんでした。インストールされていないか、実行されていません。

### Linux Dell Server 検出タスクの失敗エラー コード

これらのエラー コードは、Linux Dell Server 検出タスクが失敗した場合に表示されます。コードは、タスクの実行インスタンスの詳細に表示されます。

表 11-3. Linux Dell Server 検出タスクの失敗エラー コード

値	メッセージ	説明
7	RPM_VERIFY_FAILED	RPM 検証が失敗しました。
10	Err_OK_IsDellServer	実行に成功しました。システムはDellServer です。
11	Err_OK_IsNotDellServer	実行に成功しました。システムはDell Server ではありません。
12	Err_OK_IsNotSupportedDellServer	実行に成功しました。システムは Dellコンピュータですが、サポート可能な Dell Server でないか、サポート可能なオペレーティングシステムがありません。
21	Err_FileNotFound	エラー。サーバー リスト ファイル (DellServers.ini) が見つかりませんでした。ファイル名が SupportedDellServers.txt で指定されているものと異なります。
24	Err_InvalidCmdArgument	エラー。コマンドラインの引数が間違っています。
25	Err_CantAccessDMI	DMI クエリを実行できませんでした。

[目次のページに戻る](#)

[目次のページに戻る](#)

## レポート

### Dell™ Management Console Version 1.1 ユーザーズ ガイド


- [レポート モジュールについて](#)
- [レポート ユーザー インターフェイス](#)
- [新規 SQL レポートの作成](#)
- [新規 Dell コンピュータ レポートの作成](#)
- [Dell レポートの編集](#)
- [レポートの実行](#)
- [レポートの保存](#)
- [レポートの表示](#)
- [メトリック レポート](#)
- [グループ メトリック レポートの表示](#)

Dell™ Management Console のレポート モジュールを使用すると定義済みのレポートを表示でき、DellManagement Console で検出され監視されているさまざまなデバイスで収集したデータのカスタム レポートを作成することができます。

定義済みのレポートは、デバイスに固有のレポートで、CSV (スプレッドシート)、XML、および HTML 形式で保存できます。

レポートを表示するには、レポート モジュールを使用します。レポートは収集した情報を処理し、次の情報を表示します。

- 1 実行したタスク、および成功または失敗したタスク。
- 1 ユーザーの資産 (場所、および所有者)。

 **メモ:** レポートで利用できるデータは、リアルタイムのデータではないためタイム ラグが生じます。

#### レポートの関連メモ

- 1 電力予算および電力プロファイル情報は、次のプラットフォームではサポートされていません。
  - 1 R805 (Dell OpenManage 5.5、OpenManage 6.1、または OpenManage 6.2)
  - 1 R905 (OpenManage 6.1 または OpenManage 6.2)

このため、電力予算および電力プロファイル情報はインベントリ (SNMP 検出) および電力予算レポートで利用できません。

---

## レポート モジュールについて

レポート モジュールを使用すると、デバイスに関連付けられた、インベントリ、モニタリング、およびパフォーマンスの詳細を表示できます。

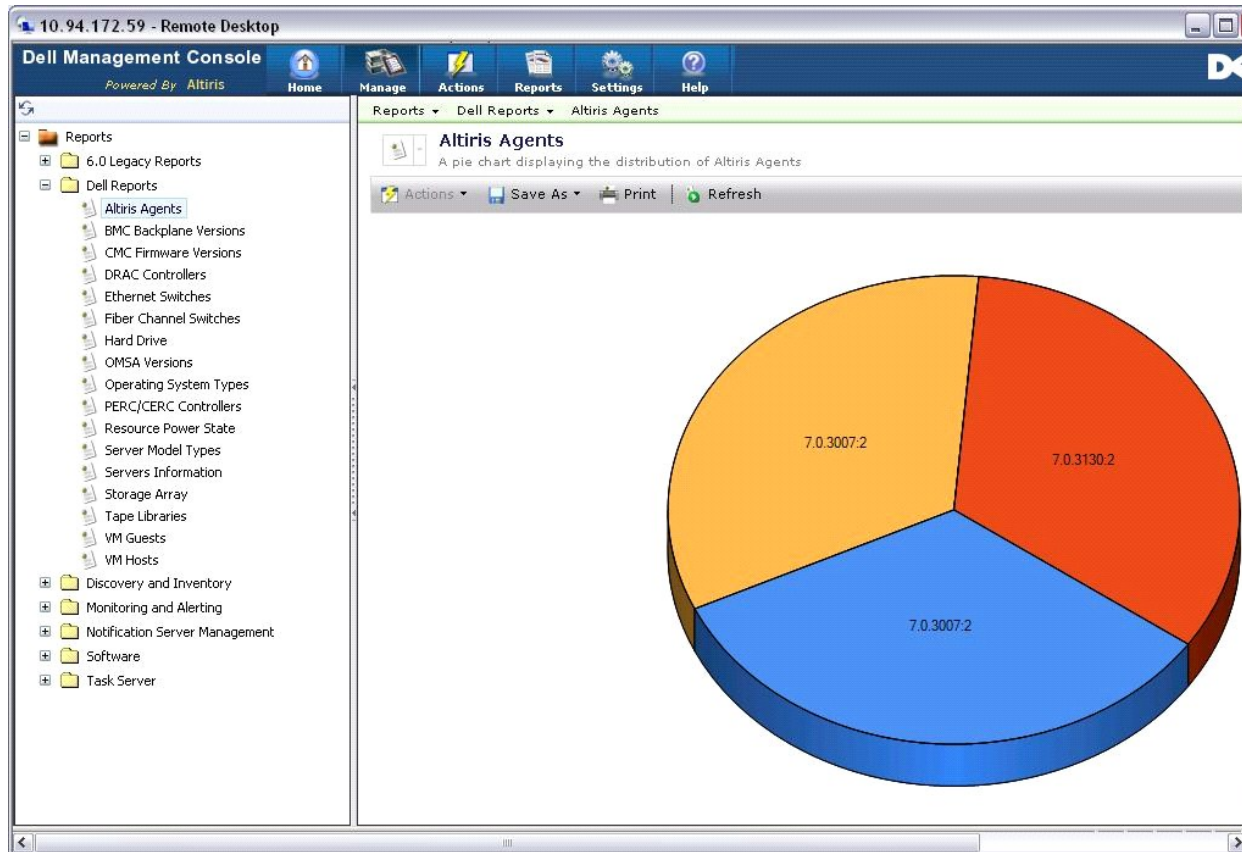
DellManagement Console Report Packs に含まれているさまざまな既存のレポートを実行できます。また、簡素なウィザードベースのフローを使用して、カスタム レポートを作成することもできます。カスタム レポートは、かなり簡素にすることも、SQL のようなクエリを含めてより複雑なレポートにすることもできます。詳細については、Symantec™ のユーザー ガイドを参照してください。

---

## レポート ユーザー インターフェイス

[**レポート**] ポータル ページにアクセスする方法 [**レポート**] → [**すべてのレポート**] を選択します。

### レポート ユーザー インターフェイスの概要



左側のウィンドウに、**【レポート】** ツリーが表示されます。このツリーから、定義済みの Dell レポートにアクセスできます。

**【Dell レポート】** をクリックします。定義済みの Dell レポートとその説明が右側のウィンドウに表示されます。

定義済みの Dell レポートごとに、選択したレポートのグラフ表示が右側のウィンドウに表示されます。右側のウィンドウから、次の操作を実行できます。

- 1 表示されたレポートを別の形式 (XML など) で表示する。
- 1 表示されたレポートをエクスポートする。
- 1 表示されたレポートを保存する (特に Web パーツとして)。「[レポートの保存](#)」を参照してください。
- 1 表示されたレポートを印刷する。

円グラフの任意の部分をクリックして、レポートに関する詳細を表示できます。

**メモ:** 新しくシステムを検出した場合、接続状態データはリソース接続状態のレポートにすぐに表示されません。

## 新規 SQL レポートの作成

ニーズを満たすレポートが見つからない場合は、新しいレポートを作成して必要な方法でデータを提示することができます。

たとえば、ネットワーク上のサーバーにあるオペレーティング システムに関するレポートが必要な場合は次の操作を行います。

1. 左側のウィンドウの **【レポート】** ツリーで、**【レポート】** を右クリックし、**【新規】** → **【レポート】** → **【SQL レポート】** を選択します。



2. [新規 SQL レポート] ページの [データ ソース] タブで、次を入力します。

```
select [OS Name] from DiscoveredMachines
```

3. **【適用】** をクリックします。


検出されたシステムのオペレーティング システムがレポートに表示されます。

---

## 新規 Dell コンピュータ レポートの作成

新しい Dell コンピュータ レポートを作成する方法

1. **【レポート】** ポータル ページで、**【レポート】** を右クリックし、**【新規】** → **【レポート】** → **【コンピュータ レポート】** を選択します。
2. **【データ ソース】** タブの **【クエリ】** サブタブで、**【ベース クエリ】** を選択し、**【ベース リソース タイプ】** ドロップ ダウン メニューから **【Dell コンピュータ】** を選択します。

