# LANDesk® System Manager 8.7

ユーザーズ ガイド

# 表紙

本書の内容は、明示か黙示かを問わず、保証やライセンスを構成するものではありません。LANDesk は、特定の目的に対する整合性、商品性、知的財産権または第三者あるいは LANDesk のその他の権利への非侵害を含むがそれらに限定されず、のその他の権利への非侵害を含むがそれらに限定されず、それらの保証やライセンス、および他のすべての責任を負いません。LANDesk の製品は、医療、救命、または生命維持装置での使用を意図したものではありません。読者は、第三者が本書に関連する可能性がある知的財産権、およびここで説明された技術を所有することを認識し、LANDesk の責任とは無関係に、適切な弁護士の助言を求めることをお勧めします。

LANDeskは、本書および関連する製品の仕様および説明書をいつでも予告なしに変更する権利を保有します。LANDeskは、本書の使用に関する保証を行わず、本書に発生しうるいかなる間違いの責務を負わないことを前提とし、ここに記載されている情報を更新する責務を負いません。

# 目次

# 概要

## LANDesk® System Manager について

LANDesk® System Manager8.70 へようこそ。LANDesk® System Manager は、Windows、Linux、HP-UX、および AIX
サーバの可用性維持を可能にするスタンドアロンの管理アプリケーションです。これは、LANDeskManagement Suite と同時にインストールおよび使用することもできます。この場合、Management Suite と同じコア データベースを使用するので、IT 全体に関するレポートの作成が容易になります。

本製品は、リソース使用量を低く抑えることに重点を置いた設計になっており、必要な場合のみ実行される「オンデマンド」のエージェントとサービスを備えています。これにより、他のタスクのためにメモリと CPU サイクルを解放できます。LANDesk
は、デバイスの可用性が企業にとって重要であることを認識しています。したがって、本製品は、24 時間体制の環境で安定した動作が可能な設計になっています。これを使用しても、デバイス上で実行されているソフトウェアの制御はユーザが実施できます。つまり、完全なエージェントをインストールしたり、特定のコンポーネントを選択したり、エージェントをインストールせずにデバイス
リストにデバイスを移動したりできます。

---

ダイアログとウィンドウを正常に表示するために、System Manager
のウェブサイトをブラウザのポップアップ ブロッカーの許可リストに追加する必要があります。

---

### バージョン 8.70 の新機能

次の機能が前のバージョンの System Manager に追加またはアップグレードされています。

**エージェントなしデバイスの管理** : Intel* AMT、IPMI、または DRAC
などのアウトオブバンド管理テクノロジが有効になっている場合に、管理エージェントをインストールせずに**[マイ デバイス]** ビューのデバイスを管理します。

**[スケジュールされているタスク] 内のカスタム グループ** :タスクを実行用に複数のカスタム
グループにグループ分けすることができます。

**ビギナー モード** :
ツールバー上のボタンにラベルを表示することができるので、新しいユーザはボタンの用途がわかりやすくなります。同様に、ラベルを非表示にすることも可能です (マウス
カーソルを合わせればヒントが表示されます)。

**ハードウェア構成** : この新しいツールを使えば、Intel* AMT
機能を持つデバイスのオプションを設定できます。Intel AMT デバイスのプロビジョニング用の ID の生成、生成された ID の表示、および Intel AMT
デバイスのプロビジョニングに関連した構成オプションの変更が行えます。さらに、デバイス上の疑わしいネットワーク アクティビティを検出およびブロックする回路ブレーカー ポリシーも定義できます。

**拡張された Active Management Technology (AMT) のサポート**： 本製品は、Intel* Active Management Technology 2 (1 に追加して) もサポートしました。AMT バージョン 2 は、エージェントなし管理と Intel* AMT 2 デバイスの自動検出もサポートしています。

## 製品の機能

System Manager
では、単純な情報収集から正確なパフォーマンス分析、セキュリティ、構成のコントロールまで、管理範囲レベルを選択することができます。System Manager には次の機能があります。

**使いやすい Web コンソール** :Web
ベースのコンソールを使用して、本製品をいつでもどこでも実行できます。このコンソールは、使いやすいインターフェイスで豊富なデータを配信できる設計になっています。コンソールは、プライマリ
ワークステーションまたはサーバ ルーム内の !ServerName!
がインストールされていないワークステーションから実行できます。製品の
URL「http:// *coreserver*/LDSM」を参照するだけです。ソフトウェア配布などのアクションの対象となる特定のデバイスを、[ターゲット デバイス]
リストに追加するサーバとして選択することによって「ターゲット指定」します。このリストは、多くの Web アプリケーションで使用されている「ショッピング カート」に似ています。

**オペレーティング システムのサポート拡張** :多様なサーバ環境を 1
つの統合されたコンソールから管理します。Windows 2000 および 2003
サーバの管理に加えて、System Manager では数種類の Linux と Unix のサポートも提供しています。

- Red Hat Enterprise Linux v3 (ES) 32-bit – U6
- Red Hat Enterprise Linux v3 (ES) EM64t – U6
- Red Hat Enterprise Linux v3 WS 32-bit – U6
- Red Hat Enterprise Linux v3 WS EM64t – U6
- Red Hat Enterprise Linux v3 (AS) 32-bit – U6
- Red Hat Enterprise Linux v3 (AS) EM64t – U6
- Red Hat Enterprise Linux v4 (ES) 32-bit – U2
- Red Hat Enterprise Linux v4 (ES) EM64t – U2
- Red Hat Enterprise Linux v4 (AS) 32-bit – U2
- Red Hat Enterprise Linux v4 (AS) EM64t – U2
- Red Hat Enterprise Linux v4 WS 32-bit – U2
- Red Hat Enterprise Linux v4 WS EM64t – U2
- SUSE* Linux Server 9 ES 32-bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

**スケジュールされたタスク表示**
:すべてのスケジュール済みおよび完了したエージェントの導入、検出、ソフトウェア更新、およびカスタム スクリプト タスクを 1

つの場所から表示します。タスクは、再スケジュール、変更、および定期的なイベントへの設定ができます。

**Intel* AMT サポート** : Intel* Active Management Technology (AMT) バージョン 1 および 2 をサポートします。Intel AMT は、OS が応答しなかったりデバイスの電源がオフになっている場合でも、アウトオブバンド (OOB) 通信によってあらゆるシステム状態のネットワーク デバイスをリモート管理する機能です。デバイス側の要件は、企業ネットワークに接続されていて、スタンバイ電源が入っていることだけです。

**IPMI サポート** :本製品は、Intelligent Platform Management Interface (IPMI) バージョン 1.5 または 2.0 対応のサーバをサポートしています。これにより、OS またはプロセッサが動作していない場合でも、ダウンしたサーバのアウトオブバンド リモート修復および自律管理データの表示が可能です。

**スクリプト作成ツール** :ローカル スケジューラ スクリプトを作成することによって、デバイスにカスタム タスクを実行できます。

**パフォーマンスの監視** :さまざまな属性を使用して、管理対象のエンタープライズ サーバまたはブレード サーバのリアルタイムのパフォーマンスを監視できます。これらの属性を追跡したり、数日間にわたって記録されたパフォーマンス データの履歴を確認したりすることもできます。監視できるデバイスは、監視エージェントがインストールされているサーバです。エージェントがインストールされていないアウトオブバンド IPMI 対応のサーバを監視することもできます。

**ブレード サーバ サポート** ;IBM のブレード シャーシとサーバ ブレードをサポートしています。検索、シャーシ検出、インベントリ、およびパッチ管理機能もサポートされます。製品ツールを使用すると、ブレードを機能、シャーシ、ラック、またはその他の条件でグループ化できるので、より効果的なデータ収集が可能になります。

**レポート機能** :データベース内のデバイス上でレポートを実行して、利用状況の統計情報、リソースの割り当て、およびその他の測定結果を表示できます。本製品には、いくつかの定型のレポートが用意されています。これらのレポートは、データベースに直接アクセスして、情報を収集したり、データを 2 次元または 3 次元の円グラフや棒グラフで表現したりします。カスタム クエリを作成すれば、追加レポートを作成できます。

**ヘルス監視/アラート** :デバイスの全体的なヘルス ステータスを容易に監視できます。ディスク容量や CPU 使用率などの測定項目にしきい値を設定したり、しきい値を超えたときにアラートを受け取る方法を設定したりできます。選択したデバイスのヘルス状態を確認して、問題によってパフォーマンスが低下したりデバイスが停止する前にアクションを実行して問題を解決できます。

**ソフトウェア更新** :System Manager 用と Intel* ハードウェア用のソフトウェア更新を受け取ることができます。ソフトウェア配布機能を使用すると、選択した更新を手動で導入できます。

**役割ベース管理**
:ユーザを追加したり、ユーザの管理役割に基づいてツールおよび他のデバイスへのアクセス権を設定したりします。役割ベース管理によって、表示および管理が可能なデバイスを決定するスコープ、および実行可能なタスク（ユーザのみのレポートなど）を決定する権限を割り当てます。

**インベントリ** :インベントリ スキャン
ツールを使用して、ハードウェアやソフトウェアの豊富な情報をコンパイルし、コア
データベースに格納します。このデータは、表示、印刷、およびエクスポートが可能です。

**デバイス検索**
:ネットワーク上のデバイスを検出します。この機能は、環境内のすべてのデバイスおよびその他のデバイスに関する基本情報を収集します。これにより、高度な制御が可能になり、ターゲット
デバイスへのエージェントの導入が高速化されます。

**Active System Console のサポート** : Active System Console
エージェントをデバイスにインストールした場合に、簡潔なシステムのヘルス概要を提供する Active System Console
をサポートします。選択したハードウェアが正常に機能しているかどうか、注意すべき問題があるかどうかが一目でわかります。 また、詳細なシステム
パフォーマンス指標を表示し、ハードウェア、ソフトウェア、ログ、および Intel* AMT および IPMI
（デバイスがいずれかに対応している場合）に関する情報の一覧も表示できます。

**エグゼクティブ ダッシュボード**
:役員がビジネスの健全度と状態を監視するために利用する一連のツール
（情報を提供するグラフ、図、ダイヤル、メーター）で構成されます。

**ヘルプ** :この製品には、スタート ガイドとコンテキストに応じたヘルプ トピックが含まれています。

## 製品用語

- **コア サーバ** :管理ドメインの中心。製品の主要なファイルおよびサービスはすべてコア
  サーバに置かれます。管理ドメインにはコア サーバを 1 台だけ配置できます。コア
  サーバは新しいサーバでも用途を変更したサーバでもかまいません。
- **コンソール** :メインのインターフェイスであるブラウザベースのコンソール。
- コア データベース : **この製品は、**データを管理するためにコア サーバに MSDE
  データベースを作成します。
- **管理デバイス**
  :製品のエージェントをインストールしているネットワークのデバイス。「デバイス」には、デスクトップ、サーバ、ラップトップ、モバイル ノート、ブレード シャーシなどが含まれます。1 台のコア
  サーバで数千台のデバイスを管理できます。
- **公開** : すべてのユーザが閲覧可能なアイテム
  （グループ、配布パッケージ、タスクなど）。ユーザが公開のアイテムを変更しても、その変更内容は公開のままになります。[公開グループ] は管理者権限を持つユーザが作成します。

- **非公開**または**ユーザ** :
  現在ログインしているユーザが作成したアイテム。これらは他のユーザには表示されません。非公開またはユーザのアイテムは、**[マイ配信方法]**、**[マイ パッケージ]**、**[マイ タスク]**ツリーに表示されます。管理者権限を持つユーザは、[非公開グループ] および [ユーザ パッケージ] と [ユーザ タスク] を表示できます。
- **共通** :他のユーザが表示可能なアイテム。ある共通アイテムの (変更を行って) オーナーシップを引き受けた場合、そのアイテムは 2 つのアイテムに分かれます。共通アイテムはそのまま残り、ユーザ アイテムが [ユーザ] フォルダに保存されます。そのアイテムの [ユーザ] インスタンスは、他のユーザには表示されなくなります。ユーザは表示可能な任意のタスクを [共通] とマークして、他のユーザと共有できます。そのアイテムのプロパティで [共通] オプションをクリアすると、そのタスクはそのユーザの [ユーザ タスク グループ] にのみ表示されます。

# はじめに



## 概要

LANDesk® System Manager をご購入いただきありがとうございます。LANDesk® System Manager は、スタンドアロン型のデバイス管理アプリケーションです。デバイスを迅速かつ効果的に管理できるので貴重な時間を最大限活用でき、時間と費用を節約します。System Manager では、デバイスの中央管理、アクション (パワー サイクル、脆弱性の評価、またはアラートの設定) ごとのデバイスのグループ化、リモートからのトラブルシューティング、ネットワーク安全性の維持、および最新パッチによるデバイスの更新を行うことができます。

このマニュアルは、System Manager をすぐに使い始めることができるように、サービスの構成、コンソールの実行、デバイスの検索、[マイ デバイス] リストへの移動、管理デバイスのアクションの構成を行う方法を説明しています。

System Manager! は Web アプリケーションなので、ブラウザを使ってアクセスでき、リモート
ワークステーションからサーバの管理を行えます。一般的な Web
アプリケーションと同様に機能しますが、より使いやすくするために Windows
型の詳細なコントロール機能も備わっています。たとえば、あるコントロールの上にマウス
ポインタを置いてダブルクリックまたは右クリックできます (Windows
アプリケーションと同じ)。たとえば、[マイ デバイス]
リストでは、サーバ名をダブルクリックして特定のデバイス情報にアクセスしたり、右クリックして実行可能なアクションを確認したりできます。

ここでは、System Manager を起動し、ネットワーク上のデバイスの検索、[マイ デバイス]
リストに移動するサーバの選択、エージェントの導入、各種タスクのためのターゲット
デバイス設定の方法をステップごとに説明します。

## インストレーション プログラムの実行

インストール時には、自動実行ページで LANDesk® System Manager
を選択します。詳しいインストール手順の説明は、『LANDesk Management Suite
インストールおよび導入ガイド』の「フェーズ 3」「フェーズ 2」に記載されています。

System Manager のインストールが完了したら、いつでも !ProductName!
を使い始めることができます。次の各セクションでは、コア
サーバ使用開始ユーティリティの実行、サービスの設定、コンピュータの検索、[マイ デバイス]
リストへのデバイスの移動による管理対象デバイスの指定、デバイスのグループ化、ユーザの追加、エージェントの導入といった必要なタスクの完了方法について説明します。これらのタスクが終了したら、System Manager の強力な機能セットがデバイス管理にどのように役立つかを探索してみましょう。

## コア サーバのライセンス認証

コア サーバのライセンス認証を行うまで、製品を実行することはできません。

コア サーバの使用開始 ユーティリティは、次のことを実行するために使用します。

- 使用開始時に新しい System Manager コア サーバのライセンスを認証する
- 既存の System Manager コア サーバを更新する、
  試用版ライセンスから通常のライセンスに切り替える、 Management Suite または System Manager にアップグレードする

各コア サーバには、そのコア サーバに固有の認可証明書が必要です。

このユーティリティは初めて再起動する時に自動的に実行されます。

コア サーバがインターネットに接続されている状態で、次の操作を実行します。

1. [スタート]、[プログラム]、[コア サーバの使用開始]
   の順にクリックします。ユーザ名とパスワードが入力されます。
2. ライセンス購入時に割り当てられた固有のユーザ名とパスワードを入力します。

3. [使用開始] をクリックします。

コア サーバは、HTTP で Software ライセンス サーバと交信します。プロキシ
サーバを使用している場合は、ユーティリティの [プロキシ]
タブをクリックし、プロキシ情報を入力します。コア
サーバがインターネットに接続している場合、ライセンス
サーバとの交信は自動で行われ、ユーザの操作は必要ありません。コア
が接続されていない場合、再起動時に [閉じる] をクリックして、認証ファイルを licensing@landesk.com
に電子メールで送ります。

定期的に、コア サーバはノード カウントの検証情報を ¥Program Files¥LANDesk¥Authorization
Files¥LANDesk.usage ファイル内に生成します。このファイルは、定期的に LANDesk Software
ライセンス サーバに送信されます。このファイルは XML
形式で、電子署名が済んでおり、暗号化されています。このファイルに手動で変更を加えると、ファイル
の内容と Software ライセンス サーバに対する次の利用状況レポートが無効になります。

- コア サーバの使用開始
  ユーティリティは、ダイアルアップによるインターネット接続を自動で起動しません。ダイアルアップ
  接続を手動で起動してライセンス認証ユーティリティを実行した場合は、ライセンス認証ユーティ
  リティはダイアルアップ接続を使用して利用状況のレポートを送信することができます。
- 電子メールでもコア サーバのライセンスを認証できます。Program Files¥LANDesk¥Authorization
  ディレクトリにある .TXT 拡張子のファイルを licensing@landesk.com に送信します。LANDesk
  カスタマ サポートは、ファイルを添付した電子メールを返信します。このメールには、コア
  サーバにその添付ファイルをコピーしてライセンス認証を完了する方法が記述されています。

## ユーザの追加

System Manager
ユーザとは、コンソールにログインし、ネットワークで特定のデバイスを対象に特定のタスクを実行するこ
とができるユーザです。ユーザは役割ベースの管理機能で管理します。役割ベース管理を使用すると、
製品ユーザに、ユーザの権限およびスコープに基づく特別な管理役割を割り当てることができます。「権
限」は、ユーザが表示して使用できる製品ツールと機能を決定します。「スコープ」は、ユーザが表示して
管理できるデバイスの範囲を決定します。さまざまなユーザを作成し、その権限およびスコープを管理要
件に合わせてカスタマイズできます。たとえば、ヘルプ
デスクの役割を果たすユーザを作成し、この役割に必要な権限をユーザに与えることが可能です。詳細
については、『System Manager ユーザーズ
ガイド』の役割ベース管理について扱っている章を参照してください。

製品をインストールすると、2 つのユーザ アカウントが自動的に作成されます
(下記を参照)。さらにユーザを追加する場合は、手動でユーザ
アカウントを作成してください。ユーザは実際にコンソールに作成されるわけではありません。代わりに、
ユーザがコア サーバの Windows NT ユーザ環境で LANDesk Management Suite
グループに追加されると、そのユーザは [ユーザ] グループ (左側のナビゲーション
ペインで、[ユーザーの管理] をクリック) に表示されます。[ユーザ] グループには、コア サーバの
LANDesk Management Suite グループに現在いるすべてのユーザが表示されます。

[ユーザ] グループには 2 つの既定ユーザがいます。既定ユーザの 1 つは「既定管理者」です。既定管理者は、本製品のインストール時にサーバにログインした管理者ユーザです。

既定ユーザのもう 1 つは「既定のテンプレート ユーザ」です。このユーザにはユーザ プロパティ (権限およびスコープ) のテンプレートが含まれており、Management Suite グループに追加された新規ユーザを設定するときに使用します。つまり、Windows NT 環境で該当するグループにユーザを追加すると、ユーザは [既定のテンプレート ユーザ] プロパティに現在定義されている権限とスコープを継承します。既定のテンプレート ユーザにすべての権限と既定の [すべてのコンピュータ] スコープが選択されていると、LANDesk Management Suite グループに配属される新規ユーザは [ユーザ] グループに追加され、Management Suite ツールおよびデバイスすべてにアクセスする権限があります。

既定のテンプレート ユーザのプロパティ設定を変更するには、[既定のテンプレート ユーザ] を選択し [編集] をクリックします。たとえば、一度に多数のユーザを追加するが、ツールまたはデバイスのすべてではアクセスを認めない場合は、最初に既定のテンプレート ユーザの設定を変更し、LANDesk Management Suite グループにユーザを追加します (以下の手順を参照)。既定のテンプレート ユーザは削除できません。

Windows NT で LANDesk Management Suite グループにユーザを追加すると、ユーザは、[ユーザ] ウィンドウで [ユーザ] グループに自動的に読み込まれ、現在の既定のテンプレート ユーザと同じ権限とスコープを継承します。ユーザの名前、スコープ、および権限が表示されます。また、ユーザ固有のログイン ID で名前を付けられた新規ユーザ サブグループが、[ユーザ デバイス]、[ユーザ クエリ]、[ユーザ レポート]、および [ユーザ スクリプト] の各グループに作成されます (管理者のみが各ユーザ グループを表示できることに注意してください)。

逆に、LANDesk Management Suite グループからユーザを削除すると、ユーザは [ユーザ] リストには表示されなくなります。ユーザのアカウントはまだコア サーバに存在し、いつでも LANDesk Management Suite グループに再追加できます。また、[ユーザ デバイス]、[ユーザ クエリ]、[ユーザ レポート]、および [ユーザ スクリプト] の各グループのユーザ サブグループは保持されるので、データを失わずにユーザを復元したり、他のユーザにデータをコピーしたりできます。

F5 を押して System Manager コンソールの [ユーザ] フレームの表示を更新します。ユーザまたはドメイン グループを LANDesk Management Suite グループに追加する方法、または新しいユーザ アカウントを作成する方法については、『System Manager *ユーザーズ ガイド*』の役割ベース管理について扱っている章にある「製品ユーザの追加」を参照してください。

ユーザまたはドメインを LANDesk Management Suite グループに追加するには

1. サーバの [**管理ツール**]、[**コンピュータの管理**]、[**ローカル ユーザーとグループ**]、[**グループ**] ユーティリティの順にクリックします。
2. [**LANDesk Management Suite**] グループを右クリックし、[**グループに追加**] をクリックします。
3. [**追加**] をクリックし、ユーザを入力するかリストから選択します (複数選択可)。
4. [**追加**] をクリックし、[**OK**] をクリックします。

**注意** : [**ユーザ**] リストのユーザ アカウントを右クリックして LANDesk Management Suite グループにユーザを追加するか、[**プロパティ**]、[**所属するグループ**]、[**追加**] の順にクリックしてグループを選択し、ユーザを追加することもできます。

ユーザ アカウントがもうサーバに存在しない場合は、最初にサーバに作成する必要があります。

新しいユーザ アカウントを作成するには

1. サーバの [**管理ツール**]、[**コンピュータの管理**]、[**ローカル ユーザーとグループ**]、[**ユーザ**] ユーティリティの順にクリックします。
2. [**ユーザ**] を右クリックし、[**新規ユーザ**] をクリックします。
3. [新規ユーザ] ダイアログで、名前とパスワードを入力します。
4. パスワード設定を指定します。
5. [**作成**] をクリックします。[**新規ユーザ**] ダイアログは開いたままなので、追加のユーザを作成できます。
6. [**閉じる**] をクリックしてダイアログを終了します。

LANDesk Management Suite グループにユーザを追加すると、コンソールの [ユーザ] グループに表示されます。

## サービスと資格情報の設定

ネットワーク上のデバイスの管理を始めるには、System Manager に必要なデバイス認証資格情報を提供する必要があります。コアにある Configure Services ユーティリティ (SVCCFG.EXE) を使って、必要なオペレーティング システム、Intel* AMT、IPMI BMC の認証資格情報を指定します。インベントリの既定、PXE 待機キュー設定、LANDesk データベース設定なども指定できます。

設定には Configure Services を次のように使用します。

- データベース名、ユーザー名、およびパスワード(インストール時に設定)。
- 管理対象デバイスに対するジョブのスケジュールに必要な資格情報(複数の管理者資格情報セットを入力できます。)
- IPMI BMC の設定に必要な資格情報(BMC の資格情報は 1 セットしか入力できません。)
- Intel AMT 対応デバイスの設定に必要な資格情報(Intel AMT の資格情報は 1 セットしか入力できません。)
- サーバ ソフトウェアのスキャン間隔、メンテナンス、インベントリ スキャン保存日数、およびログイン履歴の長さ
- 重複デバイス ID の処理
- スケジューラ構成 (スケジュールされているジョブとクエリ評価の間隔を含む)
- カスタム ジョブ構成 (リモート実行タイムアウトを含む)

1. コア サーバで、[スタート]、[プログラム]、[LANDesk]、[LANDesk Configure Services] の順にクリックします。
2. [スケジューラ] タブをクリックします。
3. [ログインの変更] ボタンをクリックします。
4. 管理対象デバイス上で使用する資格情報 (通常はドメイン管理者アカウント) を入力します。

5. [追加]
   をクリックします。管理対象デバイス上で同じ管理者ユーザ名アカウントが有効になっていない場合は、必要に応じて他の資格情報を追加します。
6. [適用] をクリックします。
7. 環境に IPMI 対応のサーバがある場合は、[BMC パスワード] タブをクリックします。[パスワード] テキスト ボックスにパスワードを入力し、[パスワードの確認入力] テキスト
   ボックスにパスワードを再入力して OK] をクリックします。すべての管理対象 IPMI サーバで同じ BMC ユーザ名とパスワードを共有する必要があります。
8. Intel AMT 対応のデバイスがある場合、[Intel AMT 構成] タブをクリックします。[ユーザ名] テキスト ボックスに現在設定されている Intel AMT ユーザ名を、[パスワード] テキスト
   ボックスに現在設定されているパスワードを入力します。[パスワードの確認入力] テキスト
   ボックスにパスワードをもう一度入力してから [OK] をクリックします。
9. 必要に応じて、ソフトウェア スキャン間隔などのその他の設定を行います。
10. [OK] をクリックして変更を保存します。

詳細については、各 Configure Services のタブで [**ヘルプ**] をクリックしてください。

## コンソールの実行

System Manager
には、ネットワーク上のデバイスを表示、設定、管理、保護するためのツールがすべて用意されています。コンソール内のツールを使用すると、配布されたパッケージをアンインストールできます。

コンソールの上部ペインには、現在ログインしているサーバとログイン時に使用したユーザ名が表示されます。[マイ デバイス] リストはコンソールのメイン
ウィンドウで、ほとんどの機能はまずここから開始します。左ペインには、使用できるツールが表示されます。コンソールの右ペインには、管理タスクを遂行できるダイアログや画面が表示されます。