 **メモ:** このドロップ ダウンからその他の Dell レポートを作成することもできます。

3. **【フィールド】** サブタブで、**【追加】** をクリックして属性を追加します。すべての Dell 属性については、[「インベントリの属性」](#)を参照してください。

 **メモ:** すべての Dell 属性には、Dell Computer または Dell Management Console というプレフィックスが付いています。

4. **【変更を保存する】** をクリックします。

表形式のレポートが表示され、選択したすべての属性が表示されます。

詳細なレポートについては、**【ヘルプ】** → **【マニュアル ライブラリ】** を選択して、Symantec のマニュアルを参照してください。

---

## Dell レポートの編集


すべての Dell レポートはデフォルトで読み取り専用です。これらのレポートを編集するには、最初にレポートを複製してください。

---

## レポートの実行

左側のウィンドウでレポートを選択します。選択したレポートが右側のウィンドウに表示されます。

一部のレポートでは、パラメータを入力できます。これらのレポート パラメータを使用して、選択または入力した値に基づいてレポートをフィルタすることができます。

 **メモ:** "%" 記号はワイルドカードで、文字数が 0 以上の文字列に一致します。

---

## レポートの保存

レポートは複数の形式で保存できます (例: HTML ファイル、XML ファイル、CSV、Web パーツ)。

上記のレポートを Web パーツとして保存する場合は、次の操作を行います。

1. **【新規 SQL レポート】** ページの **【名前を付けて保存】** ドロップ ダウン メニューで、**【Web パーツ】** を選択します。
2. 新しいレポートの名前を **【Web パーツとして保存】** ダイアログ ボックスに入力します。
3. Web パーツのサイズを選択し、**【保存】** をクリックします。

レポートは、Web パーツ フォルダに保存されます。このフォルダにアクセスするには、**【設定】** → **【コンソールの設定】** **【Web パーツ】** メニューを選択します。

この Web パーツを Dell Management ポータル ページに追加するには、「[Dell Management Console ポータル ページの変更](#)」を参照してください。

---

## レポートの表示

レポートを表示する方法

1. Dell Management Console で **【レポート】** → **【すべてのレポート】** → **【Dell レポート】** を選択します。
  2. 表示するレポートをクリックします。
- 

## メトリック レポート

これらのレポートは、デバイス グループの監視メトリックスに使用できます。

1. ピーク電力: デバイスのピーク消費電力値に関する情報を提供します。また時間や単位などの詳細も含まれています。
1. 電力予算: デバイスの電力予算、ヘッドルーム、アイドル状態の電力などの情報を提供します。

ピーク電力と電力予算レポートは表形式で表示されます。

1. スマート メトリック レポート: この機能は Dell Management Console の今後のバージョンで利用可能になります。一定期間にわたるデバイスのメトリック値の傾向に関する情報を提供します。期間、デバイスそしてメトリックを選択して詳細をグラフ形式で表示することができます。グラフのポイントをクリックすると、表にドリルダウンして各デバイスの値を表示することができます。このグラフはスマート メトリック データから派生しています。Dell Management Console を使用して多数のデバイスを管理している場合、グループ メトリックス レポートはグループ データに対してより早い応答を提供しますので、グループを表示するときにはできるだけ使用するようしてください。また、スケジュール オプションを使用してレポートを夜間に行行し、データを朝アクセスできるようにすることもできます。

スマート メトリック レポートがサポートするメトリックス: 電源監視とパフォーマンス モニタ。

スマート メトリック レポートは、Windows オペレーティング システムがあるサーバーの WMI 接続プロファイルと Linux オペレーティング システムがあるサーバーの SNMP 接続プロファイルのパフォーマンス モニタ メトリックスをサポートします。

しかし、スマート メトリック レポートはヘルス メトリックスをサポートしません。


1. グループ メトリック レポート: この機能は Dell Management Console の今後のバージョンで利用可能になります。一定期間にわたるグループのメトリック値の傾向に関する情報を提供します。期間、グループそしてメトリックを選択して詳細をグラフ形式で表示することができます。グラフのポイントをクリックすると、表にドリルダウンしてこのポイントを編成する各デバイスの値を表示することができます。このグラフはグループ メトリック データから派生しています。
- 

## グループ メトリック レポートの表示

カスタム グループのグループ メトリック レポート グループを表示するには、次の操作を行います。

1. Dell Management Console で、**【管理】** → **【組織ビューと組織グループ】** をクリックします。
2. **【組織ビュー】** ページで新しい組織ビューを作成します。
3. 新しく作成された組織ビューの下にグループを作成します (例: group-report)。

4. 新しく作成されたグループの下にサーバーを追加します。
5. 電源監視ポリシーを有効にします。
6. 電源監視ポリシーの **【監視されているターゲット】** 下で **【適用対象】** → **【リソース】** をクリックします。
7. リソースの追加ウィザードの **【Then】** 条件のドロップダウン リストでルールを追加し、**【次の中になリソースを除外する】**、**【グループ】** を選択し、ステップ 3 で作成したグループ レポートを選択します。
8. **【結果のアップデート】** をクリックし、**【名前を付けて保存】** をクリックして名前 (例: GM) を入力し、**【OK】** をクリックします。

 **メモ:** ルールの設定を保存しないとグラフは表示されません。

9. **【監視と警告】** ページで **【メトリック ライブラリ】** を選択します。
10. **【メトリック ライブラリ】** にあるグループ メトリックスには、**【対象 (Target as)】** を選択し、**【適用対象】** → **【すぐに適用する】** をクリックしてグループ (GM) を選択します。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## Dell OpenManage Server Administrator Solution の展開

Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [Deployment Solution について](#)
- [Dell OpenManage Server Administrator の展開ユーザー インターフェイス](#)
- [依存関係](#)
- [その他](#)
- [Server Administrator タスクの展開](#)

Dell™ Management Console の Deployment Solutionは、Dell OpenManage™ ITAssistant のソフトウェア アップデート機能と同様の機能を備えています。

---

### Deployment Solution について

Deployment Solution を使用すると、Dell OpenManage Agent である Dell OpenManage Server Administrator をターゲット システムに簡単にインストールできます。Dell Management Console はこのエージェントと通信を行い、ターゲットシステムのステータスとヘルスをユーザーに通知します。ServerAdministrator の詳細については、Dell サポート Web サイト [support.dell.com](http://support.dell.com) の、『Dell OpenManage Server Administrator ユーザーズ ガイド』を参照してください。

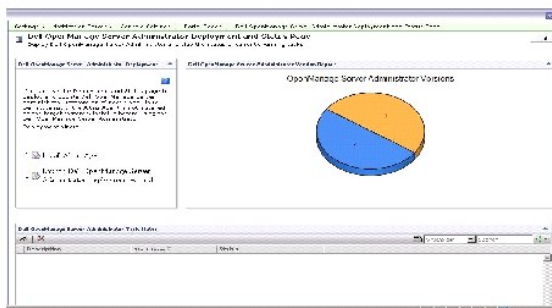
展開タスクには次の機能があります：ソフトウェア パッケージの選択、スケジュールの指定、ソフトウェア パッケージを適用するシステムの指定。Windows および Linux オペレーティング システム固有のパッケージがあります。

---

### Dell OpenManage Server Administrator の展開ユーザー インターフェイス

[ネットワークの検出] タブの [Dell Enterprise Management Quick Start] Web パーツの [Dell Management Console] ポータル ページで [Dell OpenManage Server Administrator の展開] リンクにアクセスできます。

### Dell OpenManage Server Administrator の展開ユーザーインターフェイスの概要



### 依存関係

Dell Management Console から Server Administrator を展開するには、Altiris™ Agent がターゲット システムに存在し、Dell Management Console システムに登録されていることを確認してください。

---

## その他

Server Administrator パッケージ (Microsoft Windows の場合は `sysmgmt.msi`、およびサポートされている Linux オペレーティング システムの場合は `.tar.gz` および対応する `.sign` ファイル) を Systems Management Tools and Documentation DVD または Dell Server Updates DVD から、または Dell サポート Web サイト [support.dell.com](http://support.dell.com) から取得します。

Server Administrator パッケージは、デフォルトで共有ライブラリ フォルダに作成されます。このパッケージには、**[管理]** → **[すべてのリソース]** からアクセスできます。


---

## Server Administrator タスクの展開

ソフトウェア アップデートでは、ソフトウェア アップデート タスクを作成し、管理対象システムに Server Administrator Agent を展開します。

OpenManage Server Administrator を展開する前に、管理対象システムに Altiris Agent がインストールされていることを確認してください。管理対象システムに Altiris Agent をインストールするには、「[管理対象ノードへの Altiris Agent のプッシュ](#)」を参照してください。

Dell Management Console では、Dell システムを管理するために Server Administrator をインストールする必要があります。ソフトウェア アップデート タスクを使用して、Server Administrator バージョン 5.3 以降をインストールまたはアップグレードします。

 **メモ:** Server Administrator バージョン 4.3 以降をターゲット システムに既にインストールしている場合のみ、このタスクを使用してアップグレードできます。

 **メモ:** ターゲット システムから Server Administrator をアンインストールするには、Dell サポート Web サイト [support.dell.com](http://support.dell.com) の『Dell OpenManage Server Administrator ユーザーズ ガイド』を参照してください。

## 管理対象ノードへの Altiris Agent のプッシュ

管理対象ノードへ Altiris Agent をプッシュする方法

1. Dell Management Console を起動します。
2. Dell Management Console で、次のいずれかの操作を行います。
  1. **[アクション]** → **[エージェント/プラグイン]** → **[Altiris Agent のプッシュ]** へとナビゲートします。
  1. **[Dell Management Console]** の **ポータル** ページの **[Dell Enterprise Management Quick Start]** Web パーツで、**[ネットワークの検出]** → **[Dell OpenManage Server Administrator の展開]** を選択し、**[Dell OpenManage Server Administrator の展開とステータスのページ]** で **[Altiris Agent のインストール]** をクリックします。
3. **[コンピュータの選択]** ボタンをクリックします。
4. Altiris Agent をプッシュまたはインストールするコンピュータを選択し、**[OK]** をクリックします。
5. **[Altiris Agent のインストール]** をクリックし、Altiris Agent をインストールするための資格情報を入力し、**[インストールの続行]** をクリックします。

## 管理ステーションからの Server Administrator パッケージの削除

既存の Server Administrator パッケージを Dell Management Console システムから削除するには:

1. **[管理]** → **[すべてのリソース]** をクリックします。
2. Dell OpenManage コンポーネントを検索し、同じ Dell OpenManage バージョンの **ソフトウェアコンポーネント**、**リリース**、**パッケージ** および **製品** を削除します。

Dell OpenManage Server Administrator のインポート済みパッケージを表示するには、検索フィールドに「Dell」と入力します。

## エージェント展開タスクの作成


Windows と Linux オペレーティング システムを使用している場合、エージェントの展開タスクを 2 つ作成する必要があります。1 つはサポートされている Microsoft Windows システムに Server Administrator を展開するタスクで、もう 1 つはサポートされている Linux オペレーティング システムに Server Administrator を展開するタスクです。

1. **[ホーム]** → **[Dell Management Console ポータル]** をクリックします。

**[Dell Enterprise Management]** ページが表示されます。


2. **[Dell Enterprise Management Quick Start]** Web パーツで、**[ネットワークの検出]** タブをクリックします。
3. **[Dell OpenManage Server Administrator の展開]** をクリックします。

**[Dell OpenManage Server Administrator の展開とステータス]** ページが表示されます。

 **メモ:** Server Administrator を展開する前に Altiris Agent をインストールする必要があります。Server Administrator の展開に使用したエージェントを Symantec Notification Server® に登録する必要があります。あるシステムからエージェントをプッシュし、別のシステムから Server Administrator をプッシュした場合、タスクは失敗します。Altiris Agent のインストールの詳細については、Symantec のマニュアルを参照してください。


4. **[Dell OpenManage Server Administrator の展開ウィザードの起動]** をクリックします。
5. **[Dell OpenManage Server Administrator の展開]** ページの「ステップ 1: ソフトウェア パッケージの選択」で、次のいずれかのオプションを選択し、**[次へ]** をクリックします。
  1. **新規 Software Delivery パッケージの作成。**

ローカル システム、CD/DVD、またはネットワーク ロケーションから Server Administrator インストーラを選択してアップロードします。

 **メモ:** このオプションを選択した場合、今後の使用のためにパッケージが Symantec Software Library に作成されます。

1. **既存の Software Delivery パッケージの選択。**

すでにインポートしたパッケージがある場合は、再使用できます。

 **メモ:** Server Administrator バージョン 4.3 以降をターゲット システムに既にインストールしている場合のみ、このタスクを使用してアップグレードできます。


また、Server Administrator を展開するための追加のパラメータを指定することができます。パラメータの詳細については、Dell サポート Web サイト [support.dell.com](http://support.dell.com) で、『Dell OpenManage Server Administrator ユーザーズ ガイド』を参照してください。

6. ウィザードの 2 番目のページで要件に基づき Windows または Linux パッケージを選択し、**[次へ]** をクリックします。
  - a. 次のいずれかのオプションを使用してターゲット システムを選択します。
    1. **クイック追加:** このフィールドにシステム名を入力できます。このオプションは、ターゲットシステムの数が少ない場合に役立ちます。
    1. **追加:** 検出されたシステムのリストからコンピュータを追加します。このオプションは、ターゲットシステムの数が増える場合に役立ちます。

**[コンピュータの選択]** ページが表示されます。

1. **グループの追加:** このオプションは、ターゲット システムの数が多い場合に役立ちます。
  - o Server Administrator を展開するシステムを選択し、**[OK]** をクリックします。
1. ウィザードの 3 番目のページでは、展開スケジュールとランタイム オプションを選択します。

**[今すぐ]** をクリックし、**[Dell OpenManage Server Administrator の展開]** をクリックします。

 **メモ:** タスクがメンテナンス ウィンドウを外れてスケジュールされている場合でもタスクを実行するには、**[ターゲットのメンテナンス ウィンドウのオーバーライド]** オプションを選択します。メンテナンスウィンドウの詳細については、オンライン ヘルプを参照してください。

ソフトウェア アップデートタスクは、タスクを作成するとすぐに実行されます。

ターゲット システムに Adaptec コントローラがある場合、エージェント展開タスクでシステムを再起動する必要があります。

システムを再起動する方法 **[必要に応じてターゲット システムを再起動する]** オプションを選択します。

サポートされている Linux オペレーティング システムを実行しているシステムに Server Administrator を展開する場合は、新しいタスクを作成する必要があります。Server Administrator を Linux システムに展開する場合は、対応する署名ファイルを指定する必要があります。このファイルは、Dell Server Updates DVD に収録されています。

Server Administrator MSI (Windows 用) または tar.gz (Linux用) を初めてアップロードする場合は、Server Administrator ソフトウェア アップデート パッケージが作成され、それ以降のエージェント展開タスクでは、このパッケージを再使用して、Server Administrator を別の Dellシステムに展開できます。

## タスクの詳細の表示

タスクを実行すると、ステータスが [Dell OpenManage Server Administrator **タスク ステータス**] Web パーツの [Dell OpenManage Server Administrator の **展開とステータス**] ページに表示されます。

タスクの詳細を表示するには、タスク インスタンスをダブルクリックします。

後で実行するようにスケジュールされているタスクの場合は、[Dell OpenManage Server Administrator **タスク ステータス**] Web パーツでタスクをダブルクリックして、スケジュールを変更できます。

## Software Library のデフォルト ロケーションの変更

ライブラリ フォルダのロケーションを変更するには、次の操作を行います。

1. ソフトウェア パッケージを保存するフォルダを選択します。
2. ネットワーク上でフォルダを共有し、管理者のみに書き込み許可を与えます。
3. **[設定]** → **[すべての設定]** をクリックします。
4. 左側のウィンドウで、**[設定]** → **[ソフトウェア]** → **[ソフトウェア カタログとソフトウェア ライブラリの設定]** → **[ソフトウェア ライブラリの構成]** を選択します。
5. 右側のウィンドウで、DellManagement Console への新しい共有ライブラリ ロケーションを入力します。

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## ジョブとタスクの管理

Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [ジョブとタスクのユーザー インターフェイス](#)
- [ジョブとタスク モジュールの使用](#)

タスクとは、システム上で実行するアクションのことです。

Dell™ Management Console では、ハードウェアを構成するタスクや、ターゲット デバイスの電源をリセットするタスクなどを実行できます。タスクを実行する場所によって、タスクは次のように分類されます。

- 1 クライアント タスク: クライアント タスクは、Task Server を通じてリモート コンピュータ上で実行されます。クライアント タスクでは常に、サーバーとクライアント セットとの間で通信が行われます (例: Altiris™ 電源制御タスク)。
- 1 Task Server タスク: Task Server タスクは、Symantec™ Management Console 上、または Task Server がインストールされているシステム上で実行できます。すべてのリモート Task Server は、Symantec Management Console に登録されている必要があります (例: コマンド ライン ビルダー タスク)。TaskServer タスクはクライアント タスクに似ていますが、管理対象外のシステム (Altiris Agent がインストールされていないシステム) 上で実行できます。Task Server の詳細については、オンライン ヘルプまたは Symantec のマニュアルを参照してください。

Task Server では、必要に応じて複数のジョブでタスクを再利用したり、タスクを複製および変更したりできます。

- 1 サーバー タスク: サーバー タスクは、Symantec Management Console 上で実行されます。サーバー タスクでも、タスクの目的を達成するために必要な場合は、クライアント セットとの通信が行われます (例: Network Discovery タスク)。