コンソールの利点として、すべての機能が 1 つのリモート ロケーション
(お使いのワークステーションなど)
から実行できるので、日常の保守や問題のトラブルシューティングのために、サーバ室に足を運んだり、管理対象の個々のデバイスがある場所まで行く必要がなくなります。

コンソールは次の 3 つの方法で起動できます。

- コア サーバで、[スタート]、[すべてのプログラム]、[LANDesk]、[System Manager]
  の順にクリックします。
- リモート ワークステーションのブラウザで、URLとして「http://coreserver/LDSM」と入力します。
- ダッシュボードで、[LDSM コンソール] をクリックします。

## デバイスの検索

[**検索構成**]
タブでは、検索構成の新規作成、既存の構成の編集または削除、および検索構成のスケジュールを行うことができます。各検索構成は、わかりやすい名前、スキャン対象となる IP
範囲、検索タイプで構成されます。

構成を作成したら、[**検索のスケジュール**] ダイアログで検索の実行時期を設定します。

1. 左側のナビゲーション ペインで、[**デバイス検索**] をクリックします。
2. [**検索構成**] タブで、[**新規**] ボタンをクリックします。
3. 以下に説明するフィールドに必要な情報を入力します。各フィールドへの入力が完了したら、[**追加**] ボタンをクリックして [**OK**] をクリックします。

以下に、[**検索構成**] ダイアログ ボックスの各構成要素を説明します。

- **構成名** :
  この構成の名前を入力します。構成名にはわかりやすい名前を指定して、構成内容をすぐに認識できるようにしてください。構成は 255
  文字以下とし、次の文字は使用しないでください。**"**、**+**、**#**、**&**、または **%**。これらの文字を 1
  つでも使うと、構成名は表示されません。
- **標準ネットワーク スキャン** :指定した範囲の IP アドレスに ICMP
  パケットを送信してデバイスを検索します。これは最も詳細な検索ですが、最も時間がかかります。既定では、このオプションには NetBIOS が使用され、デバイスに関する情報が収集されます。

  ネットワーク スキャン オプションには、デバイス検索が TCP パケット応答を通して OS
  タイプを検索する **IP fingerprint** オプションが用意されています。IP FingerPrint
  オプションを使用すると、検索処理が多少遅くなります。

  ネットワーク スキャン オプションには、SNMP を使ってスキャンするように設定可能な [**SNMP を使用する**] オプションもあります。[**構成**] ボタンをクリックして、SNMP
  構成の情報を入力します。
- **LANDesk CBA 検索** :標準の管理エージェント (以前の Management Suite の Common Base Agent (CBA)) をデバイスで検索します。標準の管理エージェントにより、コア
  サーバがネットワーク上のクライアントを検索して、通信することができます。このオプションは、製品のエージェントをインストールしているデバイスを検索します。ルータは標準の管理エージェントと PDS2 トラフィックをブロックします。複数のサブネット間で標準 CBA
  検索を実行するには、複数のサブネット間で指定のブロードキャストを許可するようにルータを設定する必要があります。

  CBA 検索オプションでは、デバイス検索がデバイス上の LANDesk Ping Discovery Service (PDS2) を検索する **LANDesk PDS2 検索**オプションも使用できます。LANDeskLANDesk® System Manager、Server Manager、およびLANDesk Client Manager
  などのソフトウェア製品は、PDS2
  エージェントを使用します。ネットワーク上のデバイスにこれらの製品がインストールされている場合は、このオプションを選択してください。CBA 検出は Linux
  コンピュータではサポートされていませんが、PDS2
  を選択すれば、エージェントをインストール済みの Linux コンピュータは検出が可能になります。

- **IPMI** : IPMI 対応サーバを検索します。IPMI は、管理可能なハードウェアにアクセスするためのメッセージとシステム インターフェイスを定義するために、Intel、* H-P、* NEC、* および Dell * が開発、規格化した仕様です。IPMI には、監視と復旧機能が含まれており、デバイスの電源のオン/オフまたは OS の動作状態に関係なく、多くの機能にアクセスできます。BMC が構成済みでない場合、BMC は IPMI 検出のために本製品が使用する ASF ping に応答しないことに注意してください。つまり、通常のコンピュータとして検出されることになります。クライアントをプッシュするときに、ServerConfig がシステムをスキャンして IPMI を検出し、BMC を構成します。
- **サーバ シャーシ** : ブレード サーバ シャーシ管理モジュール (CMM) を検索します。サーバ シャーシのブレードは、標準のサーバとして検索されます。
- **Intel* AMT** : Intel Active Management Technology をサポートするデバイスを検索します。
- **開始 IP** :スキャンするアドレス範囲の開始 IP アドレスを入力します。
- **終了 IP** :スキャンするアドレス範囲の終了 IP アドレスを入力します。
- **サブネット マスク** :スキャンする IP アドレス範囲のサブネット マスクを入力します。
- **追加** :ダイアログの下部の作業キューに IP アドレスの範囲を追加します。
- **クリア** : IP アドレス範囲のフィールドをクリアします。
- **編集** : 作業キューで IP アドレスの範囲を選択し、[**編集**] をクリックします。IP アドレスの範囲が作業キューの上にあるテキスト ボックスに表示され、範囲を編集したり、作業キューに新しい範囲を追加したりすることができます。
- **削除**:作業キューに対して選択した IP アドレスの範囲を削除します。
- **すべて削除** :作業キューからすべての IP アドレス範囲を削除します。

これで検索タスクの構成が完了しました。次に、ネットワークに接続されているデバイスを検索する準備として、検索タスクの実行をスケジュールします。

## 検索タスクのスケジュールと実行

[デバイス検索] タブの [スケジュール] ボタンをクリックすると、[検索のスケジュール] ダイアログが表示されます。このダイアログでは、検索を実行する時刻をスケジュールできます。検索タスクは、すぐに実行する、後で実行する、定期的に繰り返し実行する、または、1 度だけ実行して何度も繰り返し実行することのないようにスケジュールできます。

検索タスクをスケジュールしたら、[検索タスク] タブを表示して、検索ステータスを確認してください。繰り返し実行される検索タスクをスケジュールすることにより、ネットワークに新たに接続されたデバイスが自動的に検索されます。

[検索のスケジュール] ダイアログには、次のオプションがあります。

- 未スケジュール : タスクのスケジュールは設定しませんが、後で使用するために [検索構成] リストの中に残しておきます。
- すぐに開始 : できるだけ速やかにタスクを実行します。タスクの開始までに 1 分かかる場合もあります。

- スケジュールされた時刻に開始
  :指定した時間にタスクを開始します。このオプションをクリックする場合は、次の情報を入力してください。
  - 時刻 : タスクを開始する時刻
  - 日付 :
    タスクを開始する日付。ロケールの設定によって、日付順序は「日/月/年」または「月/日/年」になります。
  - 実行周期 : タスクを繰り返し実行する場合は、[日単位]、[週単位]、[月単位]
    のいずれかを選択します。[月単位] を選択し、すべての月には存在しない日付 (たとえば 31 日) を選択した場合、その日付が存在する月のみにタスクが実行されます。

検索タスクをスケジュールするには

1. 左側のナビゲーション ペインで、[検出されたデバイス] をクリックします。
2. [検索構成] タブで、目的の構成を選択して、[スケジュール]
   をクリックします。検索スケジュールを設定して [保存] をクリックします。
3. [検索タスク] タブで、検索の進行状態を監視します。[更新]
   をクリックして、ステータスを更新します。
4. 検索が完了したら、[非管理] をクリックして上の [検出されたデバイス]
   ペインにすべての検索結果を表示します (このペインは自動的には更新されません)。

## 検出されたデバイスの表示

検出されたデバイスは、[検出されたデバイス] ペインでデバイスの種類別に分類されます。既定では [コンピュータ]
フォルダが表示されます。別のカテゴリのデバイスを表示するには、左ペインでカテゴリのフォルダをクリックします。[非管理] をクリックすると、検出されたすべてのデバイスが表示されます。

- ブレード サーバ シャーシは [シャーシ] フォルダに表示されます。
- 標準のエンタープライズ デバイスは [コンピュータ] フォルダに表示されます。
- ルータとその他のデバイスは [インフラストラクチャ] フォルダに表示されます。
- Intel AMT 対応のデバイスは [Intel AMT] フォルダに表示されます。
- IPMI 対応のサーバは [IPMI] フォルダに表示されます。
- カテゴリのないデバイスは [その他] フォルダに表示されます。
- プリンタは [ プリンタ] フォルダに表示されます。

注意 : 一部の Linux サーバはオペレーティング システム名が一般の「Unix」と表示されます (または「その他」の場合もあります)。標準の管理エージェントを導入すると、これらのサーバは [マイデバイス] リストの OS 名のエントリを更新し、完全なインベントリを表示します。
検出されたサーバを表示するには

1. [デバイス検出] ページの左ペインで、[コンピュータ]
   または表示する別の種類のデバイスをクリックします。検索結果が右ペインに表示されます。
2. 検索結果をフィルタするには、フィルタ アイコン 
   をクリックし、検索する対象の一部を入力してから [検索] をクリックします。

## 名前の割り当て

ネットワーク スキャンによる検索を実行すると、返されるサーバにノード名 (またはホスト名) が割り当てられていない場合があります。これは、Linux を実行しているサーバによく見られます。[管理] を使用してサーバを [マイ デバイス] リストに移動するには、そのデバイスに名前を割り当てる必要があります。

1. [デバイス検索] ページで、名前の付いていないデバイスをクリックします。ノード名の列の空白部分をクリックする必要があります。
2. ツール バーの [名前の指定] をクリックします。
3. 名前を入力して [OK] をクリックします。

製品エージェントをデバイスにインストールすると、ホスト名が自動的にスキャンされ、コア データベースが正しい情報に更新されます。

## [マイ デバイス] リストへのデバイスの移動

デバイスが検出されたら、手動で管理対象のデバイスを選択して、[マイ デバイス] リストに移動する必要があります。デバイスを移動しても、そのデバイスにソフトウェアがインストールされるわけではありません。デバイスに対するクエリの実行、デバイスのグループ化、および [マイ デバイス] リストでのデバイスの並べ替えが可能になるだけです。特定のデバイスを特定のアクションの「ターゲット」として指定します。これは多数の Web アプリケーションにある「買い物かご」モデルに類似しています。

1. [検出されたデバイス] ビューで、[マイ デバイス] リストに移動するデバイスをクリックします。複数のサーバを選択するには、Shift キーを押しながらクリック、または Ctrl キーを押しながらクリックします。
2. [ターゲット] ボタンをクリックします。[ターゲット] ボタンが表示されていない場合は、ツール バーの [<<] をクリックします。このボタンはツール バーの一番右端にあります。または、選択したサーバを右クリックし、[ターゲット] をクリックします。
3. 下のペインで、[管理] タブをクリックします。
4. 選択して、選択したデバイスを管理データベースに移動します。あるいは選択して、ターゲット デバイスを移動します。
5. [移動] をクリックします。

[移動] をクリックすると、デバイスが [マイ デバイス] リストに移動され、デバイスの情報がデータベースに追加されます。情報がデータベースに追加されると、デバイス名、IP アドレス、OS などに基づいてその情報に対するクエリおよびレポートの実行が制限付きで可能になります。

## アクションのためのデバイスのグループ化

地域別、機能別などでデバイスをグループ化すると、それらのデバイスに対するアクションを迅速に実行できます。たとえば、特定の場所にあるすべてのデバイスのプロセッサ速度を確認することも可能です。

1. [マイ デバイス] リストで、[非公開グループ] または [公開グループ] をクリックしてから [グループの追加] をクリックします。
2. [グループ名] ボックスにグループの名前を入力します。
3. 作成するグループのタイプを選択します。
    - 静的 :
      グループに追加されたサーバ。これらのサーバは、削除されるか、ユーザがこれらのサーバを管理から除外するまでグループ内に属します。
    - 動的 : クエリで定義した 1 つまたは複数の条件に適合するサーバ。たとえば、1 つのグループに現在警告状態にあるすべてのサーバを含めることもできます。これらのサーバは、グループに対して定義された条件を満たす限り、グループ内に属します。グループ クエリ条件を満たしたデバイスは、自動的にダイナミック グループに追加されます。
4. 終了したら、[OK] をクリックします。
5. デバイスを静的グループに追加するには、[マイ デバイス] リストの右ペインでデバイスをクリックし、[移動/コピー] をクリックします。次にグループを選択し、[OK] をクリックします。

## 管理対象デバイスの設定

デバイスを検索するだけでは、管理傘下に入れることにはなりません。コンソールからデバイスを完全に管理してヘルス状態のアラートを受け取るには、あらかじめサーバに管理エージェントをインストールしておく必要があります。既定のエージェント構成 (すべての管理エージェントをインストールします) をインストールするか、独自のエージェント構成をカスタマイズしてデバイスにインストールできます。(ヘルス アラートを受信するためにはエージェント構成に監視エージェントが含まれている必要があります。)

管理エージェントは、次のいずれかの方法でインストールできます。

- [マイ デバイス] リストでデバイスをターゲット指定し、そのデバイスにリモートでエージェントをインストールするようにエージェント構成タスクをスケジュールします。(以下の手順を参照)
- コア サーバの LDlogon 共有フォルダ (//coreserver/ldlogon) にマップし、SERVERCONFIG.EXE. (手順については、『System Manager ユーザーズ ガイド』の「デバイス エージェントのインストールと設定」の章にある「エージェントのプル」を参照) を実行します。
- 自己解凍型のデバイス インストール パッケージを作成します。このパッケージをローカル デバイス上で実行してエージェントをインストールします。この操作を実行するには、管理者権限でサーバにログインする必要があります。(手順については、『System Manager ユーザーズ ガイド』の「デバイス エージェントのインストールと設定」の章にある「インストール パッケージを使用したエージェントのインストール」を参照してください。)

**エージェントをプッシュするには**

1. [マイ デバイス] リストでターゲット デバイスを指定します (前述のデバイスを [マイ デバイス] リストに移動する手順を参照)。
2. 左側のナビゲーション ペインで [エージェントの構成] をクリックし、プッシュする構成を右クリックして [タスクのスケジュール] をクリックします。
3. 左側のペインで [ターゲット デバイス] をクリックし、[ターゲット一覧の追加] ボタンをクリックします。

4. [タスクのスケジュール] をクリックし、タスクをすぐに開始する場合は [すぐに開始] をクリックし、後で開始する場合は [後で開始] をクリックしてタスクの開始日と時刻を設定して、[保存] をクリックします。

タスクのステータスは [構成タスク] タブで表示できます。

## Linux サーバ エージェントのインストール

Linux エージェントと RPM を Linux サーバ上にリモートで導入およびインストールできます。そのためには、Linux サーバを正しく設定する必要があります。Linux サーバを正しく構成する方法については、『*System Manager ユーザーズ ガイド*』の「デバイス エージェントのインストールと設定」の章にある「サーバ エージェントのインストール」を参照してください。

# アラートの設定

デバイス上で問題またはその他のイベントが発生すると (デバイスのディスク領域の不足など)、System Manager はアラートを送信します。これらのアラートは、アラートを呼び出す重要度レベルまたはしきい値を設定することで、カスタマイズできます。アラートをコンソールに送信し、特定のアクションを実行するようにアラートを設定できます。多数のイベントや潜在的な問題に対してもアラートを設定できます。製品には既定のアラートのルールセットが用意されています。この既定のルールセットは、監視コンポーネントをインストールするときに管理デバイスにインストールされます。.このアラートのルールセットは、ヘルス ステータスのフィードバックをダッシュボードおよびコンソールに提供します。この既定ルールセットには次のようなアラートが含まれます。

- ディスクが追加または削除された
- ディスク領域
- メモリ使用量
- 温度、ファン、電圧
- リモート コントロール アクティビティ
- パフォーマンス モニタ
- IPMI イベント (適用するハードウェア)

アラートについての詳細は、『System Manager ユーザーズ ガイド』の「アラートの構成」の章を参照してください。

# アラートの設定

デバイス上で問題またはその他のイベントが発生すると (デバイスのディスク領域の不足など)、System Manager はアラートを送信します。これらのアラートは、アラートを呼び出す重要度レベルまたはしきい値を設定することで、カスタマイズできます。アラートをコンソールに送信し、特定のアクションを実行するようにアラートを設定できます。多数のイベントや潜在的な問題に対してもアラートを設定できます。製品には既定のアラートのルールセットが用意されています。この既定のルールセットは、監視コンポーネントをインス

トールするときに管理デバイスにインストールされます。.このアラートのルールセットは、ヘルス
ステータスのフィードバックをダッシュボードおよび
コンソールに提供します。この既定ルールセットには次のようなアラートが含まれます。

- ディスクが追加または削除された
- ディスク領域
- メモリ使用量
- 温度、ファン、電圧
- リモート コントロール アクティビティ
- パフォーマンス モニタ

アラートについての詳細は、『System Manager *ユーザーズ ガイド*』の「アラートの構成」の章を参照してください。

## ダッシュボードの実行

ダッシュボードには、使用しているデバイスのシンプルな概要が見やすく表示されています。ダッシュボードでは、各デバイスは色分けされたアイコンで表示され、アイコンの色によってデバイスの現在のヘルスがわかります。また、主要なトラブルシューティング ツールにすばやくアクセスすることもできます。

ダッシュボードを起動するには

- コア サーバで、[スタート]、[プログラム]、[LANDesk]、[LANDeskダッシュボード] の順にクリックします。.
- リモート ワークステーションのブラウザで、URLとして「http://coreserver/LDSM/db_frameset.asp」と入力します。
- コンソールで [ダッシュボード] をクリックします。

## 次の操作

これで、Server Manager を実行することができました。ここまでで使用した Server Manager の機能はほんのわずかで、しかもその機能の一部 (デバイス検索やエージェント構成など) しか活用していません。同梱のほかのガイド (『*インストールおよび導入ガイド*』および『*ユーザーズ ガイド*』) では、製品のすべての機能についてより詳細な情報が提供されています。一部の機能を以下に紹介します。

**リモート コントロール**： リモート ファイルにアクセスしたり、双方向でファイルを転送したり、リモート アプリケーションを実行したり、デバイスをリモートで再起動するなど、デバイスで起こる多数の問題をリモートで診断およびトラブルシューティングします。リモート セッション中は、ターゲット デバイスではなく使用しているコンピュータのキーボード レイアウトを使用し、そのリモート デバイスに対してあらゆる操作をすることが可能です。すべてのアクションがリモート デバイスでリアルタイムに実行されます。

**ソフトウェア更新** :
ネットワーク全体の管理デバイスに対して現行のパッチレベルのセキュリティを確立します。管理デバイス上で動作するさまざまなオペレーティング
システムの脆弱性の評価、適切なパッチ実行可能ファイルのダウンロード、影響を受けるデバイスへの必要なパッチの導入およびインストールによる脆弱性の修正、パッチの正常インストールの確認を行って、現在の脆弱性情報を管理するための繰り返し手順を自動化できます。

**アラート** :
デバイスのいずれかが特定のしきい値に達した場合にアラートが送信します。監視機能に関連し、アラートはさまざまな方法で通知を送信できます。たとえば、デバイスのハード ドライブの使用率が 95%
に達したときに通知する場合、アラートの送信方法を選択できます (電子メール、ポケットベル
メッセージ、デバイスの再起動またはシャット ダウン、またはアラート ログへの情報追加など)。

**クエリ** : 特定のシステムまたはユーザ条件に基づいてコア
データベースにあるデバイスを検索または整理することにより、ネットワークを管理します。管理デバイスのリストに対してクエリを実行し、指定の条件 (本社にあるすべてのデバイス、または 256K の RAM
を持つすべてのデバイスなど)
に一致するデバイスを検索してアクション別にグループ化できます。これらのグループは静的
(グループのメンバは手動でのみ変更できる) または動的
(メンバはデバイスが指定の条件に一致するか一致しないかにより変化する)
のいずれかに設定することが可能です。.

**ソフトウェア配布** :ソフトウェア パッケージ (1 つ以上の MSI ファイル、実行可能ファイル、バッチ
ファイル、RPM ファイル (Linux)、または LANDesk パッケージ ビルダによって作成されたパッケージ)
をターゲット デバイスに配布するタスクを作成します。

**監視** : サポートされている監視タイプ (ASIC の直接監視、インバンド IPMI、アウトオブバンド
IPMI、および CIM など) のいずれかを使って、デバイスのヘルス
ステータスを監視します。監視によって、利用状況のレベル、OS
イベント、プロセスとサービス、パフォーマンスの履歴、およびハードウェア センサー
(ファン、電圧、温度など)
を含むデバイスに関するデータを追跡できます。アラートは監視エージェントを使ってアラート
アクションを開始する関連機能です。

**レポート機能** :
ネットワーク上の管理デバイスに関する重要な情報を提供する、用途を特定したさまざまなレポートを生成できます。Server Manager では、コア
データベースにデバイスを追加し、これらのデバイスのハードウェアおよびソフトウェア
データを収集するためにインベントリ スキャン
ユーティリティを使用します。デバイスのインベントリ表示から取得したインベントリ
データは、表示および印刷できます。また、このインベントリ
データを使用してクエリを定義したり、デバイスをグループ化できます。レポート
ツールは、スキャンしたこのインベントリ データを収集し、見やすいレポート
フォーマットに整理することで、このデータを有効に活用します。これは、規制レポートのデータを収集およびフォーマットする場合に役立ちます。

**非管理デバイス検索**：
コンソールによって管理されていないデバイスを検索します。検索は、新しいコンピュータを迅速に管理下にいれる最初のステップです。検索タスクをセットアップして、新しいコンピュータを毎月スキャンすることもできます。

**ソフトウェア ライセンス監視**：ライセンスの準拠全体を追跡します。ソフトウェア
ライセンス監視エージェントは、データ
（デバイスにインストールされているすべてのアプリケーションについて、合計使用時間
（分）、起動回数、最後に起動した日付など）
を収集し、このデータをデバイスのレジストリに保存します。データは、製品の利用状況および拒否傾向を監視するために使用できます。エージェントは、最低限のネットワーク帯域を使用して、デバイス側の製品の利用状況を受動的に監視します。このエージェントは、モバイル
デバイスがネットワークに接続していなくても、利用状況を継続的に監視します。

**OS 導入**： PXE ベースの導入ツールを使って、ネットワークのデバイスに OS
イメージを導入します。ハード ドライブが空のデバイスやオペレーティング
システムが使用できないデバイスに対して、イメージングを行うことができます。軽量 PXE
代表を使用すると、各サブネットに専用 PXE サーバを配置する必要がなくなります。OS
導入では、プロセスが開始されると、それ以降のエンド
ユーザまたは技術担当者による入力を必要とせずに新規デバイスの移行を効率よく行います。

*その他のブランドおよび名称は、それぞれの所有者に帰属します。

# ライセンス

このライセンス
プロセスを使用すると、組織は、現行の認証プロセスを実行することによって、使用許諾済みノードの契約を遵守できます。また、1 つの定義済みユーザ アカウントで複数のコア
サーバを使用することもできます。ライセンス プロセスでは、バックエンド
データベースを使用してユーザ アカウントの作成と管理を行います。ライセンス プロセスは、コア
サーバからバックエンド プロセスに対する単純な要求と応答で構成され、コア
サーバによるアクティビティの期間延長を許可します。

本製品 (またはアドオン)
をインストール後に実行する場合は、試用期間の場合は試用版ライセンスを認証するか、LANDesk
の営業担当者から購入したライセンスを認証するためにユーザ名およびパスワードを入力します。既存のアカウントに対しては、すべてのコア
サーバのライセンス認証に同じユーザ名およびパスワードを使用します。

ライセンス認証プロセスは、基本的には評価版と購入製品で同じです。デバイスがインターネットに接続している場合、このプロセスは単純に情報を交換します。デバイスがインターネットに接続されていない場合は、ファイルを電子メールで LANDesk に送信し、返送されたファイルをコア
サーバに保存する必要があります。ライセンス認証プロセスは次のように動作します。

1. ユーザがコア サーバの使用開始ユーティリティを実行します。
2. サーバおよび利用状況情報を含むファイルが作成されます。コア
   サーバの非公開キーで署名され、LANDesk の公開キーで暗号化されます。
3. インターネット接続が使用できる場合は、コア サーバと LANDesk サーバが通信して、コア
   サーバがライセンス認証ファイルをアップロードします。バックエンド
   プロセスは情報を処理し、データベースに直接書き込まれるライセンス認証情報を返信します。
4. インターネット接続が使用できない場合は、¥Program Files¥LANDesk¥Authorization Files
   フォルダにあるファイルを電子メールで licensing@landesk.com に送信してください。

# ライセンスの追加

コンソールから使用できる機能は、ライセンス キーによって異なります。新しいライセンス
キーを追加して、追加機能にアクセスしたりユーザ数を更新したりできます。インストール時に、45
日間の試用ライセンスが作成されます。コンソールを使って有効なライセンスを追加すると、この一時ライセンスは削除されます。

**ライセンス キーを追加するには**

1. 左側のナビゲーション ペインで、[**プリファレンス**] をクリックします。
2. [**ライセンス**] タブをクリックします。
3. 画面の下の「http:/www.landesk.com/contactus/」リンクをクリックします。

このリンクが正常に機能しない場合は、ブラウザのセキュリティ レベルが [中]
に設定されていない可能性があります。Internet Explorer で既定のインターネット セキュリティ レベルを
[中] に変更してください ([**ツール**]、[**インターネット
オプション**]、[**セキュリティ**]、[**インターネット**]、[**既定のレベル**] の順にクリックします)。

# コンソール

## コンソールの開始

**コンソールを開始するには**

1. コア サーバで、[**スタート**]、[**プログラム**]、[LANDesk]、[**LANDeskSystem Manager**] の順にクリックします。.