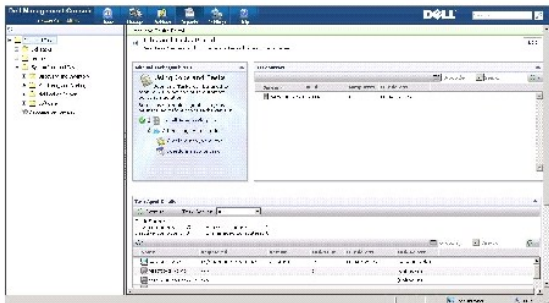
ジョブとは、2 つ以上のタスクを特定のシーケンスで実行するタスクのことです。複雑なシナリオの場合は、ジョブを互いのジョブ内にネストすることで、さまざまな状況下で実行するための前提条件を設定できます。ジョブの作成の詳細については、オンライン ヘルプを参照してください。

---

## ジョブとタスクのユーザー インターフェイス

[ジョブとタスク] ポータル ページへは、**[管理]** → **[ジョブとタスク]** をクリックすることでアクセスできます。

### ジョブとタスクのユーザー インターフェイスの概要




Quick Start: 初めてタスク ソリューションを扱う場合は、右側のウィンドウにある **[ジョブとタスク]** Web パーツを使用することをお勧めします。この Web パーツを使用すると、新しいタスクとジョブを作成して、スケジュールすることができます。

**[タスク コンピュータとデバイス]** Web パーツには、各 Task Server に関連付けられたデバイスのリストが表示されます。Task Server 上のデバイスをソートしたり、デバイスを右クリックしてそのデバイス上で実行されるタスクを表示したりできます。



[Task Server] Web パーツには、Symantec Management Console に登録されているすべての Task Server が表示されます。

左側のウィンドウでは、サンプルのジョブとタスクを表示できます。

 **メモ:** サンプルのタスクは読み取り専用タスクなので、これらのタスクは実行だけを行えます。

初めて Dell タスクを作成すると、Dell Management Console によって [ジョブとタスク] ルート フォルダの下に [Dell タスク] フォルダが作成されます。

---

## ジョブとタスク モジュールの使用

[ジョブとタスク] ポータルを表示するには [管理] → [ジョブとタスク] をクリックします。TaskManagement Solution ([新規タスクの作成] ページ) に、タスクが、ツリー構造およびフォルダでグループ化された状態で表示されます。Dell タスクは、[Dell タスク] フォルダの下でグループ化されます。

タスクは、30 分ごと、1 時間ごと、勤務時間内、毎日、毎週、毎月またはカスタム定義の間隔で実行するようにスケジュールできます。共有スケジュールにより、時刻、開始日、終了日および反復実行を指定できます。たとえば、毎日、1 度だけ、毎週、毎月、ログオン時、システムの起動時に実行するように指定できます。

タスクは、1 つまたは複数のデバイス、または 1 つまたは複数のコレクションに対して実行できます。スケジュールされたタスクの場合、入力された資格情報は保存されるので、ユーザーの介入なしにタスクを実行できます。

Dell Management Console には、シャットダウン(電源制御デバイス)、ウェイク アップ (電源制御)、コマンド ライン(スクリプトの実行) およびリモート コマンド ライン (コマンド ライン ビルダー) などの、定義済みのサンプル タスクが用意されています。これらのサンプルタスクを使用したり、タスクパラメータを適切に構成することで変更したりできます。

 **メモ:** [スクリプトの実行] を実行する前に、Altiris Agent を管理対象システム上にインストールします。

[新規タスクの作成] ページの [Dell タスク] フォルダ内にリストされているすべてのタスクは、[Dell デバイスの関連付け] タスクを除き、[サーバー ジョブ] および [クライアント ジョブ] の一部として追加できます。

[Dell デバイスの関連付け] タスクは、[サーバー ジョブ] にのみ追加できます。

Dell タスクについては、オンライン ヘルプを参照してください。

## タスクのスケジュール

システムのグループに対して、1 年間 6 月を除いた毎月第 3 土曜日の午後 6 時にシャットダウンするといったタスクをスケジュールするには、次の手順に従います。

1. [管理] → [ジョブとタスク] をクリックして、[ジョブとタスクのポータル] を表示します。
2. [ジョブとタスクの Quick Start] Web パーツで、[新規ジョブまたはタスクの作成] をクリックします。
3. [新規タスクの作成] ページで、[電源制御デバイス] タスクを選択します。
4. [シャットダウン] を選択し、[OK] をクリックします。

[電源制御デバイス - シャットダウン] タスクが作成され、[Task Server タスク] → [Dell タスク] フォルダの下に表示されます。

5. 左側のウィンドウにある [ジョブとタスク] ツリーから [電源制御デバイス - 電源オフ] タスクを選択します。

詳細が右側のウィンドウに表示されます。

6. [タスクのステータス] ウィンドウで、[新規スケジュール] を選択し、[タスクのスケジュール] ページで次の設定を構成します。

スケジュール: 共有スケジュール

共有スケジュールの選択: 月単位

[新規] をクリックします。

7. [新規共有スケジュールの作成] ページで、スケジュールの名前と説明を入力します。


[スケジュールの追加] → [予定開始時刻] を選択し、シャットダウン タスクの開始時刻として 1800 時間を選択します。

[繰り返しのスケジュール] 画面で [繰り返しなし] をクリックし、[月 (選表示)]、[第3 週] および [土曜日] を選択します。


[年 (選表示)] を選択し、6 月を除くすべての月を選択します。

8. [新規共有スケジュールの作成] ページで、[高度] をクリックし、このタスクの通年での開始日と終了日を選択し、[OK] をクリックします。
9. [新規スケジュール] ページで、[追加] をクリックして、このタスクを実行するコンピュータまたはコンピュータのグループを選択します。
10. [電源制御デバイス - シャットダウン] タスク ページで、[変更を保存する] をクリックします。

シャットダウン タスクが作成され、6 月を除く毎月の第 3 土曜日、午後6 時に実行されるようにスケジュールされます。

 **メモ:** 一部のシステムで [電源制御デバイス - シャットダウン] タスクをすぐに実行するには、[タスクのステータス] ウィンドウで、[クイック実行] をクリックし、そのシステムを選択します。

## SNMP の設定タスクの作成

 **メモ:** このタスクは、Windows オペレーティング システムを実行中の管理対象システムでのみ設定することができます。

SNMP の設定タスクを使用して、セキュリティ、トラップ、およびエージェントなどの SNMP サービス プロパティを設定することができます。


1. [管理] → [ジョブとタスク] をクリックして、[タスク管理ポータル] を表示します。
2. [ジョブとタスクの Quick Start] Web パーツで、[新規ジョブまたはタスクの作成] をクリックします。
3. [新規タスクの作成] ページの [Dell タスク] → [その他] フォルダで、[SNMP の設定] タスクを選択します。
4. 右のウィンドウの [SNMP タスクの設定] で、[SNMP サービス プロパティを追加または変更する] を選択します。
5. [セキュリティ] をクリックしてコミュニティのセキュリティ プロパティを設定します。
6. [SNMP サービス セキュリティのプロパティ] ページで受け入れられているコミュニティ名を追加し、Dell Management Console が SNMP パケットをホストから受け入れるべきかを指定します。

ID に関係なくネットワーク上の任意のホストから SNMP の要求を受け入れるには、[任意のホストからの SNMP パケットを受け入れる] をクリックします。


Dell Management Console Server から SNMP パケットの受け入れを制限するには、[これらのホストからの SNMP パケットを受け入れる] をクリックして [追加] をクリックし、ホスト名、IP または IPX アドレス ボックスに Dell Management Console server ホスト名または IP アドレスを入力します。

7. [SNMP タスクの設定] セクションで [トラップ] をクリックし、コミュニティ名を指定してトラップの送信先を設定します。
8. [SNMP タスクの設定] セクションで [エージェント] をクリックし、エージェントの物理ロケーションとこのエージェントの担当者を指定します。
9. [OK] をクリックして [SNMP の設定タスク] を作成します。

このタスクは、[Dell タスク] の下の [ジョブとタスク] ポータル ページに表示されます。

 **メモ:** このタスクを実行する前に、SNMP サービスを管理対象システムで有効にする必要があります。


10. システムのグループに対してタスクを実行するには、[新規スケジュール] をクリックします。
11. [新規スケジュールの作成] ページで、[今すぐ] を選択します。
12. [選択したデバイス] セクションで、[追加] をクリックし、このタスクを実行するデバイスを追加します。

 **メモ:** 変更を反映するには、管理対象システムで SNMP サービスを再起動する必要がある場合があります。

## 管理対象システム上で Server Administrator コマンドを実行するためのコマンドラインビルダータスクの作成

コマンドラインビルダータスクとは、Remote Server Administrator タスク、IPMI タスク、または Remote Access Controllerタスクなどの定義済みのタスクのことです。このタスクでは、定義済みのパラメータまたはコマンドのセットを使用して、1 つまたは複数の管理対象システムに対し、実行可能ファイルを実行できます。