   または

   リモート
   ワークステーションで、ブラウザを開いて、コンソールのアドレスを入力します。アドレスの形式は、http://*コア サーバ名*/ldsmhttp://*コア サーバ名*/remote です。
2. 有効なユーザ名とパスワードを入力します。

   リモート コア サーバに接続する場合は、通常の Windows ルールに従ってリモート ログインします (ユーザがコア
   サーバにローカルであれば、ユーザ名のみを入力し、ユーザがドメイン
   ユーザであれば、ドメイン名¥ユーザ名を入力します)。
3. [**OK**] をクリックします。

---

デバイスのリストとボタンがコンソールの起動時に表示されない場合は、コア
サーバのライセンスを認証する必要があります。

---

### [System Manager ログイン] ダイアログについて

このダイアログでは、コンソールを起動し、コア サーバに接続します。

- **ユーザ名** :
  ユーザを識別します。これは、管理者ユーザか、アクセス制限のある他のタイプの製品ユーザです (詳細については、「役割ベース管理」を参照)。ユーザは、コア サーバの LANDesk Management Suite グループのメンバである必要があります。リモート コア
  サーバに接続する場合は、ドメイン名とユーザ名を入力します。
- **パスワード** : ユーザのパスワード。

## コンソールの使用方法

ツールを使って、1
つのコンソールからネットワーク上のデバイスを表示、設定、管理、保護することができます。ソフトウェアまたは構成設定の更新、ハードウェアおよびソフトウェアの問題の診断、ユーザの機能およびデバイ

スに対するアクセスの役割ベース管理による制御が可能です。さらに、別の LANDesk 製品も使用している場合は、コンソールから直接これらの製品に接続できます。

コンソールの上部ペインには、現在ログインしているサーバとログイン時に使用したユーザ名が表示されます。**[マイ デバイス]**リストはコンソールのメイン ウィンドウで、ほとんどの機能はまずここから開始します。左ペインには、使用できるツールが表示されます。コンソールの右ペインには、デバイスとユーザの管理、レポートの表示、検索の実行、クエリの作成や変更などを行うためのダイアログや画面が表示されます。**[マイ デバイス]** リストのペインと列は、サイズを変更できます。デバイスにエージェントがインストールされていない場合は、名前と IP アドレスの列だけに情報が表示されます。オペレーティング システムの列にも情報が表示される場合があります。

System Manager は、ウェブ ブラウザから簡単にアクセスできる Windows アプリケーションのような機能を提供しています。

- **[マイ デバイス]**リストのデバイスを右クリックして、Pingおよびターゲットなど、そのデバイスで利用可能なオプションを表示します。
- リスト内の連続する複数の項目を選択するには、最初の項目をクリックして、**Shift** キーを押しながら最後の項目をクリックします。
- リスト内の連続しない複数の項目を選択するには、**Ctrl** キーを押しながら個々の項目をクリックします。

---

ダイアログとウィンドウを正常に表示するために、System Manager のウェブサイトをブラウザのポップアップ ブロッカーの許可リストに追加する必要があります。

**役割ベース管理**
ユーザとして**[マイ デバイス]** リストで表示や管理ができるデバイスおよび使用できる管理ツールは、管理者によって割り当てられたアクセス権限とデバイス スコープによって決まります。詳細については、「役割ベース管理」を参照してください。

---

このセクションでは次の内容について説明します。



## [マイ デバイス] リスト

**[マイ デバイス]**リストには次のグループとサブグループが表示されます。また、割り当てられているアクセス権限とデバイス

スコープによっては、独自のグループを作成できます。これにより、デバイスを簡単に管理できるようになります。

## すべてのデバイス

**[すべてのデバイス]**リストには、ユーザのスコープに基づいて、現在ログインしているユーザのデバイスがフラット形式 (サブグループのない形式) で表示されます。特定のコア
サーバに接続している場合、管理者は、そのコア
サーバによって管理されているすべてのデバイスを表示できます。一方、製品ユーザは、割り当てられたスコープにあるデバイスに限って表示できます (スコープは、データベース
クエリかまたはディレクトリの場所に基づきます)。

製品エージェント (標準の管理エージェントおよびインベントリ) が動作しているデバイスは、インベントリ スキャナによってコア データベースにスキャンされると、**[すべてのデバイス]**
リストに自動的に表示されます。通常、初期のデバイス構成の間に、最初のスキャンが実行されます。デバイスは、いったんコア
データベースにスキャンされると、管理対象デバイスとして扱われるようになります。つまり、コア
サーバによる管理が可能になります。デバイスの設定の詳細については、「クライアント エージェントの構成」を参照してください。

**[すべてのデバイス]**グループのデバイスは、インベントリ
スキャンによって自動的に入力されるので、デバイスを手動で検索する必要がまったくない場合もあります。ただし、まだコア データベースにはないデバイスを検索したり、非管理デバイスをサーバ
グループに移動したりするには、デバイス検索ツールを使用してネットワークでデバイスをスキャンできます。詳細については、「検索の使用方法」を参照してください。

**[すべてのデバイス]**グループは、各デバイスに関する次の情報を示します。**[すべてのデバイス]**をダブルクリックすると、リストが表示されます。

- **名前** :デバイス ホスト名 (Windows* コンピュータ名など)。
- **IP アドレス** :デバイスの IP アドレス。
- **ヘルス** :デバイスのヘルス
  ステータスと利用可能性。値は、正常、警告、危険のいずれかになります。
- **エージェント** :現在デバイス上で実行されているエージェント。
- **デバイス タイプ** :コンピュータのハードウェアの種類を表示 (AMT、IPMI、ASIC、または IPMI Advanced)。
- **オペレーティング システム**:デバイス上で実行されているオペレーティング システムのタイプ。
- **電源オン日時** :コンピュータがいつから中断されずに動作しているかを示す日時
  (データベースのタイム ゾーンで表示)。

デバイスを選択すると、デバイス リストの下にある **[プロパティ]**
ペインにデバイスのプロパティが表示されます。**[プロパティ]**ペインには、次に示す多くの重要なデバイス属性が表示されます。

- **ID** :デバイスの ID
  番号。この番号はデバイスが**[すべてのデバイス]**リストに追加された順番に従って割り当てられます。
- **IP アドレス** :デバイスの IP アドレス。
- **製造元** :デバイスの製造元です。
- **機種** :デバイスの機種型。
- **プロセッサ動作周波数** :デバイスの CPU の動作周波数です。
- **プロセッサ タイプ** :デバイスの CPU のタイプです。

コンソールから、詳細なインベントリの表示、およびアクション (レポートの実行など)
対象のデバイスの指定を行うことができます。

**[すべてのデバイス]**リストでデバイスをダブルクリックすると、サーバ情報コンソールが起動します。このコンソールには、デバイスの概要、構成、リモート コントロール オプション、およびアラート
ルールセット情報が表示されます。

## 公開グループ

**[公開グループ]**リストには、管理者権限を持つユーザによって作成されたデバイスのグループが表示されます。これらのグループは他のユーザにも表示されます。

このリストには、シャーシ管理モジュール (CMM)
を管理対象デバイスのリストに追加すると自動的に作成されるブレード シャーシ
グループも表示されます。このグループには、管理対象の CMM および対応する各ブレード
サーバが含まれます。シャーシ
グループは、自分で作成したグループを編集するときと同じ方法では編集できません。

グループは、静的または動的のどちらかにすることができます。動的グループには、プロセッサ動作周波数、デバイス OS、カスタム属性 (たとえばデバイス タイプ)
などの定義済みのフィルタ条件を満たすデバイスが含まれます。静的グループには、デバイスのリスト、他の静的グループ、または動的グループが含まれます。

## 非公開グループ

**[非公開グループ]**リストには、現在ログインしているユーザによって作成されたデバイスのグループが表示されます。他のユーザは、非公開グループを参照できないので、使用することもできません。

## デバイス アイコン

デバイス アイコンは、**[すべてのデバイス]**リストに表示され、各デバイスの現在のヘルス
ステータスを示します。デバイスのヘルス ステータスは、**[マイ
デバイス]**リストでデバイスを個別に選択して**[更新]**ツールバー
ボタンをクリックすることで更新できます。

次のテーブルは、デバイスとステータスのアイコンとそれらの意味を示します。

| アイコン | 説明 |
|---|---|
|  | 正常ステータスのデバイス |
|  | 警告ステータスのデバイス |
|  | 危険ステータスのデバイス |
|  | 不明ステータスのデバイス |

## ショートカット メニューの使用方法

コンソールのほとんどすべての項目
([グループ]、[デバイス]、[クエリ]、[スケジュールされているタスク]、[スクリプト] など) で、ショートカット (コンテキスト) メニューが使用できます。ショートカット
メニューにより、項目の共通タスクや重要な情報にすばやくアクセスできます。

項目のショートカット メニューを表示するには、項目を右クリックします。たとえば、**[マイ デバイス]**リストで管理対象デバイスを右クリックすると、通常、そのショートカット
メニューには次のオプションが表示されます。

- **グループから削除** :ユーザ定義グループから項目を削除します。
- **ターゲット** :選択したデバイスを [ターゲット デバイス] リストに移動します。**注意 :[ターゲット リスト]**にターゲット デバイスが表示されない場合、**[ターゲット デバイス]**タブにある**[更新]**をクリックします。
- **デバイスの Ping** :デバイスが起動しているかどうかを検証します。
- **デバイスの Tracert** :送受信されているネットワーク
  パケットと、パケットが送信先に達するまでに必要なホップ数を調べるためのルートのトレース コマンドを送信します。

このヘルプは、すべてのコンソール項目のショートカット
メニューを記載しているわけではないので、任意の項目を右クリックして使用可能なオプションを表示することをお勧めします。

## ツールの使用方法

ツールは、左ペインから使用できます。ペイン下部の矢印キーを使ってすべてのツールを表示します。

管理者には、左側のナビゲーション
ペインにすべてのツールが表示されます。他のユーザには、割り当てられた権限に対して許可されるツール（機能）のみが表示されます。たとえば、ユーザにレポート権限がない場合は、[レポート]
ツールは左側のナビゲーション ペインに表示されません。

ツールの完全なリストを次に示します。

- **ソフトウェア更新** :適用可能な更新パッケージをダウンロードします。
- **スクリプト** :スクリプトの作成と管理を行います。
- **スケジュールされているタスク**
  :スケジューラにある、（エージェント構成、脆弱性、デバイスの検索、またはスクリプトなどに基づく）すべてのタスク を表示します。
- **監視**
  :さまざまな属性を使用して、管理対象のデバイスのリアルタイムのパフォーマンスを監視します。
- **アラート**
  :アラート、しきい値、およびしきい値を超えた場合に本製品が使用する応答を構成します。
- **エージェント構成**IPMI（Baseboard Management Controller）、Linux、または Windows
  エージェントを構成します。
- **デバイス検索** :コア データベースでスキャンされないネットワーク上のデバイスを検索します。
- **ログ** : アラート
  ログを表示します。これは、管理デバイス上にフラグを立てたアラートを表示します。
- **レポート** :あらかじめ定義済みのサービスのレポートを管理します。
- **クエリ**
  :データベースに対するクエリを作成したり変更したりして、条件を満たすデバイスを特定します。
- **ユーザ**
  :ユーザの権限やスコープに基づいて、ユーザによるツールおよびデバイスへのアクセスを制御します。
- **プリファレンス** :カスタム インベントリ属性を作成したり、ライセンス情報を表示したりします。
- **ハードウェア構成** : Intel* AMT デバイスの構成オプションを表示するウィンドウを別に開きます。

ツール名をクリックすると、右ペインにツールのウィンドウが開きます。

## デバイス プロパティの表示

**[マイ**
**デバイス]**表示では、リスト内のデバイスをクリックして下のペインで**[プロパティ]**を選択することによって、デバイスに関する情報をすばやく表示できます。

デバイスに関する詳細情報は、インベントリ
データにあります。デバイスをクリックし、下のペインの**[インベントリの表示]**
タブを選択して完全な**[インベントリ]** ウィンドウを開くと、**[すべてのデバイス]** 表示にインベントリ
データを表示できます。

# デバイスのターゲット指定

[**ターゲット デバイス**] リストは、エージェントの導入や選択したデバイス グループに対するソフトウェア更新のためのスキャンなど、選択したデバイスでのタスクを実行する場合に役立ちます。

[ターゲット デバイス] リストに追加するデバイス数は、250 台以下にしてください。デバイスは、コンソール セッションがタイム アウト (アクティビティのない状態が 20 分継続) になるまでこのリストに入っています。

デバイスを [**ターゲット デバイス**] リストに追加するには、デバイスのリストのいずれかからデバイスを選択します。目的のデバイスが見つからない場合は、ツールバーの [**検索**] ボタンを使用します。1 台の特定のデバイスを検索したり、ワイルドカード % または * を使用して複数のデバイスを検索したりすることができます。[**ターゲット**] ツールバー ボタンをクリックして、[**ターゲット デバイス**] リストにデバイスを追加します。[ターゲット] ボタンが表示されない場合は、[<<] ボタンをクリックしてください。

複数のデバイスが検出される場合、リストに追加するデバイスを選択して、[ターゲット] をクリックします。返されたデバイスのリストが複数ページにわたる場合は、各ページで [**ターゲット**] をクリックしてください。複数のページのデバイスを選択することはできないので、すべてのページでこのボタンを 1 度ずつクリックします。右側のツールバー下部にある下向きの矢印をクリックして、1 ページに何台デバイスを表示するか設定できます。最大で 1 ページ 500 台まで表示可能です。リストの表示するデバイスの数を変更するには、[**プリファレンス**] の [ページの設定] を参照してください。

[**ターゲット デバイス**] リストに 1 台以上のデバイスが表示されている場合は、エージェント構成をターゲット デバイスに導入したり、非管理デバイスを [**マイ デバイス**] リストに移動したりすることができます。

**デバイスをターゲットとするには**

1. [**マイ デバイス**] リストまたは [**検出されたデバイス**] ビューで、アクション実行のターゲットとするデバイスをクリックします。複数のデバイスを選択するには、複数選択の標準的な方法 (Shift キーを押しながらクリック、または Ctrl キーを押しながらクリック) を使用してください。
2. [**ターゲット**] ボタンをクリックします。[ターゲット] ボタンが表示されていない場合は、ツール バーの [<<] をクリックします。このボタンはツール バーの一番右端にあります。

選択したデバイスは、下のペインの [**ターゲット デバイス**] タブに一覧表示されます。デバイスがこのタブに一覧表示されると、ツール (エージェントの導入など) を開いてターゲット デバイスに適用するタスクをスケジュールできるようになります。非管理デバイスをターゲットとした場合は、[**管理**] タブをクリックすると [**マイ デバイス**] リストに移動できます。

# 表示リストのフィルタ

[**マイ デバイス**] リストには、リスト内に表示するデバイスを決定するのに使用するフィルタ アイコンがあります。デバイス名または IP アドレスのいずれか 1 つの条件のみでフィルタすることも、条件を組み合わせて一部のコンピュータに焦点を合わせることもできます。

**表示リストをフィルタするには**

1. [**マイ デバイス**] リストで、[**すべてのデバイス**] をダブルクリックするか、グループを選択します。
2. ツールバーの [**フィルタ**]  をクリックします。
3. ドロップダウン リストから、[**デバイス名**] または [**IP アドレス**] を選択します。
4. テキスト ボックスに情報を入力して、指定した条件のパラメータを設定します。[**検索**] ボックスでは、「,」、「 ‘ 」、「 “ 」、および「!」という拡張文字はサポートされていません。

   デバイス名によりフィルタする場合は、ホスト名またはコンピュータ名の範囲を入力します。ワイルドカード文字を使用して、特定のコンピュータ名を検索することもできます (例 : *srv)。

5. [**検索**] をクリックします。

# グループの使用方法

デバイスをグループ化することによって、管理を容易にすることができます。グループを作成し、機能、場所、部門、デバイス属性、または必要に応じた他のカテゴリに基づいてデバイスを整理できます。たとえば、Web サーバとして構成されたすべてのサーバを含む Web サーバ グループ、または特定の OS を実行するすべてのデバイスを含むグループを作成できます。グループを右クリックして、そのグループを開いたり、削除したり、またはそのグループに含まれているすべてのデバイスをアクション (アラートのルールセット、およびエージェント導入など) をターゲットとしたりすることができます。

メインの [**マイ デバイス**] ビューには、次のグループが表示されます。

- **すべてのデバイス** :
  現在ログインしているユーザが、ユーザのスコープに基づいて表示できるすべてのデバイスをフラット リスト (サブグループのない) に一覧表示します。管理者の場合は、コア データベースにスキャンまたは移動されたすべてのデバイスが [**すべてのデバイス**] に一覧表示されます。標準管理エージェントが構成されているデバイスは、インベントリ スキャナによってコア データベースにスキャンされると、[**すべてのデバイス**] グループ/フォルダに自動的に表示されます。ユーザは、管理者を含め、[**すべてのデバイス**] にグループを作成することはできません。

- **公開グループ**: 管理者が [**すべてのデバイス**] グループから追加したグループ/デバイスとブレード シャーシ グループを一覧表示します。管理者 (管理者権限があるユーザ) はこのグループのデバイスをすべて表示できますが、ほかのユーザはスコープで許可されたデバイスのみを表示できます。管理者のみが [**公開グループ**] にグループを作成できます。
- **非公開グループ**: ユーザのスコープに基づき、現在ログインしているユーザのグループ/デバイスを一覧表示します。ユーザは、[**非公開グループ**] にのみデバイス サブグループを作成できます。[**公開グループ**] および [**すべてのデバイス**] グループからデバイスを移動またはコピーすることによって、[**非公開グループ**] またはそのサブグループにデバイスを追加できます。すべてのユーザは、[**非公開グループ**] にグループを作成できます。

---

デバイス ビューで表示、管理できるデバイス、および使用可能な管理ツールについては、「役割ベース管理」を参照してください。

---

## グループ タイプ

次の 2 つのタイプのグループを作成および管理できます。

- **静的グループ**。*静的グループ*は、そのグループに手動で追加されたデバイスで構成されています。静的グループを変更するには、手動でデバイスを追加または削除する必要があります。
- **動的グループ**。*動的グループ* は、フィルタまたはクエリ定義を満たすコンピュータで構成されています。動的グループを展開するたびに、クエリが実行され、その結果が表示されます。たとえば、1 つの動的グループに現在警告状態にあるすべてのデバイスを含めることもできます。サーバは、ステータスが変わると、このグループに追加されるか、このグループから削除されます。

**静的グループを作成するには**

1. コンソールのデバイス ビューで、親グループ (たとえば [**非公開**] グループ) をダブルクリックし、[**グループの追加**] をクリックします。
2. 新しいグループの名前を入力します。
3. [**静的**] をクリックし、[OK] をクリックします。

静的グループを作成したら、デバイスをリストから選択してツールバーの [**移動/コピー**] をクリックすることによって、グループに移動またはコピーできます。デバイスを [**すべてのデバイス**] リストからあるグループにコピーしたり、別のグループから移動/コピーしたりすることができます。

**動的グループを作成するには**

1. コンソールのデバイス ビューで、親グループ (たとえば [**非公開**] グループ) をダブルクリックし、[**グループの追加**] をクリックします。
2. 新しいグループの名前を入力します。

3. [**動的**] をクリックし、[OK] をクリックします。

動的グループを作成したら、そのグループに表示するコンピュータを決定するためのフィルタを作成する必要があります。新しいフィルタを作成するか、既存のクエリに基づいてフィルタを作成できます。

**新しいフィルタを作成するには**

1. 作成した動的グループを選択します。これにより、下のペインに**グループのプロパティ**が表示されます。
2. [**グループのプロパティ**] から、[**新規フィルタの作成**] を選択し、[**新規フィルタ**] をクリックします。
3. 使用するフィルタ条件を選択して、[OK] をクリックします。

**既存のクエリに基づいてフィルタを作成するには**

1. 作成した動的グループを選択します。これにより、下のペインに**グループのプロパティ**が表示されます。
2. [**グループのプロパティ**] から、[**既存のクエリに基づいてフィルタを作成してください**] を選択します。
3. グループのフィルタに使用する既存のクエリを選択し、[**新規フィルタ**] をクリックします。
4. 使用する別のフィルタ条件を追加して、[OK] をクリックします。

既存のクエリに基づいてフィルタを作成した後でクエリが変更された場合、そのクエリに基づくフィルタが変更内容に応じて動的に変更されることはありません。

# [アクション] タブの使用方法

**[アクション]** タブを使用して、選択したサーバやターゲット
デバイス上で操作を行います。管理コンピュータのリストからデバイスを削除したり、デバイスのパワーオン、パワー オフ、再起動、および管理デバイスとの接続の監視が行えます。

- デバイスの削除
- 電源オプション
- デバイス監視

## デバイスの削除

**[デバイスの削除]** を使用して、管理コンピュータのリストから選択したデバイスやターゲット
デバイスを削除できます。削除機能により、System Manager の任意のグループ
(既定のグループまたはユーザが作成したグループ) から 1
つまたは複数のデバイスを削除できます。デバイスがグループから削除されると、既定の
**[すべてのデバイス]** グループを含む、管理またはインベントリ
デバイスのすべてのリストから完全に削除されます。

多数のデバイスを削除すると、操作がタイムアウトする可能性があります。操作がタイムアウトした場合、その操作をより小さな操作に分割してください。

# 電源オプション

**[電源オプション]** を使用して、パワー オフ、再起動を行うことができ、管理 IPMI コンピュータの場合は、リモート デバイスのパワー オンを行うことができます。非 IPMI サーバの場合、デバイスは LANDesk エージェントを導入して、再起動、およびパワーオフ機能を実行できるようにする必要があります。IPMI コンピュータでは、パワーオン/パワーオフ機能や再起動機能を実行するために必要な IPMI 資格情報を備える必要があります。IPMI ボックスに LANDesk エージェントを導入すると、IPMI 資格情報がなくてもパワーオフ機能および再起動機能を実行できます。SVCCFG.EXE を使用して、サービス設定ユーティリティ IPMI サーバの管理に使用する IPMI BMC パスワードを設定します。

**電源オプションを使用するには**

1. **[マイ デバイス]** リストで、デバイスをクリックするか、デバイスのリストを ターゲットに指定します。
2. 下のペインで、**[アクション]** タブをクリックします。
3. **[電源オプション]** をクリックします。
4. [ターゲット デバイス] にあるデバイスについてアクションを実行するか、または選択したデバイスについてのみアクションを実行するかを選択します。
5. 次のオプションから選択します。
   - 再起動
   - 電源オフ
   - パワー オン (IPMI 対応デバイスと Wake on LAN 対応デバイスで機能)

6. **[コンソール リダイレクション ウィンドウを表示する]**をクリックして、ラウンチャのあるウルトラスリム コンテナを起動します (ラウンチャは、TTY コントロールよりも非常に容易に EM64T 向けに再コンパイルできます)。

   管理 IPMI サーバのパワーをオンにするか再起動する場合、サーバのブート情報を表示するコンソール リダイレクション ウィンドウを開くことができます。これは、サーバが再起動中か確認する場合に有用です。また、このコンソール ウィンドウを使って起動プロセスを中断し、管理されるサーバの BIOS 設定を変更することもできます。

   コンソール リダイレクション ウィンドウを表示するには、サーバの BIOS 設定でシリアル ポート経由のコンソール リダイレクションを有効にしておく必要があります。コンソールのデータはシリアル ポートに送られます。サーバと管理者コンソールを接続しているシリアル ケーブルがある場合、コンソール リダイレクションはそのケーブル経由で行われます。ない場合、System Manager は Serial over LAN (SOL) 接続を開始して、データをシリアル ポートから LAN 接続にリダイレクトします。SOL 接続は、コンソール ウィンドウが開いている間維持されます。コンソール データの表示が終了したら、ウィンドウを閉じてください。

   コンソール ウィンドウが開くと、第二のメッセージ ウィンドウが開きます。メッセージ ウィンドウは閉じることができます。コンソール リダイレクション ウィンドウが開いた後でコンソールがブート シーケンスを表示する前に、ウィンドウに文字がランダムに表示されることがあります。この文字は、サーバの BMC がハートビート メッセージを送信しているために表示されます。このメッセージは管理者コンソールへの接続に送信されています。コンピュータが起動画面を表示している間、文字は表示されませんが、起動処理が終了した後で再度表示されることがあります。

## デバイス監視

デバイス監視を使用して、選択したデバイスの接続をチェックします。デバイスがネットワーク接続を失うと、コア サーバにアラートを送信できません。デバイス監視はデバイスがネットワーク上で通信できるかどうかをチェックします。

1. **[すべてのデバイス]** リストで、デバイスをクリックするか、デバイスのリストを ターゲットに指定します。
2. 下のペインで、**[アクション]** タブをクリックして、**[デバイス モニタ]**をクリックします。
3. 現在監視されているデバイスのリストを表示するには、**[監視デバイスの表示]**をクリックします。
4. ping スイープの間隔 (分) と、本製品がデバイスとの通信を試行する回数を入力します。
5. アクションを [ターゲット デバイス] リストにあるデバイスに対して実行するか、**[すべてのデバイス]** グループにあるすべてのデバイスに対して実行するかを選択します。
6. すべてのデバイスの監視を停止するには、**[デバイスを Ping しない]** を選択します。

7. **[適用]**をクリックします。

最後にターゲット指定したデバイスのグループだけが監視されます。たとえば、ターゲット デバイス A とデバイス B を選択してデバイス監視を適用した場合、コア サーバはデバイス A とデバイス B に対してのみ ping を実行します。次にデバイス C とデバイス D を選択してデバイス監視を適用した場合、デバイス C とデバイス D だけが監視され、デバイス A とデバイス B は監視されなくなります。

# カスタム列

列の名前とフィールドを変更するには、**カスタム列**を使用します。名前は列の名前で、フィールドには列に表示できる属性（その属性が存在する場合）が表示されます。列の変更内容は、他のユーザからは見えません。カスタム列の変更内容は、[**マイ デバイス**] ビューに表示されます。

この製品には、7 つの列を持つ既定の列セットが含まれています。既定のセットを編集することはできませんが、カスタム列セットを既定として使用するために定義することはできます。

複数のフィールド名を持つ可能性のあるカスタム列を作成することは奨励しません。たとえば、[Computer.Software.Package.Name] フィールドを作成しようとしているとき、デバイスに複数のパッケージがインストールされている場合、同じデバイスには異なるパッケージ名が存在していても、System Manager には 1 行に 1 つのパッケージ名しか表示されないため、[**すべてのデバイス**] リストに同じデバイスのエントリが複数表示されることになります。

**カスタム列セットを作成するには**

1. 左側のナビゲーション ペインで、[**プリファレンス**] をクリックします。
2. [**カスタム列**] タブをクリックします。
3. [**新規**] をクリックします。
4. 列セットの名前を入力します。

5. 上のボックスで、列セットに含めるすべての列の見出しを選択し、[**追加**] をクリックします。.