コマンドラインビルダータスクを作成して、管理対象システムグループのシステムシャーシ、オペレーティングシステム、ソフトウェアプロファイルおよびハードウェアプロファイルの情報など、システム情報の概要を表示するとします。

 **メモ:** DellManagement Console でこのデータをフェッチできるように、Server Administrator を管理対象システム上にインストールする必要があります。


1. **【管理】** → **【ジョブとタスク】** をクリックして、**【タスク管理ポータル】** を表示します。
2. **【ジョブとタスクの Quick Start】** Web パーツで、**【新規ジョブまたはタスクの作成】** をクリックします。
3. **【新規タスクの作成】** ページの **【Dell タスク】** → **【その他】** フォルダで、**【コマンドラインビルダー】** タスクを選択します。
4. **【コマンドラインタイプ】** で、**【Remote Server Administrator】**、**【omreport】** の順に選択します。

**【追加】** をクリックします。


**【システム】** を選択し、**【追加】** をクリックします。


**【概要】** を選択し、**【追加】** をクリックします。


または、**【コマンド構文】** で、`omreport system summary` と入力します。

 **メモ:** ドロップダウンリストから選択できるパラメータは最大で 4 つです。4 つ選択すると、パラメータは動的に表示されなくなります。

5. **【高度...】** をクリックして、ユーザー資格情報を入力し、出力をキャプチャするログファイルへのパスを指定して **【OK】** をクリックします。

 **メモ:** 資格情報を指定しない場合、タスクではシステムログインの資格情報を使用して、管理対象デバイスとの通信を行います。

 **メモ:** タスクでは、管理ステーションのシステムログイン資格情報を使用して管理対象デバイスと通信します。したがって、サポートされている Linux オペレーティングシステムを実行している管理対象システムの資格情報を指定しない場合、タスクは失敗し、複数の「アクセスが拒否されました」というメッセージが表示されます。


 **メモ:** このタスクを Linux 上で実行している管理対象システムに対して作成している場合は、**【タスクオプション】** タブを選択してから **【SSH ポート番号】** を指定し、**【Linux 用の信頼されたキーの生成】** を選択する必要があります。

コマンドラインビルダータスクは、**【Dell タスク】** フォルダの下に表示されます。

6. システムのグループに対してタスクを実行するには、**【新規スケジュール】** をクリックします。
7. **【新規スケジュールの作成】** ページで、**【今すぐ】** を選択します。
8. **【新規スケジュール】** ページで、**【追加】** をクリックし、このタスクを実行するデバイスを追加します。

## 管理対象システム上で Remote Access Controller コマンドを実行するためのコマンドラインビルダータスクの作成

管理対象システム上で、Remote Access Controller コマンドを実行するためのコマンドラインビルダータスクを作成するとします。

 **メモ:** Dell Management Console でこれらのコマンドを実行できるようにするには、Dell Remote Access Controller が管理対象システム上に存在する必要があります。


1. **【管理】** → **【ジョブとタスク】** をクリックして、**【タスク管理ポータル】** を表示します。
2. **【ジョブとタスクの Quick Start】** Web パーツで、**【新規ジョブまたはタスクの作成】** をクリックします。

3. **【新規タスクの作成】** ページの **【Dell タスク】** → **【その他】** フォルダで、**【コマンドラインビルダー】** タスクを選択します。
4. **【コマンドラインタイプ】** で、**【Dell OpenManage Remote Access Controller】**、**【setniccfg】** の順に選択します。


**【追加】** をクリックします。

`[-s]` を選択し、値 `192.168.0.120 255.255.255.0 192.168.0.1` を入力して **【追加】** をクリックします。

または、**【コマンド構文】** で、`setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1` と入力します。

 **メモ:** ドロップダウンリストから選択できるパラメータは最大で4つです。4つ選択すると、ドロップダウンには動的に表示されなくなります。

5. **【高度...】** をクリックして、ユーザー資格情報を入力し、ログファイルへのパスを指定して **【OK】** をクリックします。

 **メモ:** 資格情報を指定しない場合、タスクでは工場出荷時のデフォルト資格情報を使用して、管理対象デバイスとの通信を行います。

コマンドラインビルダータスクは、**【Dell タスク】** フォルダの下に表示されます。

6. システムのグループに対してタスクを実行するには、**【新規スケジュール】** をクリックします。
7. **【新規スケジュールの作成】** ページで、**【今すぐ】** を選択します。
8. **【新規スケジュール】** ページで、**【追加】** をクリックし、このタスクを実行するデバイスを追加します。

## Dell デバイスの関連付けタスクの作成

**【Microsoft Active Directory のインポート】** または **【ドメインメンバーシップ/WINS のインポート】** タスクを使用するか、またはターゲットデバイスに Altiris Agent をプッシュすることでデバイスを検出すると、Dell デバイスとしては分類されません。

Active Directory のインポートまたはドメインリソースでデバイスを検出する方法の詳細については、『Dell Management Console オンラインヘルプ』を参照してください。

各検出対象デバイスに接続プロファイルを関連付け、これらのデバイスを Dell デバイスとして分類します。


接続プロファイルには、検出とインベントリのモジュールがデバイス上のリモートエージェントと通信を行うために必要なプロトコル設定と資格情報が含まれています。これらの関連付けがない場合、デバイスの検出とインベントリは正常に実行されないおそれがあります。ネットワークトポロジやプロトコル設定の変更を反映させ、新しいデバイスの関連付けを作成するには、Dell デバイスの関連付けタスクを定期的に行うように設定してください。

このタスクを作成するには:

1. **【管理】** → **【ジョブとタスク】** をクリックして、**【タスク管理ポータル】** を表示します。
2. **【ジョブとタスクの Quick Start】** Web パーツで、**【新規ジョブまたはタスクの作成】** をクリックします。
3. **【新規タスクの作成】** ページの **【Dell タスク】** → **【その他】** フォルダで、**【Dell デバイスの関連付け】** タスクを選択します。
4. 右側のウィンドウで、デフォルトの接続プロファイルを選択し、**【選択した接続プロファイルを関連付けるターゲットデバイスを選択します】** で、**【Microsoft Active Directory のインポート】** または **【ドメインメンバーシップ/WINS のインポート】** タスクを通じて検出されたデバイスを選択します。
5. **【適用対象】** → **【リソース】** を選択します。
6. **【リソースの選択】** ページで、**【次に】** ドロップダウンから **【ルールの追加】** をクリックし、**【リソースリストにないリソースを除外する】** を選択し、省略記号 (...) をクリックします。
7. **【利用できるリソース】** の **【グループ】** で、タスクを実行するデバイスを選択し、**【OK】** をクリックします。

選択したデバイスの数が、**【新規タスクの作成】** ページに表示されます。

8. タスクをすぐに実行するようにスケジュールします。

 **メモ:** **【Dell デバイスの関連付け】** はサーバータスクなので、Symantec Management Console 上のみ作成し、実行することができます。そのため、**【クイック実行】** および **【ターゲットの選択】** オプションは、**【新規スケジュール】** に表示されません。

このタスクの実行結果を表示するには:

1. **【管理】** → **【すべてのリソース】** をクリックします。
2. これに関連付けられた Dell デバイスが、**【組織ビュー】** → **【すべてのデバイス】** に表示されます。

## Dell タスクのロールアウト ポリシー

複数の階層を持つ大規模なエンタープライズを管理しているときに、ネットワーク上のデバイスをモニタする場合は、複数のシステム上に Task Server をインストールすることで、Symantec Management Console の 負荷を軽減することができます。こうすることで、Altiris Agent が最も近い Task Server にアクセスしてジョブとタスクをダウンロードできるため、ネットワークトラフィックも低減されます。

階層関係の作成と管理については、オンライン ヘルプを参照してください。

複数の階層を持つ Task Server アーキテクチャをサポートするには、Dell タスクによって、登録済みのすべての Task Server 上で Dell タスクのロールアウト ポリシーを実行する必要があります。

Dell タスクのロールアウト ポリシーを登録済みのすべての Task Server で実行するには、次を行います。

1. ビルトイン コレクションを使用しているすべての Task Server をターゲットとするロールアウト ポリシーを手動で有効にします。
1. ロールアウト ポリシーを有効にしたら、次のポーリング間隔でタスクのコンポーネントが展開されるまで待ちます。

## Site Server (Task Server) の Notification Server コンピュータへの登録

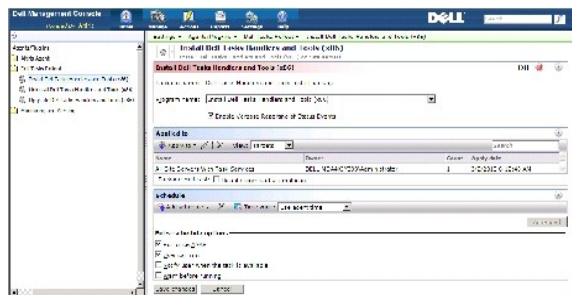
1. **【設定】** → **【Notification Server】** → **【Site Server の設定】** をクリックします。
2. 左側のウィンドウで、**【サイトの管理】** 一覧を展開します。
3. Task Server が表示されていない場合は、**【新規】** → **【Site Server】** をクリックします。
4. **【利用可能なコンピュータ】** のリストから **【Site Server】** を選択し、**【OK】** をクリックします。
5. このサーバーで稼働させるサービスを選択します。