   データベースに現在あるすべてのインベントリ
   データのリストを示すボックスが表示されます。このリストをドリル
   ダウンし、クエリ結果リストに表示する属性を選択します。クエリで返されるクライアントの識別に
   役立つ属性を選択してください。表示する属性が見つからない場合は、[カスタム属性]
   ダイアログで追加できます。ただし、これらの属性をクエリ
   ダイアログに表示するには、コンピュータに割り当てておく必要があります。

   **注意**：1:*
   関係を持つデータベース内の属性を選択した場合、そのデバイスの重複エントリが作成されます
   。1 対 1 の関係を持つ属性を選択した場合 ([Computer.System.Asset] タグなど、可能な属性が
   1 つしかない場合)、重複エントリは作成されません。

6. 列の順番を変更するには、列の見出しを選択して [**上へ移動**] または [**下へ移動**]
   をクリックします。
7. 列を削除するには、下のボックスで該当の列を選択して [**削除**] をクリックします。
8. 列に表示される見出しを変更するには、下のボックスで見出しを選択して [**編集**]
   をクリックし、変更して Enter キーを押します。次の拡張文字はサポートされていません。< , > , ' , ″ , !.
9. [OK] をクリックして、列セットを保存します。
10. [**すべてのデバイス**]
    リストを表示するときカスタム列セットを使用するには、カスタム列セットを選択してツールバーの
    [Set as current column set (現在の列セットとして設定)] をクリックします。

**カスタム列セットを編集するには**

1. 左側のナビゲーション ペインで、[**プリファレンス**] をクリックします。
2. [**カスタム列**] タブをクリックします。
3. カスタム列セットを選択し、[Edit] をクリックします。
4. 上のボックスで列の見出しを選択し、[**追加**] をクリックして列を追加します (上記のステップ 5
   にある注意を参照してください)。
5. 列を削除するには、下のボックスで該当の列を選択して [**削除**] をクリックします。

6. 列に表示される見出しを変更するには、下のボックスで見出しを選択して [**編集**]
   をクリックし、変更して Enter キーを押します。次の拡張文字はサポートされていません。< , > , ' , ″ , !.
7. 列の順番を変更するには、列の見出しを選択して [**上へ移動**] または [**下へ移動**]
   をクリックします。
8. [OK] をクリックして変更内容を保存します。

# カスタム属性

属性とは、デバイスに属する特性またはプロパティのことです。データベース内のデバイスの属性が多いほど、デバイスを一意に識別しやすくなります。LANDesk® Server Manager

を管理者権限で使用している場合にのみ、カスタム属性を作成できます。カスタム属性が作成されてコア
データベースに追加されると、管理デバイスに対してこれらの属性の値を割り当てることができます。コア
データベースにカスタム属性がまったく追加されていない場合には、**[属性の割り当て]**オプションが**[アクション]** タブに表示されません。

## カスタム属性をデバイスに割り当てるには

1. **[すべてのデバイス]** リストで、デバイスまたは複数デバイスをクリックします。
2. 下のペインで、**[アクション]** タブをクリックします。
3. 左ペインから **[属性の割り当て]** を選択します。
4. 各属性名には値のドロップダウン リストがあります。属性名のドロップダウン
   リストから値を選択します。必要に応じてこの操作を繰り返します。**[選択されたデバイス]**をクリックします。
5. **[割り当て]**をクリックしてから、**[OK]**をクリックします。

カスタム属性はターゲット指定した複数デバイスに割り当てることができます。[ターゲット]
リストにデバイスがある場合、上記手順 4 の**[ターゲット デバイス]**をクリックします。

# ページ設定

**[ページ設定]**
では、デバイスの一覧表示またはグラフィックスの表示を行うページの表示設定を指定します。

1. 左側のナビゲーション ペインで、**[プリファレンス]** をクリックします。
2. **[ページ設定]** タブをクリックします。
3. **[グラフの種類]** ドロップダウン リストから、**レポート**に表示するグラフの種類を選択します。
4. **[アイテム/ページ]**
   ボックスに、ページ付けする場合に各ページに表示されるアイテム数の上限を入力します。値は 500 アイテム以内でなければなりません。

## ビギナー モード

ツールバーのボタンにテキストを表示させて、新しいユーザが機能を特定しやすくなるようにします。このオプションが選択されない場合、アイコンのみがツールバーに表示されます。アイコンにマウスを当てるとテキストが表示されます。

1. ツールバーのボタン以外にテキストを表示させるには、**[ツールバーにテキストを表示する]**
   をクリックします。
2. **[更新]** をクリックします。

# サーバ情報コンソールの表示

サーバ情報コンソールを使用して、デバイスに関するトップレベルの概要情報の表示、CPU などのシステム情報やファン情報の表示、デバイスのキー コンポーネントのヘルス ステータスやしきい値の監視、脆弱性の管理、およびデバイスのパワー オン、パワー オフ、再起動を行います。サーバ情報コンソールには、左側のナビゲーション ペインに以下のセクションがあります。

- システム情報
- ソフトウェア更新
- 監視
- ルールセット
- 電源オプション
- ハードウェア構成

---

デバイスのサーバ情報コンソールを表示するには、まず標準の管理エージェントをそのデバイスにインストールする必要があります (「エージェントの構成」を参照)。また、サーバ情報コンソールが正しく機能するには、エージェントのインストール後にデバイスを再起動する必要があります。この再起動は、エージェントをコア サーバ上および管理デバイス上にインストールした場合に必要になります。

---

**サーバ情報コンソールを表示するには**

1. **[マイ デバイス]** 表示でデバイス名をダブルクリックします。

   コンソールが新しいブラウザのウィンドウを開き、デフォルトで **[ヘルス概要]** ページを表示します。

2. 左側のナビゲーション ペインのボタンをクリックして、サーバ情報を表示して利用可能なツールを使用します。

## システム情報

**[システム情報]** ページには、デバイスのヘルスの概要データと、ハードウェアとソフトウェアに関する情報、システム ログ、および資産やネットワーク情報などのデータが含まれます。

## ヘルス概要

**[ヘルス概要]** ページは、このデバイスのシステム ヘルスの概要をすばやく提供します。選択したハードウェアが正常に機能しているかどうか、注意すべき問題があるかどうかが一目でわかります。

いずれかのヘルス要素が警告または危険な状態になった場合、それに対応するボタンに問題が存在することを表す黄色 (警告) または赤 (危険)
のボタンが表示されます。そのボタンをクリックすると、警告または危険アラートを引き起こしたイベントの詳細が表示されます。

## システム概要

**[システム概要]**
ページでは、選択したデバイスに関する重要な情報を表示します。このページに一覧表示されている情報には、そのデバイスのハードウェア構成とソフトウェア構成に応じて次のような情報があります。

- **ヘルス** :設定した条件とパラメータで定義される、デバイスの全体的なヘルス状態。
- **タイプ** :印刷、アプリケーション、データベースなどのデバイスのタイプ。
- **製造元** :デバイスの製造元。
- **機種** :デバイスの機種型。
- **BIOS バージョン** :デバイスの BIOS のバージョン。
- **オペレーティング システム**:デバイスのオペレーティング システム。
- **OS バージョン** :オペレーティング システムのバージョン番号。
- **CPU** :デバイスのプロセッサの製造元、機種、および速度。
- **脆弱性スキャナ** :脆弱性スキャナのバージョン。
- **リモート コントロール** :リモート コントロール エージェントのバージョン。
- **ソフトウェア配布** :ソフトウェア配布エージェントのバージョン。
- **インベントリ スキャナ** :インベントリ スキャナのバージョン。
- **IPMI タイプ、IPMI バージョン** : デバイスが使用している IPMI のタイプとバージョン。
- **SDR バージョン** :デバイスの BMC の SDR (Sensor Data Record: センサー データ レコード) のバージョン。
- **BMC バージョン** : デバイスの Baseboard Management Controller (ベースボード管理コントローラ) のバージョン。
- **カーネル** : Linux デバイスの場合、インストールされているカーネルのバージョン番号。
- **監視** :デバイスの監視エージェントのバージョン番号。
- **CPU 使用率** :プロセッサの現在の使用率。
- **使用されている物理メモリ*** :デバイス上で使用されている総物理メモリの割合。
- **仮想メモリ使用量*** :デバイス上で使用されている仮想メモリの割合。
- **前回の再起動*** :デバイスが前回再起動した日時 (データベースのタイム ゾーン)。
- **ドライブ** : デバイス上のドライブ、そのドライブの総容量と使用量の割合。

この情報は、Windows のレジストリまたは Linux の設定ファイルから取得されます。

*この情報はエージェントがデバイスにインストールされている場合に表示されます。

## ハードウェア

**[ハードウェア]**
ページを使用すると、デバイスのハードウェア構成の詳細が表示されます。**[ハードウェア]**
リストの項目は、次のカテゴリにグループ分けされています。すべてのカテゴリが表示されないデバイス

もあります。たとえば、デバイスにファンと温度センサーがない場合には、リストに **[冷却装置]** カテゴリは表示されません。

- **CPU** : プロセッサとキャッシュ
- **ストレージ** : 論理ドライブ、物理ドライブ、リムーバブル メディア、およびストレージ アダプタ
- **メモリ** : 使用情報とメモリ モジュール
- **シャーシ**: サーバのシャーシ: ケースが開いているか閉じているかを表示
- **入力デバイス** : キーボード、マウス、その他のデバイス
- **マザーボード** : マザーボード、拡張スロット、および BIOS
- **冷却装置** : ファンおよび温度センサー
- **電源** : パワーサプライと電圧

**ハードウェア項目のアラートしきい値の設定**

**[ハードウェア]**
リストの一部の項目は、温度センサーなど、デバイスのセンサーからのデータを表しています。管理デバイスにサポートされているセンサーを持つコンポーネントがある場合、アラートを発生させるセンサーの数値を変更することができます。たとえば、CPU
温度センサーでは警告および危険アラートを発する数値を低くしたり高くしたりできます。しきい値は通常製造元の推奨設定にもとづいていますが、**[しきい値]** ダイアログ
ボックスを使えば、この上限設定と下限設定を変更することが可能です。

1. サーバ情報コンソールで **[システム情報]** をクリックします。
2. **[ハードウェア]** フォルダを展開して目的のハードウェア要素までドリルダウンします (たとえば **[冷却装置]**、**[温度]**など)。
3. センサーのリストからしきい値を変更するセンサーをダブルクリックします。
4. 下限および/または上限のしきい値テキストボックスに値を入力するか、あるいはトラックバーのスライダを左または右に動かして値を変更します。
5. **[更新]**をクリックして変更内容を保存します。
6. しきい値を元の設定に戻すには、**[既定値の復元]**をクリックします。

## ログ

[ログ] ページには、ローカルのシステム ログ、IPMI 対応デバイスのシステム イベント ログ (SEL)、およびアラート ログが表示されます。

アプリケーション、セキュリティ、システム ログなどのローカル
ログにはコンソールからログをクリアするボタンはありませんが、Windows の [コンピュータの管理] を使ってログを表示およびクリアできます。

デバイスの BIOS に SMBIOS ログのクリア機能がある場合には、**[Clear log]**ボタンをクリックしてログエントリをすべて削除します。BIOS
がこの操作をサポートしていない場合には、このボタンは利用できません。

## ソフトウェア

**[ソフトウェア]**
ページでは、プロセス、サービス、およびこのデバイスのパッケージの概要情報と現在の環境変数の一覧が表示されます。

- **プロセス** :
  実行中のプロセスを表示します。プロセスを終了させるには、そのプロセスを選択してから **[プロセスの強制終了]** をクリックします。
- **サービス** :
  デバイス上で利用可能なサービスとそのステータスを表示します。変更するには、サービスを選択して **[停止]**、**[開始]**、または **[再起動]** をクリックします。
- **パッケージ** :
  インストールされているパッケージとそのバージョン番号およびベンダ名を一覧表示します。
- **環境** : 現在デバイスで設定されている環境変数を一覧表示します。

## その他

**[その他]** ページでは、資産情報およびネットワーク ハードウェアと接続の概要を表示します。

- **資産情報** :
  場所や資産タグ番号などの資産管理情報の表示と編集を行います。また、シリアル番号、製造元、シャーシ タイプなどのシステム情報も表示されます。
- **ネットワーク情報** : インストールされているネットワーク
  ハードウェアの一覧、ネットワーク活動の概要、構成の概要 (IP アドレス、既定のゲートウェイ アドレス、および WINS、DHCP、DNS サーバ情報を含む)、および現在のネットワーク接続リスト (マップされたドライブ) が表示されます。

## ソフトウェア更新

**[ソフトウェア更新]**ページを使用して、選択したデバイスにおける脆弱性をスキャンします。

**検出された脆弱性を確認するには**

1. **[マイ デバイス]** ビューで、設定するデバイスをダブルクリックします。新しいブラウザ ウィンドウにサーバ情報コンソールが開きます。

2. 左側のナビゲーション ペインで、**[ソフトウェア更新]**をクリックします。

**列についての説明**

- **ID** :ベンダ定義の固有の英数字コードで脆弱性を識別します。
- **重要度**
  :脆弱性の重要度を示します。重要度には、[サービスパック]、[重要]、[高]、[中]、[低]、[該当なし]、[不明] があります。

- **タイトル** :脆弱性の性質またはターゲットを簡単なテキスト文字列で説明します。
- **言語** :脆弱性の影響を受ける OS の言語を示します。
- **公開日** :ベンダによって脆弱性が公開された日付を示します。
- **サイレント インストール** :脆弱性に対応するパッチ
  ファイルを、ユーザの介入なしに自動的にインストールするかどうかを示します。一部の脆弱性には複数のパッチがあります。脆弱性のパッチのうち自動的にインストールしないものがある場合は、**[サイレント インストール]** 属性を **[いいえ]** にします。
- **修復可能** :脆弱性がパッチ
  ファイルの配布やインストールによって修復可能かどうかを示します。利用できる値は、次のとおりです。[はい]、[いいえ]、[一部
  (複数の検出ルールを含む脆弱性については、検出されたすべての脆弱性が修復可能とは限らない)] 。

## 監視

**[監視]**を使用して、パフォーマンス カウンタおよびグラフを表示し、デバイス
コンポーネントのしきい値を設定します。この機能の詳細については、「デバイスの監視」セクションを参照してください。

**監視するパフォーマンス カウンタを選択するには**

1. **[マイ デバイス]** ビューで、設定するデバイスをダブルクリックします。新しいブラウザ
   ウィンドウにサーバ情報コンソールが開きます。

2. 左側のナビゲーション ペインで、**[監視]** をクリックします。
3. **[パフォーマンス カウンタの設定]**をクリックします。
4. **[オブジェクト]**列から、監視するオブジェクトを選択します。
5. **[インスタンス]**列から、監視するオブジェクトのインスタンスを選択します (該当する場合)。
6. **[カウンタ]**列から、監視する特定のカウンタを選択します。
7. ポーリング頻度およびカウンタ履歴を維持する日数を指定します。
8. **[カウンタが範囲を超えた後にアラート]**テキスト ボックスで、
   アラートが生成される前にカウンタがしきい値を超えることを許可される回数を指定します。
9. しきい値の上限/下限を指定します。
10. **[適用]**をクリックします。

**監視対象カウンタのパフォーマンス グラフを表示するには**

1. **[アクティブなパフォーマンス カウンタ]**タブをクリックします。
2. リストからカウンタを選択します。
3. **[カウンタ]** リストから、パフォーマンス グラフを表示するカウンタを選択します。
4. **[リアルタイム
   データの表示]**を選択して、現在のパフォーマンスのグラフを表示するか、または**[履歴データの表示]**を選択して、カウンタの選択時に ([履歴の保存] で)
   指定した期間のパフォーマンスを示すグラフを表示します。

パフォーマンス
グラフの横軸は経過した時間を表します。縦軸は測定単位を表します。たとえば、バイト/秒
(ファイル転送などを監視する場合)、パーセント (CPU 使用率などを監視する場合)、利用可能なバイト数
(ハード ドライブ容量などを監視する場合) があります。

## ルールセット

**[ルールセット]**ページを使用して、選択したデバイスに割り当てられたアラートと監視ルールセット構成のリストを表示したり、各アラートの詳細を表示します。

**アラート ルールセットを表示するには**

1. **[マイ デバイス]**ビューで、設定するデバイスをダブルクリックします。コンソールが新しいブラウザ ウィンドウに表示されます。
2. 左側のナビゲーション ペインで、**[ルールセット]**をクリックします。
3. **[アラート ルールセット]** タブをクリックします。

次のテキストでは、各アラートに関する詳細を説明します。これらの詳細の変更については、「アラートの使用方法」を参照してください。

- **状態変化** :アラートの状態が表示された状態に達すると、アラートが生成されます。
- **健全性に影響**
  :アラート状態が指定したしきい値に達すると、その状態によってデバイスの全体的なヘルス状態が影響を受けます。ヘルスに影響するアラートの選択は、[アラート ルールセット] ダイアログで設定します。
- **ルールセット名** :[アラート ルールセット] ダイアログで定義された、アラート ルールセットの名前。
- **アラート タイプ** :電子メール、SNMP トラップ、プログラムの実行など、生成されるアラートの種類。
- **アクションの構成** :[アクション ルールセット] ダイアログで定義されている、アラート生成時に発生するアクションです。
- **アラート ハンドラ** :電子メール ハンドラなど、アラートに関連したハンドラ。
- **インスタンス** :アラートのソースを表します。

**監視ルールセットを表示するには**

1. **[マイ デバイス]** ビューで、設定するデバイスをダブルクリックします。新しいブラウザ ウィンドウにサーバ情報コンソールが開きます。
2. 左側のナビゲーション ペインで、**[ルールセット]** をクリックします。
3. **[監視ルールセット]** タブをクリックします。

次のテキストでは、各監視ルールセットに関する詳細を説明します。これらの詳細の変更については、「監視について」を参照してください。

- **名前** :[監視] ページで定義された、ルールセット構成の名前。
- **ルールセット名** :ルールセットが既定かそうでないかを示します。
- **有効** :ルールセットのデバイスでの実行が有効か無効かを示します。

- **警告しきい値** :指定した値を超えた場合にデバイスがコア
  サーバに警告メッセージを送信するしきい値。
- **危険なしきい値** :指定した値を超えた場合にデバイスがコア
  サーバに危険メッセージを送信するしきい値。
- **チェック間隔** :項目を監視する頻度。

## 電源オプション

**[電源オプション]**を使用して、パワー オフ、再起動を行うことができ、管理 IPMI および Intel AMT
コンピュータの場合は、リモート デバイスのパワー オンを行うことができます。非 IPMI
サーバの場合、サーバは LANDesk
エージェントを導入して、再起動、およびパワーオフ機能を実行できるようにする必要があります。

IPMI と Intel AMT
デバイスでは、パワーオン/パワーオフ機能や再起動機能を実行するために必要な資格情報を設定する必要があります。IPMI または Intel AMT デバイスに LANDesk エージェントが導入されている場合、IPMI または Intel AMT 資格情報がなくても、パワー オフおよび再起動機能を実行できます。IPMI デバイスの BMC 資格情報または Intel AMT
デバイスの資格情報を設定するには、サービス設定ユーティリティを使用します
(「サービスと資格情報の設定」を参照)。

**選択したデバイスの電源オプションを使用するには**

1. **[マイ デバイス]**ビューで、設定するデバイスをダブルクリックします。コンソールが新しいブラウザ ウィンドウに表示されます。
2. 左側のナビゲーション ペインで、**[電源オプション]** をクリックします。
3. 次のオプションから選択します。

   -  再起動
   -  パワー オフ
   -  電源オン

## ハードウェア構成

**[ハードウェア構成]** ツールを使えば、IPMI または Intel* AMT
機能を持つデバイスのオプションを設定できます。このツールおよび任意のオプションは、対応するハードウェアを持つデバイスでのみ表示されます (たとえば、IPMI オプションはデバイスが IPMI
デバイスとして認識された場合にのみ表示されます。

Intel AMT デバイスのプロビジョニング用の ID の生成、生成された ID の表示、および Intel AMT
デバイスのプロビジョニングに関連した構成オプションの変更が行えます。さらに、デバイス上の疑わしいネットワーク アクティビティを検出およびブロックする回路ブレーカー
ポリシーも定義でき、またエージェント

プレゼンス監視機能を有効にしてデバイスの管理エージェントの継続的実行を確実にできます。詳細については、「Intel AMT サポート」を参照してください。

IPMI デバイスの場合には、ウォッチドッグ タイマ、電源オプション、および BMC ユーザ設定などの構成オプションをカスタマイズできます。また、IPMI デバイスとのアウトオブバンド通信を維持するために LAN チャネルを使用するか、シリアル オーバー LAN を使用するかを設定できます。詳細については、「IPMI BMC 構成」を参照してください。

Dell* DRAC (Remote Access Controller) のあるデバイスの場合には、Dell DRAC ログを表示し、OpenManage Server Administrator へのアクセス用ユーザ名の編集ができます。詳細については、「Dell DRAC デバイスの管理」を参照してください。

# Intel* AMT デバイスの管理

Intel* AMT デバイスが検出されて管理するためにコア データベースに追加されると、デバイスに LANDesk エージェントがインストールされていなくても、そのデバイスをいくつか制限のある方法で管理できます。(デバイスの検出とコア データベースへの移動方法については、「Intel* AMT デバイスの検出」を参照してください。)

デバイスに Intel AMT のみが構成されている場合と、Intel AMT と System Manager 管理エージェントがある場合とを比較して、使用可能な管理オプションを次の表に一覧表示しています。

| | Intel AMT のみ | Intel AMT とエージェント | エージェントのみ |
|---|---|---|---|
| インベントリ | 概要 | /X= | /X= |
| イベント ログ | /X= | /X= | /X= |
| リモート ブート マネージャ | /X= | /X= | |
| OS ネットワークの無効化 | | /X= | |
| OS ネットワークの有効化 | | /X= | |
| 再起動時の vulscan 強制実行 | | /X= | |
| インベントリ履歴 | | /X= | /X= |

| | Intel AMT のみ | Intel AMT とエージェント | エージェントのみ |
|---|---|---|---|
| リモート コントロール | | /X= | /X= |
| チャット | | /X= | /X= |
| ファイル転送 | | /X= | /X= |
| リモート実行 | | /X= | /X= |
| ウェイクアップ | | /X= | /X= |
| シャットダウン | | /X= | /X= |
| 再起動 | | /X= | /X= |
| インベントリ スキャン | | /X= | /X= |
| スケジュールされているタスクとポリシー | 制限がある | /X= | /X= |
| グループ オプション | | /X= | /X= |
| インベントリ レポートの実行 | | /X= | /X= |
| Intel AMT アラート | | /X= | /X= |

**デバイスの Intel AMT インベントリの概要を表示するには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [Intel AMT オプション] をクリックします。
3. [インベントリの概要] をクリックします。

この概要には、デバイスの GUID、製品および製造元、シリアル番号、および BIOS、プロセッサ、メモリの概要、Intel AMT

バージョン番号が表示されます。いずれかの情報が足りない場合は、[インベントリを更新する] をクリックしてデータを更新することができます。

## Enterprise モードで提供されているデバイスにアクセスする

Intel AMT デバイスを Enterprise モードで提供した場合、コア サーバは安全な通信のためにデバイスに証明書をインストールします。別のコア サーバが管理するデバイスの場合、いったん提供を解除してから新しいコア サーバで再度提供を行う必要があります。そうしないと、新しいコア サーバに一致する証明書がないので、デバイスの Intel AMT アクセスは応答しません。同様に、他のコンピュータがそのデバイスの Intel AMT 機能にアクセスしようとしても、一致する証明書がないのでアクセスできません。(プロビジョニング モードの詳細については「Intel* AMT サポート」を参照してください。)

## Intel AMT イベント ログ

System Manager には、Intel AMT デバイスが生成するイベント ログを表示するウィンドウがあります。このログにキャプチャされるイベントの種類は設定に依存します。イベントの日時、イベントのソース ([エンティティ] 列)、説明、および Intel AMT 設定で定義された重要度 (重要または重要でない) を表示できます。また、ログ データは、CSV (コンマ区切りの値) 形式でエクスポートできます。