ここで、サーバーをタスク サービス用の SiteServerとして適切に構成する必要があります。


**【ジョブとタスク】** ポータル (**【管理】** → **【ジョブとタスク】**) の **【Task Server】** Web パーツには、Notification Server コンピュータに登録されているすべての Task Server が表示されます。Notification Server および Task Server が同じシステム上にある場合、コンピュータの数は 1 と表示されます。

## Dell タスクのロールアウト ポリシー タスクの作成


1. **【アクション】** → **【エージェント/プラグイン】** → **【エージェント/プラグインのロールアウト】** をクリックします。
2. **【Dell タスクのロールアウト】** フォルダで、**【Dell タスク ハンドラとツールをインストールする】** を選択します。
3. 右側のウィンドウで、**【プログラム名】** として、**【Dell タスク ハンドラとツールをインストールする】** を選択します。



4. **【適用対象】** → **【コンピュータ】** をクリックします。

 **メモ:** Task Server の要件を満たしているタスクにのみポリシーを適用できます。詳細については、オンライン ヘルプを参照してください。

5. [コンピュータの選択] 画面で、[ルールを追加] をクリックします。
6. [次に] ドロップダウンメニューで、[次の中のコンピュータを除外する] を選択してから[コンピュータリスト] を選択し、(...) をクリックします。
7. Task Server として含めないコンピュータを選択し、[OK] をクリックします。
8. [Dell 上級タスク ハンドラのインストール] ページで、タスクのスケジュールを入力し、[変更を保存する] をクリックします。

 **メモ:** 同じ手順を使用して、Dell 構成タスク ハンドラのインストール タスクを作成できます。

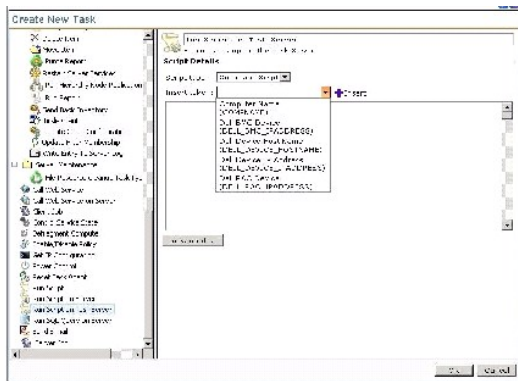
ポリシーにより、タスクが内部的に作成され、タスクのコンポーネントが展開されます。

## タスクトークン

トークンは項目であり、特定のインスタンスを除き、値を持ちません。DellManagement Console では、定義済みトークンを使用してコマンドライン タスクを作成できます。これらのトークンは、タスクが実行されるときに、ターゲット デバイスに対応する実際の値と置き換えられます。

Dell Management Console には、次の定義済みトークンが用意されています。

- 1 %DELL\_BMC\_IPADDRESS%
- 1 %DELL\_DEVICE\_HOSTNAME%
- 1 %DELL\_RAC\_IPADDRESS% および
- 1 %DELL\_DEVICE\_IPADDRESS%



上記トークンを使用してタスクを作成する方法

1. [管理] → [ジョブとタスク] をクリックして、[タスク管理ポータル] を表示します。
2. [ジョブとタスクの Quick Start] Webパーツで、[新規ジョブまたはタスクの作成] をクリックします。
3. [新規タスクの作成] ページで、[Task Server でのスクリプトの実行] タスクを選択します。
4. 右側のウィンドウで、[スクリプトタイプ] を選択します。
5. コマンドスクリプト テキストを入力し、定義済みの Dell トークンを選択します。
6. [挿入] をクリックしてスクリプト テキスト内にトークンを挿入し、[OK] をクリックします。
7. タスクが作成され、左側のウィンドウにある [ジョブとタスク] フォルダの下に表示されます。

**タスクトークンを使用したスクリプトの実行タスクを作成して、管理対象ストレージ システム上でスクリプトまたはコマンドを実行する**

[Task Server でのスクリプトの実行] タスクを作成して Naviseccli コマンドを実行し、管理対象ストレージ システムのグループでパフォーマンス ログ記録プロパティの現在値を取得できます。

**メモ:** 管理対象ストレージ システムで、Navisecli コマンドがサポートされていることを確認する必要があります。リモートのストレージ システム上で Navisecli コマンドを実行するために、管理ステーションを構成します。

1. **【管理】** → **【ジョブとタスク】** をクリックします。
2. **【ジョブとタスクの Quick Start】** Webパーツで、**【新規ジョブまたはタスクの作成】** をクリックします。
3. **【新規タスクの作成】** ページで、**【TaskServer でのスクリプトの実行】** タスクを選択します。
4. **【スクリプト タイプ】** で、**【コマンド スクリプト】** を選択します。
5. スクリプト テキストに、次のコマンド構文を入力します。

```
"C:\NaviCLITool\navisecli.exe" -h -AddUserSecurity -password mypass -scope 0 -user Tom analyzer -get -narinterval
```

6. **【トークンの挿入】** ドロップ ダウン メニューから、**DELL\_DEVICE\_IPADDRESS**トークンを選択し、**【挿入】**をクリックして、このトークンを **-h** オプションの後のスクリプト テキスト内に挿入し、**【OK】** をクリックします。

コマンドは次のように表示されます。

```
"C:\NaviCLITool\navisecli.exe" -h%DELL_DEVICE_IPADDRESS% -AddUserSecurity -password mypass -scope 0 -user Tom analyzer -get -narinterval
```

7. タスクが作成され、左側のウィンドウにある**【ジョブとタスク】**フォルダの下に表示されます。
8. 管理対象ストレージ システムのグループに対してタスクを実行するには、**【新規スケジュール】**をクリックします。
9. **【新規スケジュールの作成】** ページで、**【今すぐ】** を選択します。
10. **【新規スケジュール】** ページで、**【追加】** をクリックし、このタスクを実行する管理対象ストレージ システムを追加します。
11. タスクが実行されると、%DELL\_DEVICE\_IPADDRESS%トークンは、各ターゲット ストレージ システムの実際の IP アドレスに置き換えられます。

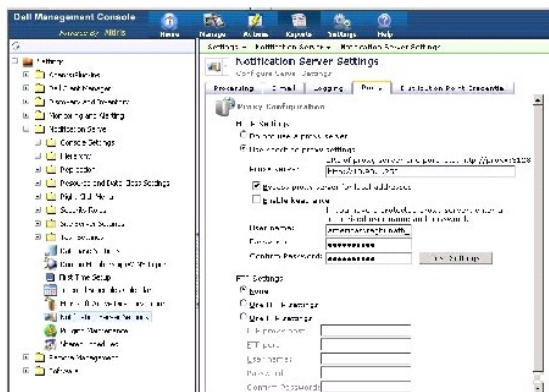
## 保証の抽出タスクの作成

保証の抽出タスクは、管理対象デバイスの保証情報をサービス タグを使用して抽出するために使用するサーバー タスクです (特に DellPowerEdge™ システム、Dell PowerConnect™ スイッチ および DRAC/CMC)。このタスクは、Dellサポート Web サイトから保証情報を取得します。

保証情報の抽出タスクを正常に実行するには、Dell Management Console が Dellサポート Web サイトへ接続できることを確認します。


プロキシ設定を構成しテストする方法

1. **【設定】** → **【すべての設定】** をクリックします。
2. 左のウィンドウで、**【Notification Server】** → **【Notification Server の設定】** をクリックします。
3. 右のウィンドウで **【プロキシ】**タブをクリックしてプロキシ設定を構成します。




保証の抽出タスクを作成するには:

1. **【管理】** → **【ジョブとタスク】** をクリックして、**【タスク管理ポータル】** を表示します。
2. **【ジョブとタスクの Quick Start】** Web パーツで、**【新規ジョブまたはタスクの作成】** をクリックします。
3. **【Dell ユーティリティ】** フォルダの下での**【新規タスクの作成】** ページで、**【保証の抽出】** タスクを選択します。
4. 右のウィンドウで、新しく検出されたデバイスの保証情報を取得する日数を入力します。

 **メモ:** 保証の抽出タスクを初めて実行する場合、このタスクはすべての管理対象デバイスの保証情報を取得します。次の実行からは、新しく検出されたデバイス（最初のタスク実行後に Dell Management Console で検出されたデバイス）の情報を取得します。古い保証情報（60日以上前に取得された保証情報）も更新します。