### Intel AMT イベント ログを表示するには

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [システム情報] をクリックします。
3. [ログ] を展開して [Intel AMT ログ] をクリックします。
4. ログを CSV 形式のファイルにエクスポートするには、ツールバーにある [**エクスポート**] ボタンをクリックし、ファイルの保存場所を指定します。
5. ログのデータをすべてクリアするには、ツールバーの [ログの消去] ボタンをクリックします。
6. ログ項目を更新するには、ツールバーの [ログの更新] ボタンをクリックします。

## Intel AMT 電源オプション

System Manager には、Intel AMT デバイスの電源をオン/オフできるオプションがあります。これらのオプションは、デバイスのオペレーティング システムが応答しない場合でも、デバイスがネットワークに接続されており、電源がスタンドバイ状態になっている限り使用できます。

System Manager が電源オプション コマンドを実行する際、場合によっては、コマンドを受けるハードウェアでそのコマンドがサポートされているか確認できないことがあります。Intel AMT のあるデバイスは、すべての電源オプションの機能をサポートしていない可能性があります (たとえば、あるデバイスは CD からの IDE-R

再起動はサポートしますが、フロッピーからの起動はサポートしないなど)。デバイスで電源オプションが機能していない場合には、ハードウェア
ベンダのマニュアルを参照してください。また、想定されるように電源オプションが機能しない場合には、Intel からそのデバイス用のファームウェアまたは BIOS の更新が出ていないか確認してください。

デバイスの電源のオン/オフを単に切り替えるか、再起動してデバイスの再起動方法を指定することが可能です。これらのオプションについては以下の表で説明します。

| | |
|---|---|
| 電源オフ | デバイスの電源をシャットダウンします。 |
| 電源オン | デバイスの電源をオンにします。 |
| 再起動 | デバイスの電源をいったんオフにしてからオンにします。 |
| 通常の起動 | デバイスで既定に設定されている起動シーケンスを使って起動します。 |
| ローカル ハード<br>ドライブから起動 | デバイスの既定起動モードに関わらず、デバイスのハードドライブから強制的に起動します。 |
| ローカル CD/DVD<br>ドライブから起動 | デバイスの既定起動モードに関わらず、デバイスの CD<br>または DVD ドライブから強制的に起動します。 |
| PXE 起動 | 再起動時に PXE<br>が有効になっているデバイスはネットワーク上の PXE<br>サーバを探し、見つかった場合にはそのデバイスで PXE<br>起動セッションが開始されます。 |
| IDE-R 起動 | 選択した IDE リダイレクション<br>オプションを使ってデバイスを再起動します (下記を参照)。 |
| BIOS セットアップの起動 | デバイスの起動時に、ユーザが BIOS<br>のセットアップ画面に入れます。 |
| コンソール リダイレクション<br>ウィンドウを表示する | デバイスの起動時に、Serial over LAN<br>モードで起動してコンソール リダイレクション<br>ウィンドウを表示します。 |

| | |
|---|---|
| IDE リダイレクション :フロッピー ディスクから再起動 | デバイスの起動時に、フロッピー ディスク ドライブまたは指定したフロッピー ディスク イメージから起動します (フロッピー ディスク イメージは .img 形式である必要があります。下記の注意を参照)。 |
| IDE リダイレクション :CD/DVD から再起動 | デバイスの起動時に、CD ドライブまたは指定した CD イメージから起動します (CD イメージは .iso 形式である必要があります。下記の注意を参照)。 |
| IDE リダイレクション :指定したイメージ ファイルから再起動 | デバイスの起動時に、指定したイメージ ファイルから起動します (下記の注意を参照)。 |

**Intel AMT 電源オプションを使用するには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [電源オプション] をクリックします。
3. 電源コマンドを 1 つ選択します。[**再起動**] を選択した場合は、起動オプションを選択します。
4. [**送信**] をクリックしてコマンドを開始します。

## IDE リダイレクション オプションの使用に関する注意点

IDE リダイレクション オプションを使用するには、起動フロッピー ディスクまたはフロッピー イメージ ファイル、および起動 CD/DVD または CD/DVD イメージ ファイルの両方を指定する必要があります。フロッピー イメージ ファイルは .img 形式で、CD イメージ ファイルは .iso 形式でなければなりません。.一部の BIOS は CD イメージをハード ドライブ上に保存する必要があります。

Intel AMT は通常前回の IDE-R 設定を記憶しますが、System Manager が 45 秒後に設定をクリアするので、次回の起動では IDE-R 機能を再起動させることはありません。.Intel AMT デバイス上の IDE-R セッションは、6 時間または System Manager コンソールがオフになるまで続きます。6 時間経過後も IDE-R の操作がまだ実行されている場合、その操作は強制終了されます。

## Intel AMT コンピュータでの脆弱性スキャンの強制実行およびネットワーク アクセスの無効化

Intel AMT が構成されているデバイスに LANDesk エージェントがインストールされると、悪意あるソフトウェアやデバイスへのアクセスを妨げるような他の問題の解決に役立つ機能が追加されます。

amtmon.exe サービスが LANDesk
エージェントとともにインストールされます。.デバイスでこのサービスが実行されると、次回再起動時に脆弱性スキャンを強制的に実行して、デバイスに悪意のあるソフトウェアがあるか発見しようとします。デバイスとの通信に失敗した場合、悪意のあるソフトウェアがすべての CPU
サイクルを使用しているためにオペレーティング
システムが無効になっているときなど、オペレーティング
システムが機能していなくても、デバイスのネットワーク接続を無効にすることができます。ネットワーク接続を無効にすれば、そのデバイスから望まないパケットがネットワークに拡散するのを防ぐことができます。

Intel AMT デバイスに LANDesk エージェントをインストールすると、[Intel AMT オプション]
ページで次のオプションが使用できるようになります。

- **オペレーティング システム ネットワーク 接続**:[無効] をクリックすると、OS のネットワーク
  スタックが無効になってネットワークへのアクセスが中断します。[有効]
  をクリックすると、無効になっていた OS のネットワーク アクセスが有効になります。
- **再起動後に脆弱性スキャンを実行します**
  :脆弱性スキャナをデバイスの次回起動時に実行します。

デバイスが応答しない場合や悪意のあるソフトウェアが実行している恐れがある場合、推奨する使用方法は、まず、次回再起動時に脆弱性スキャンを実行して、問題の特定を試みることです。問題が解決せずコンピュータがネットワークを感染/攻撃している場合、またはデバイスにアクセスできない場合は、OS NIC を無効にすることもできます。

**再起動後に脆弱性スキャンを強制実行するには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. デバイス コンソール ウィンドウで、[Intel AMT オプション] をクリックします。
3. [構成オプション] をクリックし、[スキャン]
   をクリックします。次回再起動時にスキャンを実行するというメッセージがデバイスに表示されます。
4. デバイスをシャットダウンまたは再起動するには、前述の Intel AMT リモート ブート
   マネージャの機能を使用します。

**応答しないデバイスのネットワーク接続を無効または有効にするには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. デバイス コンソール ウィンドウで、[Intel AMT オプション] をクリックします。
3. デバイスのネットワーク
   カードを無効にして、ネットワーク上の他のデバイスとの通信を停止するには、[無効]
   をクリックします。ネットワーク接続が無効になると、デバイスにネットワーク
   カードが無効になったというメッセージが表示されます。
4. デバイスが安全にネットワークに接続できるようになったら、[有効]
   をクリックします。接続が回復すると、デバイスにネットワーク
   カードが再度有効になったというメッセージが表示されます。

# Intel AMT 構成画面を開く

System Manager には、Intel AMT
構成画面を開くリンクがあります。この画面は、デバイスのステータス、ハードウェア情報、Intel AMT
イベント ログ、リモート ブートの設定、およびネットワーク設定を表示するために Intel
から提供されているインターフェイスです。また、そのデバイスの Intel AMT ユーザ
アカウントの追加と編集も行えます。この画面を表示するウィンドウは System Manager
コンソールから独立しており、このインターフェイスの使用方法に関する質問は、デバイスの製造元のテクニカル サポートに問い合わせる必要があります。

**Intel AMT 構成画面を開くには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. デバイス コンソール ウィンドウで、[Intel AMT オプション] をクリックします。
3. [Intel AMT コンソール] をクリックして、[Intel AMT Web コンソールを起動する] をクリックします。

# 役割ベース管理

## 役割ベース管理について

役割ベース管理を使用して、システムの管理役割に基づいて本製品のツールやその他のデバイスへのユーザ
アクセスを設定します。役割ベースの管理によって、表示や管理できるデバイスの範囲および実行できるタスクを割り当てます。

管理者（管理者権限を持つユーザ）は、左側のナビゲーション ペインにある
**[ユーザ]**をクリックすると、役割ベース管理ツールにアクセスできます。

役割ベース管理を使用すると、製品ユーザに、ユーザの権限およびスコープに基づく特別な管理役割を割り当てることができます。「*権限*」は、ユーザが表示して使用できる製品ツールと機能を決定します。「*スコープ*」は、ユーザが表示して管理できるデバイスの範囲を決定します。

各ユーザの責任、実行を許可する管理タスク、および表示、アクセスや管理を許可するデバイスに基づいて役割を作成します。デバイスへのアクセスを、国、地域、州、市、または 1
つのオフィスや部門のような場所に制限できます。あるいは、特定のプラットフォーム、プロセッサ
タイプ、他のデバイス
ハードウェアまたはソフトウェア属性に制限することもできます。役割ベース管理を使用すると、作成する役割の数、ユーザに対する役割の割り当て、およびデバイス
アクセスのスコープを自由に設定できます。

### 管理ロールの例

次のテーブルは、実装が可能な管理役割、ユーザが実行する共通タスク、ユーザがその役割を効率よく果たすために必要な権限の一覧を示します。

| 役割 | タスク | 必要な権限 |
|---|---|---|
| 管理者 | コア<br>サーバの設定、ユーザの管理、アラートの設定、他社製品の統合など<br>（当然ながら、すべての権限を持つ管理者は、すべての管理タスクを実行できる） | 管理者<br>（すべての権限があると想定） |
| 資産マネージャ | デバイスの検索、デバイスの設定、インベントリ<br>スキャナの実行、インベントリ履歴追跡の有効化など | デバイス検出、ソフトウェア配布、公開クエリ管理 |
| レポート マネージャ | あらかじめ定義されたレポートの実行、レポートの印刷 | レポート |

| 役割 | タスク | 必要な権限 |
|---|---|---|
| | など | (すべてのレポートに必要) |

これらは役割のほんの一部の例です。役割ベース管理は柔軟性があり、カスタム役割を必要なだけ作成できます。異なるユーザに同じ権限を割り当てることができる場合がありますが、狭いスコープにデバイスを限定したセットにアクセスを制限できます。管理者でも、特に特定の地区または管理デバイスを対象にする管理者の場合は、スコープによって制限できます。役割ベース管理をどのように活用するかは、ネットワークとスタッフのリソースだけでなく、特別なニーズによって異なります。

役割ベース管理を実装して施行するには、現在のローカル Windows ユーザを製品のユーザに指定するか、新しいローカル Windows ユーザを作成して製品のユーザとして追加し、このユーザを Management Suite ユーザ グループに追加して必要な権限 (製品機能に対する) とスコープ (管理デバイスに対する) を割り当てるだけです。次の手順に従ってください。

## 権限について

権限を使用すると、特定のツールおよび機能にアクセスできます。対応するタスクを実行するには、ユーザは必要な権限を持つ必要があります。たとえば、スコープ内でデバイスをリモート コントロールするには、ユーザはリモート コントロール権限が必要です。複数の LANDesk 管理製品がインストールされている場合、権限はどのコンソールからでもユーザに割り当てることができ、すべてのコンソールで有効です。

ユーザに権限が割り当てられていない場合、その権限に関連したツールはコンソール上でそのユーザに表示されません。たとえば、ユーザにレポート権限が割り当てられていなければ、左側のナビゲーション ペインにはレポート項目が表示されません。下の表は、ユーザがそれぞれのツールを表示するために必要になる権限を表わしています。

| ツール | 左側のナビゲーション ペインに表示されるために必要な権限 |
|---|---|
| マイ デバイス | 基本 Web コンソール |
| エージェント構成 | 管理者 |
| アラート | アラートと監視 |
| デバイス検索 | デバイス検索 |
| 監視 | アラートと監視 |
| クエリ | 基本 Web コンソール、公開クエリ管理、レポート |

| ツール | 左側のナビゲーション ペインに表示されるために必要な権限 |
|---|---|
| レポート | レポート、パッチ管理 |
| スケジュールされているタスク | デバイス検索 |
| スクリプト | パッチ管理 |
| ユーザ | 管理者 |
| ソフトウェア更新 | パッチ管理 |
| プリファレンス | 基本 Web コンソール |
| ハードウェア構成 | 管理者 |

権限および権限を使用した管理役割の作成方法の詳細については、次の説明を参照してください。

**スコープがデバイスへのアクセスを制御する**
これらの権限によって許可される機能を使用する際に、ユーザは常にスコープ
(表示して操作できるデバイス) により制限されます。

## 管理者

管理者権限は、すべての ツールにアクセスできます
(ただし、これらのツールの使用についても管理者のスコープ内のデバイスに限定されます)。

これは、既定のテンプレート
ユーザの設定を変更しない限り、追加された新規ユーザの既定の権限です。

管理者権限を使用すると、ユーザは次の操作を行うことができます。

- 左側のナビゲーション ペインでの **[ユーザ]** ツールの表示とアクセス
- 左側のナビゲーション ペインの **[プリファレンス]**での製品のライセンスの表示
- 以下の権限により許可されるすべてのタスクの実行

**管理者ユーザを削除することは推奨しません。**特定の LDSM
コンソールにログインした最後の管理者であるとき、Windows の [コンピュータ管理] で Management Suite
グループから管理者ユーザを削除すると、コンソールに再びログインしようとする際に問題が生じることがあります。削除後 20
分以内は管理者としてログインできますが、アクションを実行したり、管理者としてログインしているコンソ

ール ブラウザの表示を更新 (F5 キー)
すると、それ以降は管理者のみに属している権限にアクセスできなくなります。いかなる状況においても、最後の管理者ユーザは削除しないことをお勧めします。

---

**権限とツールに関する注意**
管理者権限は、**ユーザ** ツール
とのみ関連付けられます。ユーザが管理者権限を持たない場合は、このツールはコンソールに表示されません。

コンソールのすべてのツールは、対応する権限と関連付けられます (下記を参照)。

---

## デバイス検索

デバイス検索権限を使用すると、ユーザは次の操作を行うことができます。

- ネットワーク スキャン、標準の管理エージェント検索、IPMI 検索など、多くの方法で、コア データベースにインベントリ スキャンを送信していないデバイスをネットワーク上で検索します。
- 定期検索のスケジュール
- 検索から管理へのデバイスへの移動

## 公開クエリ管理

公開クエリ管理権限を使用すると、ユーザは次の操作を行うことができます。

- すべてのユーザに使用可能なクエリの作成
- 公開クエリを作成または削除する機能
- 既存の公開クエリを変更または編集する機能

## レポート

レポート権限を使用すると、ユーザは次の操作を行うことができます。

- 左側のナビゲーション ペインでの **[レポート]**ツールの表示とアクセス
- あらかじめ定義したレポートの実行

## パッチ管理

パッチ管理権限は、脆弱性スキャン機能に固有です。詳細については、「ソフトウェア更新ツールの使用」を参照してください。

### 基本 Web コンソール

基本 Web
コンソール権限を使用すると、ユーザはこの権限に関連付けられている機能を使用できます。次に、使用可能な機能と、その機能に含まれる例外を説明します。

- **マイ デバイス** (この権限では、公開グループを更新したり **[アクション]** タブのデバイスを削除したりすることはできません)
- プリファレンスの変更 (カスタム属性は変更できません)

### アラートと監視

アラートと監視権限を使用すると、ユーザは次の操作を行うことができます。

- ドライブ、プロセッサ、メモリ、プロセス、システムの Web サーバによって転送されるバイト/秒など、さまざまなシステムおよび OS コンポーネントのパフォーマンスの監視
- すべての管理デバイスのヘルスのトラック
- 重要度レベル ([危険]、[警告]、[情報]、[OK]、[不明]) またはしきい値 (ハード ディスク使用率がハード ディスク容量の 90% を超えた場合、など) を基準にして送信されるアラートのカスタマイズ
- アラートがしきい値を超えた場合に実行されるアクションの選択 (ログに情報を追加、通知を電子メール送信、コアまたは個々のデバイス上でプログラムを実行、SNMP トラップをネットワークの SNMP 管理コンソールに送信)

## 製品ユーザの追加

製品ユーザとは、製品のコンソールにログインし、ネットワークで特定のデバイスを対象に特定のタスクを実行することができるユーザです。

製品ユーザは実際にコンソールに作成されるわけではありません。代わりに、ユーザがコア サーバの Windows ユーザ環境で LANDesk Management Suite グループに追加されると、そのユーザは **[ユーザ]**タブ (左側のナビゲーション ペインで、**[ユーザー]**をクリック) に表示されます。**[ユーザ]** グループには、コア サーバの LANDesk Management Suite グループに現在いるすべてのユーザが表示されます。

**[ユーザ]** グループには次の 2 つの既定ユーザがいます。

- **既定のテンプレート ユーザ** :このユーザは基本的にユーザ プロパティ (権限およびスコープ) のテンプレートで、LANDesk Management Suite グループに追加された新規ユーザを設定するときに使用します。つまり、Windows 環境で該当するグループにユーザを追加すると、ユーザは [既定のテンプレート ユーザ] プロパティに現在定義されている権限とスコープを継承します。既定のテンプレート ユーザにすべての権限と既定の [すべてのコンピュータ] スコープが選択されていると、LANDesk Management Suite グループに配属される新規ユーザは **[ユーザ]** グループに追加され、製品ツールおよびデバイスすべてにアクセスする権限があります。

  既定のテンプレート ユーザのプロパティ設定を変更するには、[既定のテンプレート ユーザ] を右クリックし **[権利の編集]**をクリックします。たとえば、一度に多数のユーザを追加するが、ツールまたはデバイスのすべてではアクセスを認めない場合は、最初に既定のテンプレート ユーザの設定を変更し、LANDesk Management Suite グループにユーザを追加します (以下の手順を参照)。

  既定のテンプレート ユーザは削除できません。

- **既定管理者**
  :既定管理者は、本製品のコアのインストール時にサーバにログインした管理者ユーザです。

Windows で LANDesk Management Suite グループにユーザを追加すると、ユーザは、**[ユーザ]** ウィンドウで **[すべてのユーザ]** グループに自動的に読み込まれ、現在の既定のテンプレート ユーザと同じ権限とスコープを継承します。ユーザの名前、スコープ、および権限が表示されます。

Windows ユーザ環境の LANDesk Management Suite グループからユーザを削除すると、ユーザはアクティブではなくなり、**[ユーザ]** グループから削除できます。ユーザのアカウントはまだサーバに存在し、いつでも LANDesk Management Suite グループに再追加できます。また、**[ユーザ デバイス]**、**[ユーザ クエリ]**、**[ユーザ レポート]**、および **[ユーザ スクリプト]** の各グループのユーザ サブグループは保持されるので、データを失わずにユーザを復元したり、他のユーザにデータをコピーしたりできます。

**[ユーザ]** リストを更新して新しく追加したユーザを表示するには、ブラウザで **[ユーザ]** をクリックして **[更新]** ボタンをクリックします。

**ユーザまたはドメインを LANDesk Management Suite グループに追加するには**

1. サーバの **[管理ツール]**、**[コンピュータの管理]**、**[ローカル ユーザーとグループ]**、**[グループ]**ユーティリティの順にクリックします。
2. **[LANDesk Management Suite]** グループを右クリックし、**[グループに追加]**をクリックします。
3. **[追加]**をクリックして、ユーザを入力するかリストから選択します (複数選択可)。
4. **[追加]**をクリックし、**[OK]**をクリックします。

---

**注意** :[ユーザ] リストのユーザ アカウントを右クリックし、**[プロパティ]**、**[所属するグループ]**、**[追加]** の順にクリックして LANDesk Management Suite グループにユーザを追加することもできます。

---

ユーザ アカウントがもう Windows に存在しない場合は、最初にサーバに作成する必要があります。

**新しいユーザ アカウントを作成するには**

1. サーバの **[管理ツール]**、**[コンピュータの管理]**、**[ローカル ユーザーとグループ]**、**[ユーザ]** ユーティリティの順にクリックします。
2. **[ユーザ]** を右クリックして、**[新しいユーザ]**をクリックします。
3. [新しいユーザ] ダイアログで、名前とパスワードを入力します。
4. パスワード設定を指定します。
5. **[作成]**をクリックします。[新しいユーザ] ダイアログは開いたままなので、追加のユーザを作成できます。
6. **[閉じる]**をクリックしてダイアログを終了します。
7. LANDesk Management Suite グループにユーザを追加すると、コンソールの [ユーザ] グループに表示されます。

製品ユーザの権限とスコープを割り当てることができます。

# スコープの作成

スコープは、製品ユーザが表示および管理できるデバイスを定義します。複数の LANDesk 管理製品がインストールされている場合、スコープはどのコンソールからでもユーザに割り当てることができ、すべてのコンソールで有効です。

コアデータベースにスキャンされた管理対象デバイスの全部または 1 つのみを含めるか、1 つも含めないことによりスコープを大きくすることも小さくすることも可能です。この柔軟性は、モジュール化されたツール アクセスと組み合わせることにより、役割ベース管理を多用途に対応する管理機能に高めます。

## 既定スコープ

役割ベース管理には次の 2 つの既定スコープがあります。これらの 2 つのあらかじめ定義されたスコープは、既定のテンプレート ユーザのユーザ プロパティを設定する際に役立ちます。

- **(既定の) [コンピュータなし] スコープ** :
  データベースに格納されているデバイスのすべてを除外します。
- **(既定の) [すべてのコンピュータ] スコープ** :
  データベースに格納されているデバイスのすべてを含めます。

既定のスコープは、編集も削除もできません。

## カスタム スコープ

以下のタイプのカスタム スコープを作成し、ユーザに割り当てることができます。

- **クエリベース** : カスタム
  クエリ検索に一致するデバイスだけにアクセスを制御します。既存のクエリを選択するか、[**クエリ**]
  ダイアログで新しいクエリを作成して、スコープを定義できます。クエリの作成方法の詳細については、「データベース クエリの作成」を参照してください。
- **グループベース**: 選択したグループ内のデバイスだけにアクセスを制御します。[**グループ スコープ プロパティ**] ダイアログでグループを選択して、スコープを定義します。

ユーザには、複数のスコープを割り当てることができます。ユーザに複数のスコープを割り当てる場合、累積的な有効スコープ
(スコープの割り当てを組み合わされることによって、デバイス範囲全体がアクセスおよび管理可能になる) はシンプルなコンポジットです。

ユーザの有効スコープは、スコープを随時追加および削除することでカスタマイズできます。すべてのスコープ タイプは、同時に使用できます。

**スコープを作成するには**

1. 左側のナビゲーション ペインで、[**ユーザ**] をクリックします。
2. [**スコープ**] タブで [**新規クエリ スコープ**]または [**新規グループ スコープ**] ツール バー ボタンをクリックします。
3. 新しいスコープの名前を入力します。
4. クエリベースを選択した場合、既存のクエリを選択するか、[**定義**] をクリックして新しいクエリを作成します。[OK] をクリックします。
5. グループベースを選択した場合、グループを選択して [OK] をクリックします。
6. [OK] をクリックしてスコープを保存し、ダイアログを閉じます。

# ユーザへの権限とスコープの割り当て

- [ユーザ権利/スコープ] ダイアログについて
- [リモート コントロール設定] ダイアログについて

製品ユーザを追加し、権限およびそれによる機能とツールへのアクセス制御を確認したら、デバイス スコープを作成して、管理デバイスへのアクセスを許可または制限します。役割ベース管理を確立する際には次のステップで、各ユーザに適切な権限とスコープを割り当てます。

ユーザの権限とスコープは、いつでも変更できます。

ユーザの権限またはスコープを変更すると、変更内容は、ユーザが次回にコンソールにログインしたときに有効になります。

**ユーザに権限とスコープを割り当てるには**

1. 左側のナビゲーション ペインで、[**ユーザ**] をクリックします。

2. ユーザのリストを展開すると、コア サーバの Windows NT 環境で現在 LANDesk Management Suite グループのメンバであるすべてのユーザが表示されます。

   このリストには、ユーザ名および割り当てられた権限が表示されます
   (チェック記号は権限が有効またはアクティブであることを示します)。

3. ユーザを右クリックして、[**編集**] をクリックします。
4. [**ユーザ権利/スコープ**]
   ダイアログで、必要に応じて権限チェックボックスをオンまたはオフにします。
5. [**スコープ**] タブをクリックしして [**割り当てるスコープ**] リストからスコープを選択します。
6. [**適用**] をクリックします。

リストのユーザ名の隣に新しい権限が表示され、ユーザが次回コア
サーバに接続したときに有効になります。

**スコープを削除するには**

1. 左側のナビゲーション ペインで、[**ユーザ**] をクリックします。
2. [**スコープ**] タブで、削除するスコープをクリックして [ **削除**] をクリックします。[**OK**]
   をクリックします。

スコープを削除するときは注意が必要です。削除対象のスコープが割り当てられているユーザは、そのスコープによって以前禁止されていた権限にアクセスできるようになるからです。

## [ユーザ権利/スコープ] ダイアログについて

このダイアログでは、ユーザに割り当てられた権限とスコープを表示および変更します。ユーザを選択して [**編集**] をクリックすると、ダイアログが表示されます。

**[権利] タブ** : ユーザに割り当てられた権限を一覧表示します。

- **管理者**
- **デバイス検索**
- **公開クエリ管理**
- **レポート**
- **パッチ管理**
- **基本 Web コンソール**
- **アラートと監視**

**[スコープ] タブ** : ユーザに割り当てられたスコープを一覧表示します。

- **割り当てるスコープ** : ユーザの現在のスコープを示します。
- **追加** : [**スコープの追加**] ダイアログが表示され、ユーザに追加するスコープを選択できます。
- **削除**:選択したクエリを削除します。
- **キャンセル** : 変更内容を保存せずにダイアログを閉じます。

# デバイス検索

## デバイス検索の使用方法

デバイス検索は、検索を行っているコアのエージェントをインストールしておらず、同じコア
データベースにインベントリ
スキャンを送信していないデバイスをネットワーク上で検索します。デバイス検索は、複数の方法でネットワーク上のデバイスを検索します。

- **ネットワーク スキャン** : ICMP Ping
  スイープを実行してコンピュータを検索します。これは最も詳細な検索ですが、より時間がかかります (IP FingerPrint が使用されている場合)。特定の IP
  およびサブネット範囲に検索を限定できます。既定では、このオプションには NetBIOS
  が使用され、デバイスに関する情報が収集されます。IP Fingerprinting
  を選択することもでき、ほとんどの場合 OS タイプも提供されます。ネットワーク スキャン
  オプションには、一部のプリンタのような SNMP デバイスに対して SNMP
  を使ってスキャンするように設定可能な **[SNMP を使用する]**オプションもあります。
- **CBA 検索** :標準の管理エージェント (以前の Management Suite の Common Base Agent (CBA))
  をコンピュータで検索します。このオプションでは、Server Manager、System Manager
  などがインストールされているコンピュータが検索されます。PDS2 オプションを選択して、古い
  LANDesk PDS2 エージェントを使用するデバイスを検索できます。CBA 検出は Linux
  コンピュータではサポートされていませんが、PDS2
  を選択すれば、エージェントをインストール済みの Linux コンピュータは検出が可能になります。
- **IPMI** :サーバの電源のオン/オフまたは OS の動作状態に関係なく、Baseboard Management
  Controller (BMC) にアクセスできるようにする Intelligent Platform Management Interface
  が利用可能なサーバを検索します。
- **サーバ シャーシ** : ブレード サーバ シャーシ管理モジュール (CMM) を検索します。サーバ
  シャーシのブレードは、標準のサーバとして検索されます。
- **Intel* AMT** :サーバの電源のオン/オフまたは OS
  の動作状態に関係なく、制限された管理機能にアクセスできるようにする Intel Active
  Management Technology (バージョン 1) 対応デバイスを検索します。

デバイス検索は、各デバイスの基本情報を検索します。以下の情報のすべてがすべてのデバイスで使用できるとはかぎりません。

- **ノード名** :検出されたデバイス名 (取得可能な場合)。
- **IP アドレス** :検出された IP アドレス。
- **サブネット マスク** :検出されたサブネット マスク。
- **カテゴリ** :デバイスが属するデバイス検索グループ。
- **OS 名** :検出されたオペレーティング システムの説明 (取得可能な場合)。

デバイスがデバイス検索で最初に検出されたら、デバイス検索はコア
データベースを参照して、そのデバイスの IP アドレスと名前が **[マイ デバイス]**

リスト内のデータベースに既に存在しているかどうかを確認します。**[非管理]**リスト内のデバイスは、再検索されてより多くのデータをもたらす可能性があります。一致する情報がある場合、デバイス検索はそのデバイスを無視します。一致する情報がない場合、デバイス検索はデバイスを**非管理デバイス**テーブルに追加します。**非管理テーブル**に含まれるデバイスは、System Manager ライセンスを使用しません。コア データベースにインベントリ スキャンを送信したデバイスは管理デバイスと見なされます。デバイスを **[すべてのデバイス]**グループに移動すると、**[検出されたデバイス]** リストでは表示されなくなります。

IPMI デバイスには、IPMI として検出されて IPMI の全機能が利用できるように設定されている BMC (Baseboard Management Controller) が必要です。BMC が設定されていないと、デバイスは通常のコンピュータとして検出されます。その場合、そのデバイスを管理デバイスのリストに追加して、ハードウェア構成機能を実行して BMC パスワードを設定します。すると、デバイスの IPMI 機能が本製品によって認識されます。BMC の IP アドレスが OS の IP アドレスと同じである必要はないので、BMC の IP アドレスへの直接のエージェント プッシュができないことがあります。標準のエージェントを BMC の IP にプッシュするには、標準の IP の再検索が必要な場合があります。BMC IP は、IP エージェントのプッシュを受け入れられます。

Intel* AMT (バージョン 1) が有効なデバイスを Intel AMT デバイスとして認識し検出するためには、Intel AMT ユーザ名およびパスワードを使って設定されている必要があります。検出後、ハードウェア構成機能を実行して Intel AMT 設定を設定し、デバイスを Small business モードまたはセキュアな Enterprise モードにプロビジョニングすることができます。

デバイス検索を自動化するために、検索が定期的に実行されるようにスケジュールできます。たとえば、ネットワークをサブネットで 3 分割し、毎晩、異なるサブネットに対して Ping スイープを実行するようにスケジュールします。すべての検索はコア サーバによって実行されます。

ネットワーク上でデバイスを検索し、管理するには、次の手順を実行します。

- 検索構成の作成
- 検索のスケジュールと実行
- 検出されたデバイスの表示
- **[マイ デバイス]**リストへの検出されたデバイスの移動

## ファイアウォールで保護されているデバイスでの非管理デバイスの検索の使用方法

通常、非管理デバイスの検索では、Windows Firewall などのファイアウォールを使用しているデバイスは、手動でファイアウォールを設定しない限り、検出できないことに注意してください。次のポートを開く必要があります。これらの設定を変更するには、Windows の [コントロール パネル] から [Windows ファイアウォール] にアクセスします。

**管理サーバ** :

- ファイルおよびプリンタの共有 :TCP 139, 445; UDP 137,138
  (この設定をしないとプッシュが機能しません)

- ソフトウェア配布 :TCP 9595 (この設定をしないとプッシュが機能しません)
- 詳細 – ICMP :[エコー要求の着信を許可する] (この設定が有効でないと検出されません)

**コア サーバ :**

- インベントリ : 5007
- リモート コントロール : 9535

# 検索構成の作成

**[検索構成]**タブでは、検索構成の新規作成、既存の構成の編集または削除、および検索構成のスケジュールを行うことができます。各検索構成は、わかりやすい名前、スキャン対象となる IP 範囲、検索タイプで構成されます。

構成を作成したら、**[検索のスケジュール]** ダイアログで検索の実行時期を設定します。

1. 左側のナビゲーション ペインで、**[デバイス検索]**をクリックします。
2. **[検索構成]**タブで、**[新規]**ボタンをクリックします。
3. 以下に説明するフィールドに必要な情報を入力します。各フィールドへの入力が完了したら、**[追加]**ボタンをクリックして **[OK]**をクリックします。

以下に、**[検索構成]**ダイアログ ボックスの各構成要素を説明します。

- **構成名**
  :この構成の名前を入力します。構成名にはわかりやすい名前を指定して、構成内容をすぐに認識できるようにしてください。構成は 255 文字以下とし、次の文字は使用しないでください。**"**、**+**、**#**、**&** または **%**。これらの文字を 1 つでも使うと、構成名は表示されません。
- **標準ネットワーク スキャン** :指定した範囲の IP アドレスに ICMP パケットを送信してデバイスを検索します。これは最も詳細な検索ですが、最も時間がかかります。既定では、このオプションには NetBIOS が使用され、デバイスに関する情報が収集されます。

  ネットワーク スキャン オプションには、デバイス検索が TCP パケット応答を通して OS タイプを検索する **IP fingerprint** オプションが用意されています。IP FingerPrint オプションを使用すると、検索処理が多少遅くなります。

  ネットワーク スキャン オプションには、SNMP を使ってスキャンするように設定可能な **[SNMP を使用する]**オプションもあります。**[構成]**ボタンをクリックして、SNMP 構成の情報を入力します。詳細については、「SNMP スキャンの構成」を参照してください。

- **LANDesk CBA 検索** :標準の管理エージェント (以前の Management Suite の Common Base Agent (CBA)) をデバイスで検索します。標準の管理エージェントにより、コア サーバがネットワーク上のクライアントを検索して、通信することができます。このオプションは、製品のエージェントをインストールしているデバイスを検索します。ルータは標準の管理エージェントと PDS2 トラフィックをブロックします。複数のサブネット間で標準 CBA 検索を実行するには、複数のサブネット間で指定のブロードキャストを許可するようにルータを設定する必要があります。

  CBA 検索オプションでは、デバイス検索がデバイス上の LANDesk Ping Discovery Service (PDS2) を検索する**[LANDesk PDS2 検索]**オプションも使用できます。LANDeskLANDeskÂ® System Manager、Server Manager、およびLANDesk Client Manager などのソフトウェア製品は、PDS2 エージェントを使用します。ネットワーク上のデバイスにこれらの製品がインストールされている場合は、このオプションを選択してください。CBA 検出は Linux コンピュータではサポートされていませんが、PDS2 を選択すれば、エージェントをインストール済みの Linux コンピュータは検出が可能になります。
- **IPMI** :IPMI 対応サーバを検索します。IPMI は、管理可能なハードウェアにアクセスするためのメッセージとシステム インターフェイスを定義するために、Intel、* H-P、* NEC、* および Dell * が開発、規格化した仕様です。IPMI には、監視と復旧機能が含まれており、デバイスの電源のオン/オフまたは OS の動作状態に関係なく、多くの機能にアクセスできます。BMC が構成済みでない場合、BMC は IPMI 検出のために本製品が使用する ASF ping に応答しないことに注意してください。つまり、通常のコンピュータとして検出されることになります。クライアントをプッシュするときに、ServerConfig がシステムをスキャンして IPMI を検出し、BMC を構成します。IPMI の概要については、「IPMI サポート」を参照してください。
- **サーバ シャーシ** : ブレード サーバ シャーシ管理モジュール (CMM) を検索します。サーバ シャーシのブレードは、標準のサーバとして検索されます。
- **Intel* AMT** : Intel Active Management Technology をサポートするデバイスを検索します。
- **開始 IP** :スキャンするアドレス範囲の開始 IP アドレスを入力します。
- **終了 IP** :スキャンするアドレス範囲の終了 IP アドレスを入力します。
- **サブネット マスク** :スキャンする IP アドレス範囲のサブネット マスクを入力します。
- **追加** :ダイアログの下部の作業キューに IP アドレスの範囲を追加します。
- **クリア** : IP アドレス範囲のフィールドをクリアします。
- **編集** : 作業キューで IP アドレスの範囲を選択し、**[編集]**をクリックします。IP アドレスの範囲が作業キューの上にあるテキスト ボックスに表示され、範囲を編集したり、作業キューに新しい範囲を追加したりすることができます。
- **削除**:作業キューに対して選択した IP アドレスの範囲を削除します。
- **すべて削除** :作業キューからすべての IP アドレス範囲を削除します。

**構成を編集または削除するには**

- **[検索構成]**タブで、編集または削除する構成をクリックし、**[編集]**または [削除] をクリックします。

## SNMP スキャンの構成

ネットワーク スキャンの検出で SNMP を使用できます。使用ネットワークの SNMP
構成にしたがって、検索構成で追加の SNMP
情報を入力する必要があります。**[SNMP]**オプションの横にある **[構成]** をクリックすると、3
つのオプションがある **[SNMP 構成]**ダイアログが表示されます。

- **再試行** :デバイス検索が SNMP 接続を試行する回数。
- **応答を待機する時間 (秒)** : デバイス検索が SNMP の応答を待機する時間。
- **ポート** : デバイス検索が SNMP クエリを送信するポート。
- **コミュニティ名** : デバイス検索が使用する SNMP コミュニティ名。
- **SNMP V3 を構成する** : デバイス検索は SNMP V3
  もサポートしています。このボタンをクリックすると、**[SNMP V3 構成]**ダイアログで SNMP V3
  オプションを構成できます。

**[SNMP V3 構成]**ダイアログには次のオプションがあります。

- **ユーザ名** :デバイス検索がリモート SNMP サービスと認証に使うユーザ名。
- **パスワード** :リモート SNMP サービス用のパスワード。
- **認証タイプ** :SNMP が使用している認証タイプ。**[MD5]**、**[SHA]**、または **[なし]**
  の可能性があります。
- プライバシー**タイプ** :SNMP サービスが使用している暗号化メソッド。**[DES]**、**[AES128]**、**[なし]**
  の可能性があります。
- プライバシー **パスワード** : 特定のプライバシー タイプで使うパスワード。**[なし]**をプライバシー
  タイプに選択している場合は利用できません。

# 検索のスケジュールと実行

**[検索構成]**タブの**[スケジュール]** ボタンをクリックすると、**[スケジュールされているタスク]**
ダイアログが表示されます。このダイアログでは、検索構成の実行時期をスケジュールできます。検索構成は、すぐに実行する、後で実行する、または定期的に繰り返し実行する、または一度だけ実行するようにスケジュールできます。

検索タスクは **[検索タスク]**
タブから再スケジュールまたは削除することができます。検索をスケジュールしたら、**[検索タスク]**タブを表示して、検索ステータスを確認してください。また、**[スケジュールされているタスク]**ツールから検索タスクのステータスにアクセスすることもできます。検索タスクが完了したら、まだコア
データベースにはない新しいデバイスが検出されたデバイス カテゴリに追加されます。

**[スケジュールされているタスク]** ダイアログには、次のオプションがあります。

- **共通タスクに表示する** :
  他のユーザにもタスクを表示します。他のユーザがこのタスクを編集または実行すると、そのユーザがそのタスクのインスタンスの所有者になります。
- **所有者** : タスクの所有者。

- **未スケジュール** :(既定) 後でスケジュールできるように、[タスク] リストのタスクを未スケジュールのままにしておきます。
- **すぐに開始** :できるだけ速やかにタスクを実行します。タスクの開始までに 1 分かかる場合もあります。
- **スケジュールされた時刻に開始** :指定した時間にタスクを開始します。このオプションをクリックする場合は、次の情報を入力してください。
    - **日付** :タスクを開始する日付。ロケールの設定によって、日付順序は「日/月/年」または「月/日/年」になります。
    - **時刻** :タスクを開始する時刻です。
    - **実行周期** :タスクを繰り返す場合は、頻度 (日、週、または月) を選択します。[月] を選択し、すべての月には存在しない日付 (たとえば 31 日) を選択した場合、その日付が存在する月にのみタスクが実行されます。

**検索をスケジュールするには**

1. 左側のナビゲーション ペインで、**[デバイス検索]** をクリックします。
2. **[検索構成]** タブで、検索をスケジュールする構成を選択して、**[スケジュール]** をクリックします。検索スケジュールを設定します。終了したら、**[保存]**をクリックします。
3. **[検索タスク]**タブで検索の進行状況を監視します。
4. 検索が完了したら、上部にある**[デバイス検出]** ペインですべての検索結果を確認します。検索タスクをダブルクリックすると、デバイス数と割合はゼロになります。これらの数値が管理デバイスに結び付けられており、検索タスクにまだターゲットがないためです。

**[検索タスク]**タブには、検索ジョブのステータスが表示されます。ステータスには次の情報が含まれます。

- 検索構成の名前。
- タスク ステータス。[処理中]、[すべて完了]、[完了したものはありません]、[失敗] のいずれかが表示されます。
- 最後にタスクが実行された時刻。
- タスクの実行タイプ。

**検索を削除または再スケジュールするには**

既に実行されたかものであるかどうかに関係なく、タスクをリストから削除する場合は、タスクをクリックして、**[削除]**をクリックします。タスクがまだ実行されていないものであったり、定期的に繰り返されるタスクである場合、それらのジョブを削除すると、それ以降実行されなくなります。

また、タスクをクリックして **[編集]**をクリックしてから**[スケジュール]** を選択し、スケジュールをリセットすることによって、リスト内の検索タスクを再度実行するようにスケジュールしなおしたり、別の時刻に実行するようにスケジュールしなおすことも可能です。すぐにタスクを再実行するには、タスクを選択して**[すぐに開始]** をクリックします。

**検索タスク ステータスを表示するには**

1. 左側のナビゲーション ペインで、**[検出されたデバイス]**をクリックします。
2. そのパネルのツールバーにある**[検索タスク]**タブまたは **[更新]** をクリックします。

# 検出されたデバイスの表示

**[デバイス検索]**
上部ペインに検出されたすべてのデバイスを表示します。このペインには、実行されたすべての検索の結果が表示されます。新しい検索を実行すると、検出されたデバイスはすべてこのリストに追加されます。

デバイス検索でデバイスが検出されると、そのデバイス タイプを識別して次のカテゴリの 1 つに追加します。

- **シャーシ**:ブレード サーバ シャーシ管理モジュール (CMM) が含まれます。
- **コンピュータ** :コンピュータが含まれます。Linux システムは、**[OS 名前]** 列に "Unix system" とラベル付けされます。
- **インフラストラクチャ** :ルータおよびその他のネットワーク ハードウェアが含まれます。
- **Intel AMT** :Intel* Active Management Technology をサポートするデバイスが含まれます。.
- **IPMI**:IPMI 対応デバイスが含まれます。
- **その他** :識別されないデバイスが含まれます。
- **プリンタ** :プリンタが含まれます。

これらのカテゴリを使用して**デバイス検索**を整理しておくと、目的のデバイスが容易に検索できます。見出しをクリックすると、列の見出しでデバイス リストを並べ替えることができます。デバイス検索は、デバイスを毎回正しく分類するわけではありません。誤って識別されたデバイスを正しいグループに含めるには、移動するデバイスを右クリックして **[移動]** をクリックして、適切なカテゴリを選択してから **[OK]** をクリックします。

時にコア サーバがリストに 2 つ表示されることがあります。これは、同じコンピュータが別の検索メカニズム (たとえば CBA、IPMI、CMM、PDS1、および PDS2) によって検出されており、そのコンピュータの情報がそのメカニズムでデータベースに追加されているために発生します。

検出されたデバイスにエージェントを導入して、そのデバイスがコアにインベントリ スキャンを送信すると、検出されたデバイスは、検出されたデバイス リストから削除されます。

## [デバイス] リストのフィルタ

ツール バーの **[フィルタ]**フィールドを使用して、指定した検索条件に一致するデバイスを検索します。フィルタ対象として、ノード名、IP アドレス、サブネット マスク、カテゴリ、または OS

名を指定できます。フィルタを使用すると、フィルタする属性別にデバイスがアルファベット順にソートされます。

**デバイス リストをフィルタするには**

1. 左側のナビゲーション ペインで、**[デバイス検索]**をクリックします。
2. **[非管理]** ツリーで、フィルタするグループをクリックします。
3. **[フィルタ]** で、フィルタする属性をクリックします。(**[フィルタ]** が表示されていない場合は、>>をクリックすると展開されます。)
4. 属性の隣のボックスに、フィルタするテキストを入力します。
5. **[検索]**をクリックします。

## カテゴリの追加

デバイス
カテゴリを作成して、非管理デバイスをグループ化できます。デバイスを別のカテゴリに移動すると、後からデバイス検索によってそのデバイスを検出されたときも、再びそのグループに表示されます。コンソールで管理しないことがわかっているデバイスは他のグループに移動しておくと、**[コンピュータ]** グループ内で新しいデバイスが確認しやすくなります。

デバイスを含むグループを削除した場合、そのデバイスは デバイス検索によって**[その他]** グループに移動されます。

**デバイス カテゴリを追加するには**

1. **[デバイス検索]**ビューで、**[カテゴリの追加]**をクリックします。
2. **[カテゴリ名]**ボックスにグループの名前を入力して、**[OK]** をクリックします。
3. 追加したカテゴリを削除するには、**[カテゴリの削除]**をクリックし、[OK]をクリックして削除を確定します。

# [マイ デバイス] リストへの検出されたデバイスの移動

デバイスは検出した後に **[マイ デバイス]**リストに移動できます。デバイスを移動する過程で、デバイス情報がデータベースに追加されます。情報がデータベースに追加されると、エージェント構成の導入、その情報に対するクエリおよびレポートの実行、およびその他の多くの管理タスクを実行できます。

アウトオブバンドで管理可能なデバイス (IPMI、Intel AMT、または DRAC 機能を持っているデバイス) の場合、エージェントを導入せずにそのデバイスを管理するオプションもあります。こうすると、デバイス情報がデータベースに保存され、デバイスの BMC が設定されるので、デバイスのアウトオブバンド管理ハードウェアで許可される管理機能が使用できるようになります。

**[マイ デバイス] リストへ検出されたデバイスを移動するには**

1. **[デバイス検索]** ビューで、**[マイ デバイス]** リストに移動するデバイスをクリックします。複数のサーバを選択するには、Shift キーを押しながらクリック、または Ctrl キーを押しながらクリックします。
2. **[ターゲット]**ボタンをクリックします。選択したデバイスは、**[ターゲット デバイス]**タブに一覧表示されます。
3. **[管理]**タブをクリックします。
4. **[選択されたデバイスを移動します]**を選択します。
5. デバイスがアウトオブバンドで管理可能であり、管理エージェントを導入しない場合には、**[アウトオブバンド対応デバイスをエージェントレスで管理します]**を選択します。
6. **[移動]**をクリックします。

デバイスは非管理デバイスのリストから削除されて、**[マイ デバイス]**リストに表示されます。

アウトオブバンド管理オプションを選択した場合、下部ペインの **[移動ステータス]**をクリックして移動プロセスのステータスを表示できます。構成のエラーはここに表示されます。IPMI 対応デバイスを **[マイ デバイス]** リストに移動するには、サービス設定ユーティリティに適切な BMC 資格情報を入力して、コア サーバがデバイスを正しく認証するようにする必要があります。

シャーシ管理モジュール (CMM) を **[マイ デバイス]** リストに移動すると、その CMM は**[すべてのデバイス]** リストに表示され、グループとして**[公開グループ]** リストにも表示されます。グループの詳細には、CMM およびシャーシ内の利用可能なベイとそのベイ内のブレード サーバ名のリストが表示されます。ブレード サーバは、個別のサーバとしても検出および管理されます。

# Intel* AMT デバイスの検索

System Manager には、Intel* Active Management Technology (Intel* AMT) バージョン 1 で構成されたデバイスを検出するオプションがあります。デバイスを Intel AMT デバイスとして検出するにはまず、そのデバイスで Intel AMT 構成画面にアクセスし、製造元の既定のパスワードをセキュア パスワードに変更しておく必要があります。(Intel AMT 構成画面へのアクセス方法の詳細については製造元のマニュアルを参照してください。)この手順を行わないと、デバイスは検出されますが Intel AMT デバイスとして認識されず、Intel AMT デバイスとして検出させた場合に表示されるインベントリ サマリ情報を表示できません。

---

Intel AMT バージョン 2 デバイスはこの手順では検出されません。Intel AMT 構成画面にプロビジョニング ID とコア サーバの IP アドレスが入力された後で、デバイスは自動的に検出されます。バージョン 2 の操作に関する詳細は「Intel AMT デバイスの設定」を参照してください。

---

### Intel AMT デバイスを検出するには

1. 左側のナビゲーション ペインで、[デバイス検索] をクリックします。
2. [新規]
   をクリックして新しい構成を作成して、その構成の名前を入力します。あるいは、既存の構成をクリックし、[編集] をクリックして変更します。
3. [Intel AMT デバイスを検出します] を選択します。
4. アドレス範囲をスキャンするための開始 IP アドレスと終了 IP アドレスを入力して、サブネット マスクを入力します。
5. [追加] をクリックして、[OK] をクリックします。
6. 構成をクリックして [スケジュール] をクリックします。スケジュール
   オプションを設定するか、[すぐに開始] をクリックしてから [保存] をクリックします。
7. スキャンの進行状況を表示するには、[検索タスク] タブをクリックします。

Intel AMT で構成されているデバイスは、[Intel AMT]
というラベルのフォルダに表示されます。このフォルダから、デバイスを選択して管理デバイスのリストに移動できます。

デバイスを管理するためにデバイスをコア
データベースに追加するには、デバイスのユーザ名/パスワードがサービス設定ユーティリティに保存されているユーザ名/パスワードに一致している必要があります。これにより System Manager
がデバイスを認証できるようになります。サービスの設定ユーティリティでパスワード構成を保存すると、コア データベースにその情報が保存され、System Manager は Intel AMT
デバイスを認証できるようになります。

異なる資格証明を持った Intel AMT
デバイスがある場合、管理を開始する前に個々のデバイスの資格証明がサービス設定ユーティリティにある資格証明と一致しているか確認する必要があります。

Intel AMT デバイスが検出され、[マイ デバイス]
リストに移動されると、サービスの設定ユーティリティで選択したモードを使ってそのデバイスが自動的に提供されます。Small Business モードはネットワーク インフラクストラクチャ
サービスなしでセキュアではない基本的な管理機能を提供し、Enterprise
モードは大企業向けで、DHCP、DNS、TLS 証明機関サービスなどのネットワーク
サービスをベースとしたセキュリティを提供します。

コア サーバでプロキシ サーバを使用している場合、Intel AMT デバイスを検出するには、そのプロキシ サーバが Digest Access Authentication (Digest 認証) をサポートしている必要があります。

### Intel AMT のパスワードを設定するには

1. [スタート]、[プログラム]、[LANDesk]、[Configure Services] の順にクリックします。[**Intel AMT 構成**] タブをクリックします。