**【既存の保証情報をすべて削除する】** を選択してすべての保証情報を更新するか、**【情報を取得する日数】** に値を入力して部分的に更新することができます。

 **メモ:** 保証レポートに取得した情報が表示されない場合は、プロキシ設定が正しく有効化されているかを確認し、この後のすべてのレポートに対し **【既存の保証情報をすべて削除する】** のオプションを選択する必要があります。

5. Dell Management Console が多数のデバイスを管理している場合、保証の抽出タスクが完了するまで時間がかかる可能性があります。タスクが長時間実行されている場合、タスクが情報を取得して処理するサイズを指定（**【一度に情報をアップデートするデバイス数】** フィールドで指定）することができます。

**【保証レポート】** をクリックし、指定した数のデバイスの分の取得情報を表示することができます。

6. **【OK】** をクリックします。

このタスクは、**【システム ジョブとタスク】** → **【Notification Server】** の下の **【ジョブとタスク】** ポータル ページに表示されます。

7. システムのグループに対してタスクを実行するには、**【新規スケジュール】** をクリックします。
8. **【新規スケジュールの作成】** ページで、**【今すぐ】** を選択します。

Dell Management Console デバイス リストから削除され、すでに Dell Management Console によって管理されていないデバイスに関する履歴情報を表示することができます。この情報は、保証の抽出タスクを実行する度に保証レポートでアップデートされ、**【デバイス ステータス】** の列に表示されます。

---

[目次のページに戻る](#)



[目次のページに戻る](#)

## Dell™ Management Console Version 1.1 ユーザーズ ガイド



**メモ:** メモには、コンピュータのより良い使用に役立つ重要な情報が示されています。



**注意:** 注意には、使用説明書に従わなかった場合に被る可能性のあるハードウェアの障害またはデータの損失について示されています。

警告には、物的損害、人的傷害または死に至る可能性のあることについて示されています。

**このドキュメント内の情報は、予告なしに変更されることがあります。**

©2010DellInc.Allrightsreserved.

どのような形式であってもDell Inc. の書面による許可なしにこれらの資料を複製することは厳しく禁じられています。

このテキストで使用されている商標: Dell, DELL ロゴ, PowerEdge, PowerVault, PowerConnect, OpenManage, および EqualLogic は、Dell Inc. の商標です。Microsoft, Windows, およびWindows Server は、米国または他の国、あるいはその両方におけるMicrosoftCorporationの商標または登録商標です。Altiris, Symantecおよび Notification Server は、Symantec Inc.の商標または登録商標です。Brocade, Itrrepid および McData は、Brocade Communications Systems, Inc.の商標です。

その他の商標および商号は、それらの商標と商号またはその製品であることを明確にするため、このドキュメント内で使用される場合があります。Dell Inc. は、所有していない商標と商号において、一切の所有権を放棄します。

2010 年 3 月

---

[目次のページに戻る](#)

[目次のページに戻る](#)

## Dell Management Console の

### ユーザーインターフェイス


Dell™ Management Console Version 1.1 ユーザーズ ガイド

- [\[ホーム\] メニュー : Dell Management Console ポータルページ](#)
- [アプリケーションの起動](#)

この章では、Dell™ Management Console のユーザー インターフェイス (UI) の外観について説明します。

Symantec™ Notification Server® の基礎となるフレームワークによって、豊富なコントロールを備えた動的なユーザー インターフェイスが提供されます。

Dell Management Console は、C:\Program Files\Dell\Systemgt\dmc にあります。起動アイコンは、[スタート] ボタン → [プログラム] → [Dell OpenManage Applications] → [Dell Management Console] → [Dell Management Console] にあります。

 **メモ:** Secure Socket Layer (SSL) が Dell Management Console に対して有効になっている場合は、デスクトップおよび [スタート] メニューのショートカットが新しい SSL ロケーションをポイントするように編集します。例: <https://localhost/Dell/console>

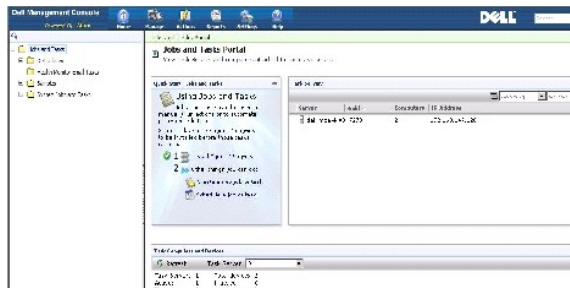
Dell Management Console はメニュー方式で、次の 6 つのメニューで構成されています。

- 1 ホーム
- 1 管理
- 1 アクション
- 1 レポート
- 1 設定
- 1 ヘルプ

それぞれの機能に基づいて、各メニューの下にサブメニューがグループ化されています。Dell Management Console のサブメニューの例は次のとおりです。

- 1 **[ホーム]** メニューには、Dell Management Console ポータルのサブメニューがあります。プラグインをインストールすると、それぞれのポータルがこのメニューの下で利用可能になります。
- 1 **[管理]** メニューには、コンピュータ、ユーザー、リソースからタスクおよびイベントを管理できる、すべてのコンポーネントがあります。
- 1 **[アクション]** メニューには、検出、インベントリ、モニタリングおよびエージェントの展開などの、ネットワーク デバイス上で実行するアクションがあります。
- 1 **[レポート]** メニューには、Dell Management Console のすべての利用可能なレポートがあります。
- 1 **[設定]** メニューには、セキュリティ、SymantecNotification Server および Dell Management Console を構成するためのサブメニューがあります。
- 1 **[ヘルプ]** メニューでは、オンライン ヘルプやその他のマニュアルへのリンクにアクセスできます。このメニューから、すべての機能についての情報を検索できます。

サブメニューを選択するとページが表示され、このページの左側のツリー構造をナビゲートすることができます。右側には、データをグラフィカルに表示するさまざまな Web パーツがあります。たとえば、[ジョブとタスク] ポータル ページでは、左側のウィンドウにツリー構造が表示されます。右側のウィンドウには [Quick Start - ジョブとタスク]、[Task Server] および [タスク コンピュータとデバイス] Web パーツが表示されます。

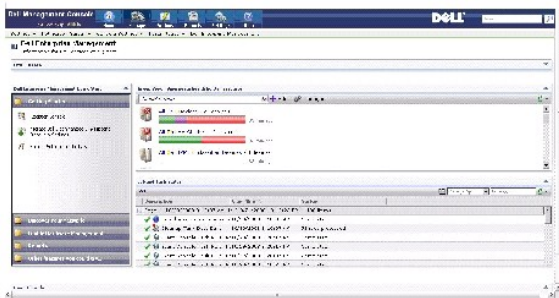


---

## [ホーム] メニュー : Dell Management Console ポータルページ

Dell Management Console には、ネットワーク上の Dell デバイスを管理および監視する際に、ダッシュボードやタスクに簡単にアクセスするためのポータル ページが用意されています。このページへは、**[ホーム]** → **[Dell Management Console ポータル]** からアクセスできます。

このポータル ページには、デバイスのヘルス、タスクのステータス、警告などの Web パーツがあります。



Dell Management Console の使用をするには、**[Dell Enterprise Management Quick Start]** Web パーツを選択します。この Web パーツ上で利用できるさまざまなタブから、Dell Management Console を構成することができます。

**[Dell Enterprise Management Quick Start]** Web パーツから、次の操作を行うことができます。

- 1 Dell OpenManage™ IT Assistant からの検出範囲の移行
- 1 ネットワーク上のデバイスの検出とそれらの監視
- 1 検出済みのデバイスのインベントリの収集とアップデートの適用
- 1 Dell 固有のレポートの使用または新規レポートの作成

## Dell Management Console ポータル ページの変更

ポータル ページから Web パーツを追加したり移動したりできます。

1. **[Dell Management Console ポータル]** ページの右上隅で、**[編集]** を選択します。

 **メモ:** このページの **[編集]** ボタンは、Dell Management Console を Dell の Web サイト [dell.com/openmanage/register](http://dell.com/openmanage/register) で登録した場合にのみ表示されます。

2. **[Web パーツの選択]** で、ポータルページ上で表示する Web パーツを選択し、**[追加]** をクリックします。

選択した Web パーツがポータル ページに追加されます。Web パーツは、ポータル ページ上の任意の場所にドラッグ アンドドロップできます。

3. **[適用]** をクリックします。

---

## アプリケーションの起動

Dell Management Console から他のアプリケーションを起動することができます。検出されたデバイスのタイプに応じて、Dell Management Console は、デバイスのシステム管理アプリケーション用に、統合された起動ポイントを提供します。

デバイスのアプリケーションを起動するには、次のオプションから選択します。

- 1 [管理] メニュー
- 1 リソース マネージャ
- 1 [設定] メニュー
  - 1 Dell OpenManage Network Manager
  - 1 Dell OpenManage RAC Console

## 管理メニュー

1. Dell Management Console で、**[管理]** → **[すべてのデバイス]** をクリックします。
2. **[すべてのデバイス]** ページで、サーバーなどのデバイスを開いて右クリックし、**[管理アプリケーション]** を選択します。