2. 現在のユーザ名とパスワードを入力します。Intel AMT
   デバイスを管理するためには、このユーザ名とパスワードが Intel AMT
   構成画面で設定されているものに一致する必要があります (コンピュータの BIOS
   設定からアクセスできます)。
3. ユーザ名およびパスワードを変更するには、[**New Intel AMT password** (新しい Intel AMT
   パスワード)] セクションを使用します。
4. コア
   データベースにデバイスを追加して管理するとき、デバイスを提供するために使用するモード
   (Small Business または Enterprise) を選択します。
5. [**OK**] をクリックします。この変更は、そのクライアント設定の実行中に行います。

**検出された Intel AMT デバイスを管理デバイスのリストに移動するには**

1. 非管理デバイスのリスト内の 1 つ以上のデバイス名をクリックします。
2. ツール バーの [ターゲット] ボタンをクリックします。
3. 下部ウィンドウの [管理] ボタンをクリックし [ターゲット デバイスの移動] を選択してから、[移動]
   をクリックします。

   リストに管理するデバイスがすべて表示されている場合、選択して下部ウィンドウにある [管理]
   ボタンをクリックし、[選択されたデバイスを移動します] を選択してから [移動] をクリックします。

デバイスは非管理デバイスのリストから削除されて、[すべてのデバイス]
リストに表示されます。デバイスを [マイ デバイス] リストに移動すると、Intel AMT
の初期設定がバックグラウンド
プロセスで実行されます。この間、他の検出または管理タスクを続行できます。

Intel AMT デバイスの管理の詳細については、「Intel* AMT デバイスの管理」と「Intel* AMT
サポート」を参照してください。

# デバイス エージェントのインストールと設定

## エージェントのインストールと設定の概要

コンソールでクライアントをフルに管理できるようにするには、あらかじめクライアントに管理エージェントをインストールする必要があります。既定のエージェント構成
(すべての製品エージェントをインストールします)
をインストールするか、独自のエージェント構成をカスタマイズしてデバイスにインストールできます。System Manager
のインストールではコアにエージェントが自動ではインストールされません。コアにエージェントをインストールしてから、手動でコアを再起動する必要があります。ヘルス
アラートを受信するためにはエージェント構成に監視エージェントが含まれている必要があります。

管理エージェントは、次のうち 1 つの方法でインストールできます。

- エージェントの導入。**[マイ デバイス]**リストでデバイスをターゲット指定し、そのデバイスにリモートでエージェントをインストールするようにエージェント構成タスクをスケジュールします。
- インストール パッケージを使用したエージェントのインストール。自己解凍型のデバイス インストール パッケージを作成します。このパッケージをローカル
デバイス上で実行してエージェントをインストールします。この操作を実行するには、管理者権限でサーバにログインする必要があります。
- エージェントのプル。コア サーバの ldlogon 共有フォルダ (*// サーバ名*/ldlogon) にドライブをマップし、SERVERCONFIG.EXE を
- 手動でポータブル USB ドライブのあるデバイス上で実行します (「インストール パッケージを使用したエージェントのインストール」を参照)。

インストールと構成の説明は、『*ユーザーズガイド*』の「デバイス エージェントの構成」の章を参照してください。

---

**注意 :[エージェントの構成]**ページで構成を選択して
**[既定に設定]**をクリックすることにより、特定のデバイス構成を既定の構成にすることができます。IPMI BMC のみの構成を既定の構成にすることはできません。既定の構成は削除できません。

---

Windows
システムでは、下記のようなポート設定で製品が完全に機能するためには、ファイアウォールを手動で構成する必要があります。これらの設定を変更するには、Windows の [コントロール パネル] から [Windows ファイアウォール] にアクセスします。

**管理サーバ :**

- ファイルおよびプリンタの共有 :TCP 139, 445; UDP 137,138
(この設定をしないとプッシュが機能しません)
- ソフトウェア配布 :TCP 9595 (この設定をしないとプッシュが機能しません)

- 詳細 :ICMP – [エコー要求の着信を許可する] (この設定が有効でないと検出されません)

**コア サーバ :**

- インベントリ : 5007
- リモート コントロール : 9535

これを実行するには、**[スタート]**、**[コントロール パネル]**、**[セキュリティ センター]**の順にクリックします。

## 既存のエージェントの更新

標準の管理エージェントまたはリモート コントロール
エージェントがまだインストールされていないデバイスにも、エージェント構成をプッシュできます。認証資格設定の詳細については、『*ユーザーズ ガイド*』の「エージェントの構成」を参照してください。

エージェント
パッケージをインストールすると、以前のエージェントが削除されて新しいエージェントがインストールされます。削除する必要のあるエージェントを含まない新しいエージェント
パッケージを作成することによって、目的のエージェントをアンインストールできます。

## エージェントのアンインストール

サーバからエージェントをアンインストールする必要がある場合は、次の手順に従ってください。

**警告 :** Uninstallwinclient.exe は、**/noreboot** スイッチをコマンド
ラインに使用しない限り、エージェントのアンインストール後に既定でデバイスを再起動します。再起動はアンインストールを完了するために必須です。再起動を開始した場合、サーバは通知なしに再起動し、他のすべてのアプリケーションも強制終了されます。/noreboot
スイッチを使うと、サーバは再起動せずに動作を続けます。

**エージェントをサーバからアンインストールするには**

1. 管理者権限のあるアカウントでサーバにログインします。
2. コア サーバの**ldmain**共有フォルダにドライブをマップします。
3. コマンド プロンプトを開き、ManagementSuite
   フォルダのドライブ文字を変更してから、次のように入力します。

   uninstallwinclient.exe /noreboot

アンインストールは自動的に実行され、すべてのエージェントが削除されます。

**[スタート]**、**[ファイル名を指定して実行]** を選択し、**¥¥*core name*¥ldmain¥uninstallwinclient.exe /noreboot** を選択することもできます。

**エージェントを Linux サーバからアンインストールするには**

1. linuxuninstall.tar.gz ファイルを Linux デバイスの一時ディレクトリにコピーします。これは、コアサーバの ManagementSuite 共有フォルダに見つけられます。

   Linux デバイスには Samba がインストール/構成されていないことがあるので、直接コピーすることはできません。通常、コアから pscp するか、リムーバブル メディアにいったんコピーします。
2. (Linux コンピュータ上の) シェル プロンプトから、tar と x、z、f オプションを使ってこのファイルを解凍します。

   tar -xzf linuxuninstall.tar.gz
3. ファイルの解凍後に、シェル プロンプトの現在のディレクトリから linuxuninstall スクリプトを実行します。

   ./linuxuninstall.sh

# エージェントの設定

コンソールでクライアントをフルに管理できるようにするには、あらかじめクライアントに管理エージェントをインストールする必要があります。System Manager のインストールではコアにエージェントが自動ではインストールされません。コアにエージェントをインストールしてから、手動でコアを再起動する必要があります。既定のエージェント構成の 1 つを利用するか、コンソールで新しいエージェント構成を作成したら、その構成を次の 3 つのうちいずれかの方法で Windows または Linux デバイスにインストールできます。

- エージェント構成を作成し、**[マイデバイス]**リストでデバイスをターゲット指定して、そのデバイスにリモートでエージェントをインストールするようにエージェント構成タスクをスケジュールします。
- 自己解凍型のインストール パッケージを作成します。このパッケージをローカル デバイス上で実行してエージェントをインストールします。この操作を実行するには、管理者権限でサーバにログインする必要があります。詳細については、「インストール パッケージを使用したエージェントのインストール」を参照してください。
- Windows デバイスから、コアの ldlogon 共有フォルダ (¥¥*myserver*¥ldlogon) にマッピングして SERVERCONFIG.EXE を実行します。

**エージェント構成を作成するには**

1. 左側のナビゲーション ペインで、**[エージェントの構成]** をクリックします。
2. **[新規]**をクリックします。

3. **[構成名]** ボックスに新しい構成の名前を入力します。

   作成する構成の説明になるような名前を入力します。既存の名前または新しい名前を指定できます。

4. 構成のプラットフォームを選択します。
5. その構成のインストール タイプを選択します (ユーザが選択した構成または IPMI BMC のみの構成)。**[構成]**にある**[IPMI BMC のみの構成]**を選択してIPMI 対応デバイス上の BMC (Baseboard Management Controller) を設定します。

   IPMI BMC のみの構成は、BMC (Baseboard Management Controller) をアウトオブバンド アクセスに設定し、フル インベントリ スキャンを実行し、自身を削除します。IPMI BMC のみの構成を既定の構成にすることはできません。IPMI BMC のみの構成を作成した場合、以下の手順で説明される編集オプションの大部分が利用できないことに気をつけてください。

6. 作成した構成を選択し、**[編集]** をクリックします。

   各種タブのいくつかのオプションには、選択した構成に対して設定可能ではないため、淡色表示されているものもあります。
7. **[エージェント]** タブで、導入するエージェントを選択します。

   - **すべて** : 選択したサーバにすべてのエージェントをインストールします。
   - **標準の管理エージェント** :デバイスとコア サーバの間の通信の基盤になります。これは必須エージェントです (BMC のみの構成の場合を除く)。このエージェントの処理の大部分は、オンデマンドです。
   - **ソフトウェア更新** :ソフトウェア更新スキャナをインストールします。このエージェントがインストールされると、スキャナの実行方法を設定できるようになります。これはオンデマンドのエージェントではありません。
   - **監視** :選択したサーバに監視エージェントをインストールします。監視エージェントは、ASIC の直接監視、インバンド IPMI、アウトオブバンド IPMI、および CIM などの多くのタイプの監視に対応しています。これはオンデマンドのエージェントではありません。
   - **Active System Console** :System Manager のインターフェイスまたはメニューを通して Intel Active System Console にアクセスできるようにするエージェントをインストールします。このエージェントは、Intel 製マザーボードを持つデバイスでのみサポートされています。

8. **[構成システムのタイプ]**ボックスで、タイプを選択します。このボックスが淡色表示になっている場合は、タイプがすでに選択されています。

9. **[再起動]**オプションを選択します。

   手動による再起動を選択した場合、デバイスはインストール後に再起動されません。エージェントの構成後は、デバイスを再起動する必要はありません。デバイスを手動で再起動する必要があります。

   更新ファイルがロックされている場合、エージェントの更新には再起動が必要になります。

10. [インベントリ] タブで、インベントリ
    スキャナ構成の設定を指定します。これらの設定について次に説明します。
    - **自動更新** : ソフトウェア スキャン中にリモート デバイスがコア サーバからソフトウェア リストを読み取ります。このオプションが設定されている場合、デバイスがソフトウェア リストにアクセスできるように、各デバイスのドライブをコア サーバの LDLOGON ディレクトリにマップする必要があります。ソフトウェア リストへの変更は、デバイスに直ちに適用できます。
    - **手動更新** : ソフトウェア スキャン中にタイトルを除外するために使用されるソフトウェア リストが各リモート デバイスにダウンロードされます。ソフトウェア リストがコンソールから変更されるたびに、リモート デバイスにソフトウェア リストを手動で送信する必要があります。
    - **インベントリ スキャナ設定** :インベントリ スキャナが実行する時間です。頻度を選択したり、スタートアップ時に実行するように指定できます。管理サーバからスキャナを手動で実行することができます。その場合、[スタート]、[プログラム]、LANDesk [Management]、[インベントリ スキャン] の順にクリックして起動してください。Linux では、root としてログインした後、次のコマンドラインから実行します。/usr/LANDesk/ldms/ldiscan -ntt

      - **スタートアップ時に実行する** :デバイスのスタートアップ時にインベントリ スキャナを実行します。HP-UX 構成を作成している場合、HP-UX は日単位、週単位、月単位で実行する cron ジョブとして実行するように設定されているために、このボタンは淡色表示になります。これは編集できません。
      - **開始日時** :スキャナの実行が可能な時間の範囲を指定します。デバイスが指定した時間内にログインすると、インベントリ スキャンが自動的に実行されます。デバイスがすでにログインしている場合は、開始時間が来ると、インベントリ スキャンが自動的に開始されます。このオプションは、一度にすべてのデバイスにスキャンを送信するのではなく、段階的にインベントリ スキャンを実行する場合に便利です。
      - **実行周期** :増加を表す数値 (1、2、3、など) と測定単位 (分、時間、日など) を入力します。

- **制限** : インベントリ
  スキャナが実行可能な日と時間を制限します。**[時間]**、**[曜日]**、**[日付]**
  をクリックして、抱合的パラメータを入力します。たとえば、**[日付]**に「10」、**[時間]**
  に「1:00 AM and 3:00 AM」を入力すると、インベントリ スキャナに毎月 10 日の
  1:00 AM と 3:00 AM の間に実行することを許可します。

- **[ソフトウェア更新]**タブでソフトウェア更新スキャナを実行させる日付と時間を設定します。
  スキャナはスケジュールされているタスクを必要とせずに自動的に実行します。
  **スタートアップ時に実行する**
  :デバイスのスタートアップ時にソフトウェア更新スキャナを実行します。
- **開始日時**
  :スキャナの実行が可能な時間の範囲を指定します。デバイスが指定した時間内にログインすると、ソフトウェア更新スキャンが自動的に実行されます。デバイスがすでにログインしている場合は、開始時間が来ると、ソフトウェア更新スキャンが自動的に開始されます。このオプションは、一度にすべてのデバイスにスキャンを送信するのではなく、段階的にスキャンを実行する場合に便利です。
- **実行周期** :増加を表す数値 (1、2、3、など) と測定単位 (分、時間、日など) を入力します。
- **制限** :
  ソフトウェア更新スキャナが実行可能な日と時間を制限します。**[時間]**、**[曜日]**、**[日付]**
  をクリックして、抱合的パラメータを入力します。たとえば、**[日付]**に「10」、**[時間]**に「1:00 AM and 3:00 AM」を入力すると、インベントリ スキャナに毎月 10 日の 1:00 AM と 3:00 AM の間に実行することを許可します。

12. **[ルールセット]** タブで、構成に含める任意の監視またはアラート
    ルールセットを選択します。これらのルールセットは、ldlogon/alertrules
    フォルダに保存されています。新しいルールセットは、**[監視]**または
    **[アラート]**に作成できます。新しく作成したルールセットをドロップダウン
    リストに表示するには、カスタム ルールセットの XML を生成する必要があります。
13. データベースに情報を保存するには、**[変更内容の保存]**
    をクリックします。構成を配布可能なパッケージとして保存するには、**[ファイルとして保存する]**
    をクリックします。

---

**注意** :**[エージェントの構成]** ページで構成を選択して
**[既定に設定]**をクリックすることにより、特定のエージェント構成を既定の構成にすることができます。既定の構成は削除できません。

---

**エージェント構成タスクをスケジュールするには**

1. 左側のナビゲーション ペインで、**[エージェントの構成]** をクリックします。
2. エージェントの構成をクリックして **[タスクのスケジュール]**をクリックします。
3. ターゲット デバイスとタスク スケジュールのリストを編集します。
4. **[保存]**をクリックします。

**[タスクのスケジュール]** をクリックすると、タスクが作成されます (ターゲット
デバイスがなく、スケジュールはされていません)。このエージェント構成タスクを保存しないでキャンセルする場合、そのタスクがすでに作成されていて、**[タスク]** リストに [スケジュールされていません]

というステータスといっしょに表示されていることに注意してください。**[マイ タスク]** リストから削除できます。

---

エージェント構成タスクが完了したら、コンソール内のデバイスに関する情報を表示するためにデバイスを再起動する必要があります (「サーバ情報コンソールの表示」を参照)。この再起動は、エージェントをコア サーバ上および管理デバイス上にインストールした場合に必要になります。エージェント構成プロセスでは再起動時間を選択できるので、再起動はサーバの使用を妨害しません。

---

# 管理デバイスへのエージェントの導入

デバイスを検出したら、それらのデバイスにエージェントを導入できます。サポートされている Windows、Linux、および HP-UX デバイスにのみエージェントを導入できます。Windows デバイスにエージェントを導入するには、管理者権限が必要であり、Linux と HP-UX デバイスでは root 権限が必要です。

以下に示す方法のいずれかを使用して、非管理デバイスにエージェントを導入できます。

- 検索ジョブおよび検索ジョブを処理するスケジューラ サービス用に構成したドメイン管理アカウントによるプッシュ型の導入。ドメイン管理アカウントは、スケジューラ サービスに、サーバ エージェントをインストールするのに必要な権限を与えます。これは、Windows NT 系のサーバで機能します。
- 標準の管理エージェントによるプッシュ型の導入。サーバが多くの LANDesk ソフトウェア製品によって使用される標準の管理エージェントをインストールしている場合は、ドメイン管理アカウントを使用しないで導入できます。

検出されたデバイスに導入する場合は、**[非管理]** ツリーの **[フィルタ]** オプションを使用します。IP アドレスをフィルタして、デバイスを特定します。

Windows システムでは、下記のようなポート設定で製品が完全に機能するためには、ファイアウォールを手動で構成する必要があります。これらの設定を変更するには、Windows の [コントロール パネル] から [Windows ファイアウォール] にアクセスします。

**管理サーバ :**

- ファイルおよびプリンタの共有 :TCP 139, 445; UDP 137,138 (この設定をしないとプッシュが機能しません)
- ソフトウェア配布 :TCP 9594、9595 (この設定をしないとプッシュが機能しません)
- 詳細 – ICMP :[エコー要求の着信を許可する] (この設定が有効でないと検出されません)

**コア サーバ :**

- インベントリ : 5007
- リモート コントロール : 9535

## デバイス認証資格情報の設定

標準の管理エージェントをインストールしている非管理デバイスには、エージェント導入のための認証資格情報が必要ありません。標準の管理エージェントをインストールしていない Windows OS サーバにエージェントをインストールするには、コンソール デバイス上のスケジューラ サービスが必要な権限を取得するのに使用する資格情報を指定する必要があります。

非管理デバイスにデバイス エージェントをインストールするには、スケジューラ サービスが管理者アカウントでデバイスに接続できる必要があります。スケジューラ サービスが使用する既定のアカウントは、LocalSystem です。LocalSystem の資格情報は、通常ドメイン内にないデバイスについて有効です。

デバイスがドメイン内にある場合は、ドメインの管理者アカウントを指定する必要があります。複数のドメインで非管理デバイスを設定する場合は、一度に 1 つのドメインを設定する必要があります。スケジューラ サービスは 1 セットの資格情報で認証し、各ドメインは異なるドメイン管理者アカウントが必要なためです。

コア サーバには、インベントリ オプションをカスタマイズする際に使用できるサービス設定ユーティリティが含まれています。このユーティリティはコア サーバにおいてのみ実行できます。

**スケジューラ サービスのログイン資格情報を設定するには**

1. コア サーバ上でサービスの設定ユーティリティを起動するには、**[スタート]**、**[プログラム ファイル]**、**[LANDesk]**、**[サービスの設定] をクリックします。**
2. **[スケジューラ]**タブをクリックします。
3. **[ログインの変更**ボタンをクリックします。
4. サービスがクライアント上で使用する資格情報、通常はドメイン管理者アカウントを入力します。

# エージェントのインストール

コンソールで作成したエージェント構成は、デバイスにインストールする必要があります。System Manager のインストールではコアにエージェントが自動ではインストールされません。コアにエージェントをインストールしてから、手動でコアを再起動する必要があります。

クライアント エージェント パッケージは、単一の自己解凍実行ファイルです。既定では、パッケージはコア サーバの ¥Program Files¥LANDesk¥ManagementSuite¥ldlogon フォルダに保存されます。この実行ファイルを実行すると、ユーザが何も入力しなくてもクライアント エージェントが自動的にインストールされます。正常にエージェントを管理デバイスをインストールするためにブラウザは必須ではありません。

## エージェントのインストール

新しいクライアント構成を作成してそれをコンソールから配布することによってエージェントを更新するか、非管理デバイスにエージェントを直接インストールできます。

クライアント エージェント パッケージを 1 つインストールすると、別のクライアント エージェント パッケージをインストールするときにすべてのエージェントが削除され、選択したエージェントだけがインストールされます。削除する必要のあるエージェントを含まない新しいクライアント エージェント パッケージを作成することによって、目的のエージェントをアンインストールできます。

## エージェントのアンインストール

デバイスからエージェントをアンインストールする必要がある場合は、「エージェントのインストールと設定の概要」を参照してください。

# インストール
# パッケージを使用したエージェントのインストール

エージェントのインストール方法の 1 つとして、自己解凍型のデバイス エージェント パッケージを使用する方法があります。この方法を使用すると、CD または USB ドライブにファイルをコピーして、エージェントを手動でインストールできます。これらのパッケージを作成するには、**[構成]**ダイアログの下にある**[ファイルとして保存する]** をクリックします。

1. **[エージェントの構成]** をクリックして、構成名をダブルクリックします。
2. **[エージェントの構成]** ダイアログで、**[ファイルとして保存する]**、**[閉じる]** をクリックします。

**[ファイルとして保存する]**
をクリックすると、指定した構成名と同じ名前の自己解凍型実行可能パッケージが作成されます。パッケージがコア サーバの ¥Program Files¥LANDesk¥ManagementSuite¥ldlogon¥ConfigPackages フォルダで使用できるまでに数分かかる場合があります。

この実行ファイルを実行すると、ユーザが何も入力しなくてもエージェントがインストールされます。この場合、管理者権限でログインしている必要があります。

---

パッケージをインストールするためにユーザが管理者権限でログインできない場合は、管理者が電子メール、Web ダウンロード、ログイン スクリプト、または共有から導入できます。

---

# エージェントのプル

このセクションでは、コマンド ラインからエージェントを導入する方法の詳細についてを説明します。SERVERCONFIG.EXE コマンドライン パラメータを使用して、デバイスにインストールされているコンポーネントを制御できます。SERVERCONF

IG.EXE はスタンドアローン モードで起動できます。SERVERCONFIG.EXE は、Windows サーバから読み込み可能な *http:¥¥coreserver¥LDLogon* 共有フォルダにあります。

SERVERCONFIG.EXE はデバイス設定に SERVERCONFIG.INI を使用します。

## SERVERCONFIG.EXE について

SERVERCONFIG.EXE は、次のプロセスで、Windows NT ファミリ サーバを管理できるように設定します。

1. SERVERCONFIG
   は、コンピュータが管理エージェントを使って設定されているかどうかを調べます。設定されている場合は、SERVERCONFIG
   はすべてのコンポーネントを削除して、選択したコンポーネントを再インストールします。
2. SERVERCONFIG は適切な初期化ファイル (SERVERCONFIG.INI)
   を読み込み、そのファイルに含まれている命令を実行します。

SERVERCONFIG.EXE には、次のコマンドライン パラメータを使用できます。

| **パラメータ** | **説明** |
|---|---|
| /I | 含めるコンポーネント (引用符が含まれる) :<br><br>"Common Base Agent"<br><br>"Inventory Scanner"<br><br>"Alerting"<br><br>"Vulnerability Scanner"<br><br>"Server Monitor"<br><br>これらのパラメータは同一コマンド<br>ライン上で結合できます。たとえば次のとおりです。<br><br>SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner" |
| /L または /Log= | サーバが設定されたか設定されなかったかを記録する CFG_YES および CFG_NO ログ ファイルへのパスです。 |
| /LOGON | [LOGON] という接頭辞が付いたコマンドを実行します。 |
| /N または /NOUI | ユーザ インターフェイスを表示しません。 |

| パラメータ | 説明 |
|---|---|
| /NOREBOOT | 終了時サーバを再起動しません (既定)。 |
| /REBOOT | 実行後に強制的に再起動します。 |
| /X= | 除外するコンポーネント。たとえば次のとおりです。<br><br>SERVERCONFIG.EXE /X=SD |
| /CONFIG=<br><br>/[CONFIG]= | 既定の SERVERCONFIG.INI ファイルの代わりに使用するサーバ コンフィグレーション ファイルを指定します。<br><br>たとえば、NTTEST.INI<br>という設定ファイルを作成した場合は、次の構文を使用します。<br><br>SERVERCONFIG.EXE /CONFIG=TEST.INI<br><br>カスタム .INI ファイルは SERVERCONFIG.EXE<br>と同じディレクトリに存在する必要があります。また、/config<br>パラメータでは、接頭辞 NT<br>を付けないファイル名を使用することに注意してください。 |
| /? または /H | ヘルプ メニューを表示します。 |

## エージェント構成の作成

**[エージェントの構成]**を使用して、サーバ エージェント構成
(管理サーバ上にインストールされるエージェントなど)
の作成および更新を行います。グループ固有の必要に応じて、異なる構成を作成できます。たとえば、Web サーバとアプリケーション サーバに対して別の構成を作成できます。

サーバに構成をプッシュするには、次の手順を実行する必要があります。

- **エージェント構成の作成** :サーバ用に固有の設定を設定します。
- **エージェント構成のスケジュール** :サーバに、またはサーバから構成をプッシュし、コア サーバの LDLogon 共有フォルダから SERVERCONFIG.EXE を実行します。

**エージェント構成を作成するには**

1. コンソールで、**[エージェントの構成]**をクリックします。
2. **[新規]**ツールバー ボタンをクリックします。
3. **構成名**を入力し、オペレーティング システムを選択して、**[OK]**をクリックします。
4. 新しい構成名をクリックして、**[編集]**をクリックします。

5. 導入するエージェントを選択します。
6. ダイアログの上部のタブを使用して、選択したコンポーネントに関連したオプションに移動します。必要に応じて、選択したオプションをカスタマイズします。
7. **[変更内容の保存]**をクリックして、ダイアログを閉じます。
8. この構成を既定に設定する場合は、**[既定に設定]**をクリックします。