**[Dell OpenManage Server Administrator]**、**[SOL プロキシ]** および **[Telnet]** などの、システム管理アプリケーションのオプションが表示されます。

これらのアプリケーションを起動して適切なアクションを実行できます。

接続プロファイルによっては、デバイスで利用できるオプションが異なる場合があります。たとえば、SNMPプロトコルを使用してデバイスを検出した場合、次のオプションを利用できます。

- 1 Dell OpenManage Server Administrator
- 1 Dell Remote Access Controller (DRAC) が存在するシステムの場合は RAC Console
- 1 DRAC が存在するシステムの場合は RAC Telnet
- 1 リモート デスクトップ (Microsoft® Windows® システムのみ)
- 1 SOL プロキシ
- 1 Telnet
- 1 EqualLogic

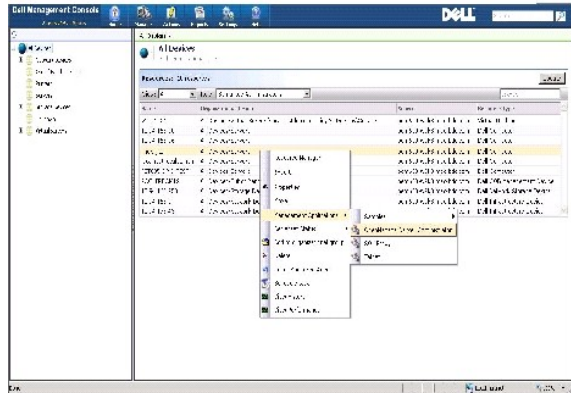
一方、WMI プロトコルを使用してデバイスを検出した場合、次のオプションを利用できます。

- 1 Dell OpenManage Server Administrator
- 1 リモート デスクトップ
- 1 SOL プロキシ
- 1 Telnet

IPMI では次のオプションを利用できます。

- 1 SOL プロキシ
- 1 Telnet

接続プロファイルの詳細については、「[新しい接続プロファイルの作成](#)」および「[デフォルトの接続プロファイルの編集](#)」を参照してください。



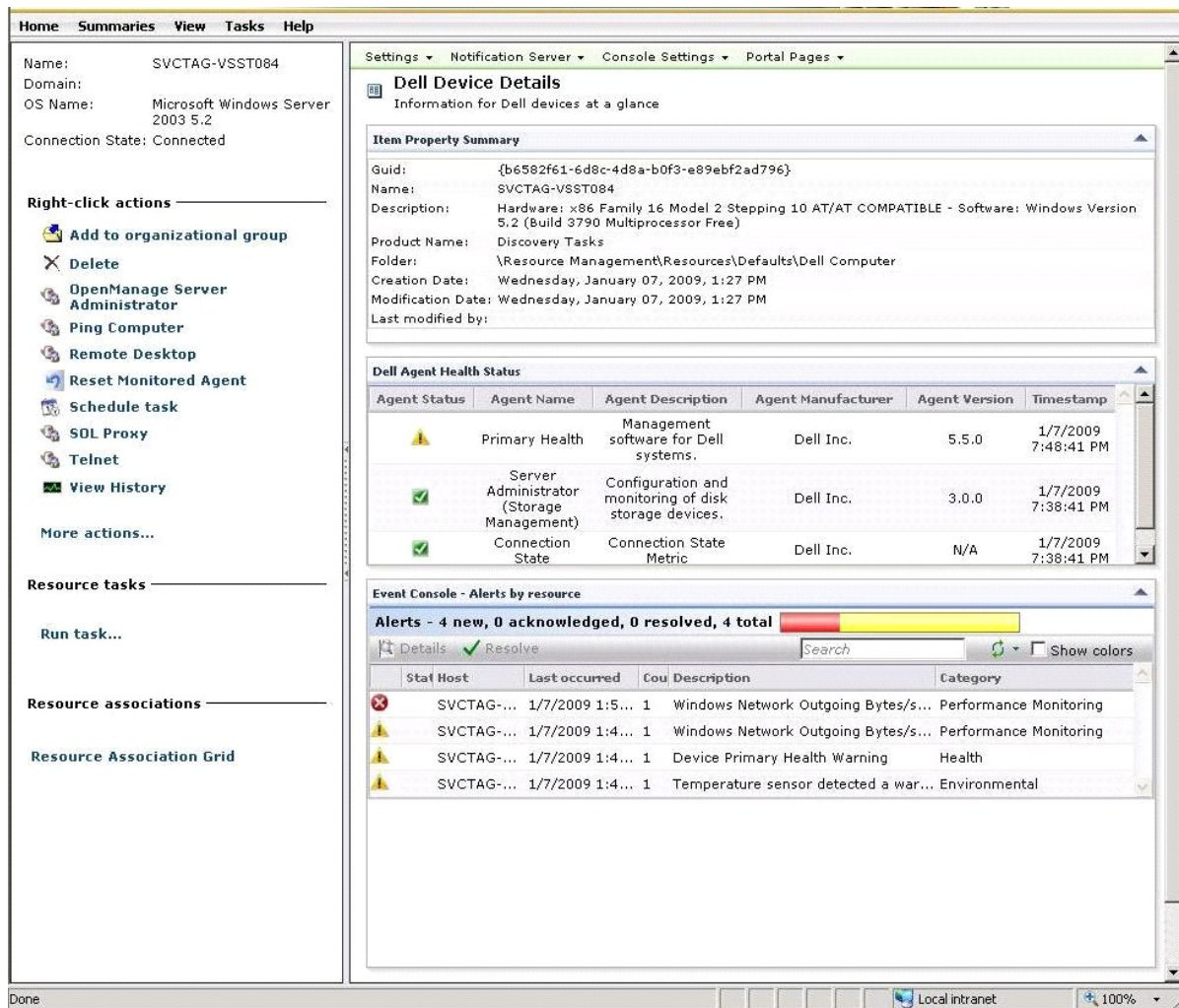
## リソース マネージャ

1. **【管理】** → **【すべてのデバイス】** をクリックします。
2. **【すべてのデバイス】** ページで、サーバーなどのデバイスを右クリックし、**【リソース マネージャ】** を選択します。

デバイス名をダブルクリックして、リソース マネージャにアクセスすることもできます。

3. **【リソース マネージャ】** ページには、このデバイスのハードウェア、フィルタおよびポリシーの概要、このデバイスにスケジュールされているタスクのカレンダーなど、デバイスに関するすべての情報が表示されます。

**【リソース マネージャ】** ページの左ウィンドウの **【右クリック アクション】** には、デバイスのシステム管理アプリケーションが表示されます。



## [設定] メニュー - Dell OpenManage Network Manager

1. Dell Management Console で、[設定] → [コンソール] → [右クリック アクション] を選択します。
2. [管理アプリケーション] ウィンドウで、アプリケーションをクリックします。例として Dell OpenManage Network Manager アプリケーションをクリックします。

Dell OpenManage Network Manager ページが表示されます。


**メモ:** このアプリケーションは、インフラストラクチャ デバイス用の右クリック オプションであるため、[リソース タイプ] は [Dell インフラストラクチャ デバイス] と表示されます。

ネットワーク デバイスのリソース タイプについては、[表4-1](#) を参照してください。


表 4-1. Dell デバイスのリソース タイプ

Dell デバイス	リソース タイプ
Dell PowerEdge™ システム	Dell コンピュータ
プリンタ	Dell プリンタ
Dell EMC	Dell ネットワーク ストレージ デバイス
テープ	Dell ネットワーク バックアップ デバイス
Dell PowerConnect™/KVM/ファイバ チャネル スイッチ	Dell インフラストラクチャ デバイス
Dell Remote Access Controller	Dell OOB (アウト オフ バンド) 管理デバイス

Dell PowerVault™ MD アレイ	Dell ネットワーク ストレージ デバイス
Dell EqualLogic グループ	

 **メモ:** デバイスのリソースタイプは変更しないことをお勧めします。

3. このアプリケーションはコマンドラインタイプであるため、このアプリケーションのデフォルト ロケーションは **[コマンド ライン]** 上に表示されます。


 **メモ:** このアプリケーションをデフォルト以外のロケーションにインストールした場合は、**[コマンド ライン]** 上に表示されているロケーションを編集してください。

## [設定] メニュー - Dell OpenManage RAC Console


1. Dell Management Console で、**[設定]** → **[コンソール]** → **[右クリック アクション]** を選択します。
2. **[管理アプリケーション]** ページの左側のウィンドウで、アプリケーションをクリックします。例として RAC Console アプリケーションをクリックします。

Dell OpenManage RAC Console ページが表示されます。

3. このアプリケーションは、Dell アウト オブ バンド (OOB) デバイス用の右クリック オプションであるため、**[リソース タイプ]** は **[Dell OOB 管理デバイス]** と表示されます。

 **メモ:** デバイスのリソースタイプは変更しないことを強くお勧めします。

4. このアプリケーションは URL タイプであるため、このアプリケーションのデフォルト ロケーションは **[ベース URL]** 上に表示されます。

 **メモ:** URL がデフォルトと異なるか SSL を有効にしている場合は、アプリケーションが正しく起動するように URL を編集してください。

---

[目次のページに戻る](#)