## Linux エージェント構成のプル

### Linux エージェント構成をプルするには

1. Linux デバイスに一時ディレクトリを作成して (/tmp/ldcfg など)、次をそのディレクトリにコピーします。
    1. LDLOGON¥unix¥linux ディレクトリのすべてのファイル。
    2. 構成に基づいて名づけられたシェル スクリプト (<*構成名*>.sh) を一時ディレクトリにコピーします。
    3. 構成に基づいて名づけられた *.0 ファイルを一時ディレクトリにコピーします。* は、8 つの文字を表します (0-9、a-f)。
    4. <*構成名*>.ini ファイルに一覧表示されているすべてのファイルを一時ディレクトリにコピーします。これらのファイルを特定するには、「FILE*xx*」という INI ファイルを探します。「*xx*」は数字です。検索される大部分の項目は、手順 1 でクライアントにコピーされていますが、.XML ファイルはコピーする必要があります。ファイル名は変更できませんが、次の例外があります。
        - alertrules¥<*任意のテキスト*>.ruleset.xml は、internal.ruleset.xml に名称変更する必要があります。
        - monitorrules¥<*任意のテキスト*>.ruleset.monitor.xml は、masterconfig.ruleset.monitor.xml に名称変更する必要があります。
2. デバイスに IPMI および BMC がある (インストレーションに監視機能も含まれている) 場合、次の行をコマンド ラインに入力します。

    export BMCPW="(bmc password)"

3. ルートとして実行し、構成のシェル スクリプトを実行します。たとえば、スクリプトの名前が「pull」の場合、以下に使用されているフルパスを使用します。

    /tmp/ldcfg/pull.sh

4. 一時ディレクトリとその中のファイルをすべて削除します。

注意 : エージェントを Linux デバイスへプッシュまたはプルしてから

./linuxuninstall.sh -f ALL

を実行し、そのデバイスをクリアしてから再度プッシュまたはプルを行った場合、GUID のあるファイルが、この操作の完了後にデバイス上に唯一残されるファイルになります。

-f オプションにより、製品のすべてのディレクトリが削除されます。詳細については、「Linux のアンインストール ドキュメント」を参照してください。

## スタンドアローン エージェント構成パッケージの作成

通常は、エージェント構成ユーティリティ SERVERCONFIG.EXE が管理デバイスのエージェントを設定します。希望する場合は、**[エージェントの構成]**ウィンドウを使用して、実行されるサーバにエージェント構成をインストールする単一の自動解凍型実行ファイルを作成できます。これは、CD またはポータブル USB ドライブからエージェントをインストールする場合に便利です。

## デバイスへのエージェント構成のプッシュ

**エージェント構成をプッシュするには**

1. コンソールで、エージェントを導入するデバイスを選択して、**[ターゲット]**をクリックします。
2. 左側のナビゲーション ペインで、**[エージェントの構成]**をクリックします。
3. プッシュするエージェント構成を右クリックして、**[タスクのスケジュール] をクリックします。**
4. **[タスクのスケジュールのプロパティ]**ダイアログ ボックスで、**[ターゲット デバイス]**をクリックし、**[ターゲット一覧の追加]**をクリックします。
5. **[タスクのスケジュール]**をクリックします。
6. エージェントを導入する時刻を指定して、**[保存]**をクリックします。

# Linux サーバ エージェントのインストール

Linux エージェントと RPM を Linux サーバ上にリモートで導入およびインストールできます。そのためには、Linux サーバを正しく設定する必要があります。Linux サーバにエージェントをインストールするには、ルート権限が必要です。

既定の Linux のインストール (Red Hat 3 と 4、および SUSE) には、Linux 標準エージェントに必要な RPM が含まれています。**[エージェントの構成]** で監視エージェントを選択する場合は、追加 RPM、sysstat が必要です。製品に必要なすべての RPM のリストについては、『*System Manager Deployment Guide*』を参照してください。

最初の Linux エージェント構成では、コア サーバは SSH を使用してターゲット Linux サーバに接続します。認証されたユーザ名とパスワードで SSH 接続を確立しておく必要があります。この製品は、公開キーと秘密キーによる認証をサポートしていません。コア サーバと Linux サーバ間のすべてのファイアウォールで SSH ポートを許可する必要があります。コア サーバからの SSH 接続をサードパーティ製 SSH アプリケーションでテストすることを検討してください。

Linux エージェントのインストール パッケージには、シェル スクリプト、エージェントの tarball、.INI エージェント構成、およびエージェントの認証証明書が含まれています。これらのファイルは、コア サーバの LDLogon 共有フォルダに格納されます。シェル スクリプトは、tarball からファイルを抽出して RPM をインストールし、エージェントの構成で指定した間隔でエージェントのロードとインベントリ スキャナを実行するようにサーバを設定します。ファイルは /usr/landesk に配置されます。

コア サーバ上のスケジューラ サービスを、Linux サーバ上の SSH 認証資格情報 (ユーザ名とパスワード) を使用するように設定する必要もあります。スケジューラ サービスは、これらの資格情報を使用してサーバにエージェントをインストールします。サービス設定ユーティリティを使用して、スケジューラ サービスで代替の資格情報として使用する SSH 資格情報を入力します。このユーティリティが完了すると、スケジューラ サービスを再起動するように要求されます。再起動を要求されない場合は、**[スケジューラ]**タブで **[停止]** をクリックしてから**[開始]** をクリックして、サービスを再起動します。これにより、変更が反映されます。

## Linux エージェントの導入

Linux サーバを設定してコア サーバに Linux 資格情報を追加したら、Linux エージェントを導入できるように、**[マイ デバイス]**リストにサーバを追加する必要があります。サーバにエージェントを導入するには、そのサーバを**[マイ デバイス]** リストに追加しておく必要があります。そのためには、**[デバイス検索]** で Linux サーバを検索します。

### Linux サーバを検索するには

1. **[デバイス検索]** で、各 Linux サーバの検索ジョブを作成します。標準のネットワーク スキャンを使用して、検索する範囲の開始 IP と終了 IP に Linux サーバの IP アドレスを入力します。多数の Linux サーバがある場合は、IP アドレスの範囲を入力します。検索する IP 範囲を追加したら、**[OK]**をクリックします。
2. 作成した検索タスクをクリックし、**[スケジュール]**をクリックすることによって、そのタスクをスケジュールします。タスクが終了したら、管理する Linux サーバが検索プロセスで検出されているか確認します。
3. **[デバイス検索]**で、管理するサーバを選択し、**[ターゲット]**をクリックしてこのデバイスを [ターゲット]リストに追加します。ウィンドウの下半分にある **[管理]**タブをクリックします。**[選択されたデバイスを移動します]** をクリックして**[移動]**をクリックします。これにより、**[マイ デバイス]**リストにサーバが追加されるので、導入先のサーバとして選択できるようになります。

### Linux エージェント構成を作成するには

1. **[エージェントの構成]**で、**[新規]**をクリックします。
2. 構成名を入力して**[HP-UX]** または **[Linux Server Edition]** をクリックし、インストールのタイプ (サーバまたはデスクトップ) を選択してから **[OK]**をクリックします。
3. 作成した構成を選択し、**[編集]**をクリックします。
4. エージェントを選択します。

5. **[インベントリ]** タブで、オプションとスキャナの実行間隔を選択します。インストール スクリプトによって、選択した間隔でスキャナを実行する cron ジョブが追加されます。
6. **[ルールセット]** タブで、構成に含める任意の監視またはアラート ルールセットを選択します。これらのルールセットは、ldlogon/alertrules フォルダに保存されています。
7. **[変更内容の保存]**をクリックします。

エージェント構成を導入するには、**[エージェントの構成]**で構成を選択して **[タスクのスケジュール]**をクリックします。**構成タスク]**[で、タスクを構成してタスクの進捗状況を監視します。

**注意** :インベントリ スキャナがインストール後に最初のスキャンを完了するまでは、Linux デバイスのヘルス情報は取得できません。

### Linux エージェント構成をプルするには

1. Linux デバイスに一時ディレクトリを作成して (/tmp/ldcfg など)、次をその一時ディレクトリにコピーします。
   - LDLOGON¥unix¥linux ディレクトリのすべてのファイル。
   - 構成に基づいて名づけられたシェル スクリプト (<*構成名*>.sh)。
   - 構成に基づいて名づけられた *.0 ファイル。* は、8 つの文字を表します (0-9、a-f)。
   - <*構成名*>.ini
     ファイル内に一覧表示されているすべてのファイル。これらのファイルを特定するには、「FILE*xx*」という INI ファイルを探します。「*xx*」は数字です。検索される大部分の項目は、手順 1 でクライアントにコピーされていますが、.XML ファイルはコピーする必要があります。ファイル名は変更できませんが、次の例外があります。
     - alertrules¥<*任意のテキスト*>.ruleset.xml は、internal.ruleset.xml に名称変更する必要があります。
     - monitorrules¥<*任意のテキスト*>.ruleset.monitor.xml は、masterconfig.ruleset.monitor.xml に名称変更する必要があります。

2. デバイスに IPMI および BMC がある (インストレーションに監視機能も含まれている) 場合、次の行をコマンド ラインに入力します。

   export BMCPW="(bmc password)"

3. ルートとして実行し、構成のシェル スクリプトを実行します。

   /tmp/ldcfg/lsminstall.sh

4. 一時ディレクトリとその中のファイルをすべて削除します。

**注意**：エージェントを Linux デバイスへプッシュまたはプルしてから

./linuxuninstall.sh –f ALL

を実行し、そのデバイスをクリアしてから再度プッシュまたはプルを行った場合、GUID のあるファイルが、この操作の完了後にデバイス上に唯一残されるファイルになります。

–f オプションにより、製品のすべてのディレクトリが削除されます。詳細については、「Linux のアンインストール ドキュメント」を参照してください。

## インベントリ スキャナのコマンド ライン パラメータ

インベントリ スキャナである ldiscan には、実行方法を指定するコマンドライン パラメータがいくつかあります。それぞれの詳細については ldiscan –h または man ldiscan の説明を参照してください。各オプションには、'–' または '/' という接頭辞が付きます。

| パラメータ | 説明 |
|---|---|
| –d=Dir | ルートではなく Dir<br>ディレクトリでソフトウェアのスキャンを開始します。既定では、スキャンはルート ディレクトリで開始されます。 |
| –f | ソフトウェア スキャンの強制 :–f<br>を指定しないと、スキャナは**[構成]**、**[サービス]**、**[インベントリ]**、**[スキャナの設定]** の順に選択した場所のコンソールに指定された日数間隔で (既定では毎日) ソフトウェアをスキャンします。 |
| –f– | ソフトウェアのスキャンを無効にします。 |
| –i=ConfName | コンフィグレーション ファイル名を指定します。既定のファイル名は /etc/ldappl.conf です。 |
| –ntt=address:port | コア サーバのホスト名または IP アドレス。ポートはオプションです。 |
| –o=File | 指定された出力ファイルにインベントリ情報を書き込みます。 |
| –s=Server | コア<br>サーバを指定します。このコマンドはオプションであり、互換性の維持のみを目的としています。 |

| パラメータ | 説明 |
|---|---|
| –stdout | インベントリ情報が標準出力に書き込まれます。 |
| –v | スキャン時に詳細なステータス メッセージを表示します。 |
| –h または –? | [ヘルプ] 画面を表示します。 |

## 例

テキスト ファイルにデータを出力するには、次のように入力します。

```
ldiscan –o=data.out –v
```

コア サーバにデータを送信するには、次のように入力します。

```
ldiscan –ntt=ServerIPName –v
```

## Linux インベントリ スキャナ ファイル

| ファイル | 説明 |
|---|---|
| ldiscan | 実行するアクションを示すコマンドライン<br>パラメータによって実行される、実行可能ファイルです。スキャナを実行するすべてのユーザには、ファイルを実行するための十分な権限が必要です。<br><br>このファイルには、前述の対応プラットフォームごとに異なるバージョンがあります。 |
| /etc/ldiscan.conf | このファイルは常に /etc に存在し、次の情報が含まれています。<br><br>• インベントリに割り当てられた固有の ID<br>• 前回のハードウェア スキャン<br>• 前回のソフトウェア スキャン<br><br>スキャナを実行するすべてのユーザには、このファイルの読み取りおよび書き込みの属性が必要です。/etc/ldiscan.conf 内の固有の ID<br>は、初めてインベントリ<br>スキャナを実行したときにコンピュータに割り当てられる固有の番号です。この番号は、コンピュータを識別するときに使用します。この番号が変更された場合は、コア<br>サーバはそのコンピュータを別のコンピュータとして扱います。そのため、データベース内でエントリが重複する場合があります。 |

| ファイル | 説明 |
| --- | --- |
| | **警告** :作成後に固有の ID 番号を変更したり、ldiscan.conf ファイルを削除したりしないでください。 |
| /etc/ldappl.conf | このファイルは、ソフトウェア スキャンの実行時にインベントリ スキャナがレポートする実行可能ファイルのリストをカスタマイズします。ファイルにはいくつかの例が含まれており、使用するソフトウェア パッケージのエントリを追加する必要があります。検索条件はファイル名とファイル サイズに基づきます。このファイルは通常 /etc に存在しますが、-i= コマンドライン パラメータを使用することにより、スキャナは他のファイルを使用できます。 |
| ldiscan.8 | ldiscan の man ページです。 |

## コンソールの統合

Linux コンピュータがコア データベースにスキャンされると、次のことを実行できます。

- Linux インベントリ スキャナによりコア データベースに返された属性にクエリを実行します。
- レポート機能を使用して、Linux スキャナが収集した情報を含むレポートを生成します。たとえば、Linux はオペレーティング システムの概要レポートで OS タイプとして表示されます。
- Linux コンピュータのインベントリ情報を表示します。

---

**[システムの稼動時間] に対するクエリはアルファベット順に並び替えられ、予期しない結果を返します。**
特定の日数 (たとえば 10 日間) よりも長く実行されているコンピュータの台数の検出にクエリを実行するには、[システムの稼働時間] ではなく [システム起動] に対してクエリを実行します。システムの稼働時間は単に ″x 日、y 時、z 分、および j 秒間″ から構成される文字列であるため、そのクエリ結果は予期しない結果を返す可能性があります。並べ替えは時間の間隔ではなく、アルファベット順で行われます。

**ldappl.conf で参照される config ファイルへのパスはコンソールに表示されません。**
ldappl.conf ファイルの ConfFile エントリにはパスが含まれている必要があります。

---

# デバイスの監視

## 監視について

System Manager では、デバイスのヘルス
ステータスを監視する方法がいくつかあります。監視機能により、デバイスに関する次のようなさまざまなデータを追跡できるようにさまざまなソースからのデータが収集されます。

- 利用状況のレベル
- OS イベント
- プロセスとサービス
- パフォーマンスの履歴
- ハードウェア センサ (ファン、電圧、温度など)

この章では、管理デバイスを監視するさまざまな機能について説明します。

- デバイスへの監視エージェントのインストールとデバイスに導入する監視ルールセットの作成
- デバイスのパフォーマンス カウンタの設定とパフォーマンス データの監視
- 変更時にアラートを発行する構成変更の監視
- **デバイス監視**機能を使って定期的にデバイスを ping する接続の監視

アラートは、監視エージェントに関連する機能で、電子メールの送信やページャ
メッセージ、デバイスの再起動またはシャットダウン、アラート ログへの情報の追加などのアラート
アクションの起動に監視エージェントを使用します。アラートは、監視可能なあらゆるデバイス
イベントから発行できます。詳細については、「アラートの使用方法」を参照してください。

**注意**

- 監視エージェントとの通信は、GET、POST、または XML 要求の形式で HTTP over TCP/IP
  を使用して行われます。要求に治する応答は、XML または HTML テーブル ドキュメントです。
- デバイスのヘルス状態についてのクエリ (Computer.Health.State)
  を実行および保存する場合は、データベースの状態が数字で表されることに注意します。数字はステータスに対応しており、4=危険、3=警告、2=標準, 1=情報、null、0=不明となっています。
- ハードウェア監視は、デバイスにインストールされているハードウェアの機能とハードウェアの正しい構成に依存します。たとえば、S.M.A.R.T.
  監視機能を持つハードドライブがデバイスにインストールされているが、S.M.A.R.T.
  検出がデバイスの BIOS 設定で有効になっていない場合、または BIOS が S.M.A.R.T.
  ドライブをサポートしていない場合、監視データは利用できません。
- 特定のコンピュータからのレポートが停止している場合は、LDCLIENT フォルダにある
  restartmon.exe
  を使ってコレクタとすべての監視プロバイダを再開させることができます。このユーティリティは、レポート機能がインストールされていて、レポート機能が中断されているコンピュータ用です。このユーティリティを使って、デバイスを再起動せずにコレクタとプロバイダを再開します。

## デバイスへの監視エージェントの導入

デバイスに監視エージェントをインストールすると、System Manager はデバイスのヘルス状態に関する最新の概要を提供します。監視エージェントは、管理デバイスにインストール可能な 6 つのエージェントのうちの 1 つです。デバイスのハードウェアと構成を定期的、周期的に確認し、変更があればデバイスのヘルス ステータスに反映させます。デバイスのヘルス ステータスは、[**マイ デバイス**] リストのステータス アイコンで表示され、詳細はログ エントリ（デバイスの [**システム情報**] サマリに表示）とグラフ（デバイスの [**監視**] サマリ ページに表示）に表示されます。

たとえば、監視対象のデバイスのディスク ドライブが一杯になっている場合、ディスクが 90% 使用の場合は警告ステータス アイコンを表示し、95% 使用の場合は危険ステータス アイコンに変わるように設定できます。また、ディスク領域アラートのルールを含んだアラート ルールセットがデバイスに設定されていれば、同じディスク ドライブ ステータスについて、アラートも受信できます。

デバイスには、既定の監視ルールセットを導入するか、必要に応じて、関心のあるヘルス アイテムのみを含んだカスタム ルールセットを作成できます。

## 監視ルールセットの作成

監視エージェントがデバイスで確認する内容を定義した監視ルールセットを作成することにより、デバイスで監視する内容をユーザが選択できます。ルールセットの導入は、1 つのデバイスまたはグループのターゲット デバイスに対して行うことができます。たとえば、ストレージ専用のサーバ用に 1 つのルールセットを定義し、Web サーバには別のルールセットを用意することも可能です。

既定の監視ルールセットには 16 のアイテムが含まれます。ルールセットを作成する際には、これらのアイテムを個々にオンまたはオフにしたり、確認する頻度を指定したりできます。またアイテムによっては、パフォーマンスしきい値を設定できます。デバイス上で実行している特定のサービスを監視対象として選択することもできます。

アラート ルールセットの作成と導入の全体的なプロセスは次のようになります。

1. ルールセットを導入するデバイスを選択し、[**ターゲット**] をクリックしてこのデバイスを [**ターゲット デバイス**] リストに追加します。
2. 監視ルールセットの作成または編集ルールセットで監視するそれぞれのイベントに対して監視機能をオンにするチェックボックスを選択する必要があることに注意してください。既定ですべてのイベントが監視対象になっているわけではありません。また、サービスなど一部のイベントでも、監視対象にする各サービスを選択する必要があります。（上記の手順を参照。）
3. そのルールセットをターゲット デバイスに導入します。ルールセットを導入する前に、必要に応じてターゲット デバイスを追加できます。（上記の手順を参照。）

**監視ルールセットを作成するには**

1. 左側のナビゲーション ペインで、[**監視**] をクリックします。
2. [**新規**] をクリックし、構成の名前と説明を入力して [**OK**] をクリックします。
3. 左の列にある構成を選択します。
4. アイテムのリストから、変更するアイテムをクリックして [**編集**] をクリックします。
5. アイテムの監視をオフにするには、チェック ボックスの選択を外して [**更新**] をクリックします。
6. アイテムの監視頻度を変更するには、[**秒**] または [**分**] を選択してテキスト ボックスで数値を指定します。
7. 適用する場合は、警告または危険ステータスのしきい値の割合を設定します。
8. **サービス**の監視には、ドロップダウン リストから OS を選択します。監視するサービスを 1 つまたは複数選択し（複数選択には [Ctrl] キーを押しながらクリックします）、>> をクリックしてサービスを右側のリストに追加します。
9. 変更した各アイテムについて、[**更新**] をクリックして変更を構成に適用します。変更したアイテムを元に戻すには、[**元に戻す**] をクリックすると元の設定が復元されます。

---

コア サーバから監視構成の中のサービスを編集した場合、[**利用可能なサービス**] リストには、インベントリ データベースから既知のサービスが表示されます。LANDesk エージェントが 1 つ以上のデバイスに導入され、インベントリ スキャンの結果がコア サーバに返されるまで、[**利用可能なサービス**] リスト ボックスにはサービスが表示されません。たとえば、Linux サービスをリストから選択するには最初に Linux デバイスにエージェントを導入する必要があります。

---

**監視ルールセットを導入するには**

1. 左側のナビゲーション ペインで、[**マイ デバイス**] をクリックして、[**すべてのデバイス**] グループをクリックします。
2. ルールセットを導入するデバイスを選択し、[**ターゲット**] をクリックしてこのデバイスを [**ターゲット デバイス**] リストに追加します。
3. 左側のナビゲーション ペインで、[**監視**] をクリックして、[**ルールセットの導入**] タブをクリックします。
4. [**監視ルールセット**] ボックスで、導入するルールセットを選択します。
5. リンクをクリックして [**ターゲット デバイス**] リストを表示します。このリストからデバイスを削除するには、サーバを右クリックして [**削除**] をクリックします。（デバイスを追加するには、ステップ 2 に従ってターゲット リストにデバイスを追加する必要があります。）
6. [**導入**] をクリックして、選択したルールセットをターゲット デバイスに導入します。

導入プロセスの一部として、導入されるルールセットとルールセットが導入されるデバイスのリストが XML ページとして作成されます。このレポートはコア サーバの LDLOGON ディレクトリに保存され、データベースに割り当てられている連番を使った名前が付きます。ルールセットの導入を行わずにこの XML ページだけを表示する場合は、[**XML の生成**] ボタンをクリックし、リンクをクリックして XML ファイルを表示します。ルールセットを XML として作成すると、[**エージェント構成**] 設定に利用可能なルールセットのリストを表示できます。

## ModemView サービスをオフにする

ModemView サービスは、モデム コール (受信と送信の両方)
を監視してアラートを発行するサービス/ドライバです。このサービスは MFC を使用するため、約 10 MB のメモリを消費します。デバイスにモデムがない場合は特に、このサービスを実行する必要はありません。

**ModemView サービスをオフにするには**

1. 対象のデバイスで (直接またはリモート コントロールで) [**スタート**]、[**コントロール パネル**]、[**管理ツール**]、[**サービス**] の順にクリックします。
2. [**LANDesk Message Handler Service**] をダブルクリックします。
3. [**開始タイプ**] で [**手動**] を選択し、[**OK**] をクリックします。

または、[**サービス ステータス**] で [**停止**] をクリックすることもできます。

# パフォーマンス カウンタの設定

System Manager では、管理デバイス上で監視するパフォーマンス項目 (カウンタ)
を選択できます。ハードウェア コンポーネント (ドライブ、プロセッサ、メモリなど)、OS コンポーネント (プロセスなど)、またはアプリケーション コンポーネント (システムの Web
サーバによって転送されるバイト/秒など)
を始めとして、さまざまなアイテムを監視できます。パフォーマンス
カウンタを選択すると、項目をポーリングする頻度や、アラートが生成される前に許可されるパフォーマンスのしきい値や違反数も指定できます。

パフォーマンス カウンタを選択していると、[**監視**] ページでグラフをリアル
タイムに表示したり、履歴データを表示して、パフォーマンスを監視できます。詳細については、「パフォーマンスの監視」を参照してください。

**監視するパフォーマンス カウンタを選択するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。新しいブラウザ ウィンドウにサーバ情報コンソールが開きます。
2. 左側のナビゲーション ペインで、[**監視**] をクリックします。
3. [**パフォーマンス カウンタの設定**] をクリックします。
4. [**オブジェクト**] 列から、監視するオブジェクトを選択します。
5. [**インスタンス**] 列から、監視するオブジェクトのインスタンスを選択します (該当する場合)。
6. [**カウンタ**] 列から、監視する特定のカウンタを選択します。

   目的のカウンタがリストに表示されていない場合は、[**カウンタの再読み込み**] をクリックすると、リストが新しいオブジェクト、インスタンス、またはカウンタで更新されます。

7. ポーリング頻度 ([**チェック間隔**]) およびカウンタ履歴を維持する日数を指定します。

8. [**カウンタが範囲を超えた後にアラート**] テキスト ボックスで、
   アラートが生成される前にカウンタがしきい値を超えることを許可される回数を指定します。
9. しきい値の上限/下限を指定します。
10. [**適用**] をクリックします。

**注意**

- パフォーマンス ログ ファイルは急速にサイズが大きくなります。1 台のカウンタを 2
  秒間隔でポーリングする場合、パフォーマンス ログに毎日 2.5 MB の情報が追加されます。
- 警告アラートは、Windows または Linux デバイスでパフォーマンス
  カウンタが下限のしきい値を下回った場合に生成されます。Linux デバイスでは、パフォーマンス
  カウンタが上限のしきい値を超えた場合にも、警告アラートが生成されます。Windows
  デバイスでは、パフォーマンス
  カウンタが上限のしきい値を超えた場合には、重大アラートが生成されます。
- しきい値の設定時には、しきい値の上限を超えても下限を下回ってもアラートが生成されるということに留意してください。ディスク容量などの場合では、デバイスの容量が不足した場合にのみアラートが必要になります。この場合、上限のしきい値は十分に大きい数値に設定しておかないと、デバイスの空き容量が増えた際にアラートが生成されてしまうことになります。
- [**カウンタが範囲を超えた後にアラート**]
  の数を変更すると、解決されない問題や孤立したイベントがある場合には、それに焦点を合わせることができます。たとえば、Web サーバから送信されるバイトを監視する場合、System Manager はバイト/秒が連続して高くなると、警告することができます。または、匿名の FTP
  接続が一定のユーザ数を超えるときには常に警告するように、1、2
  などの低い数字を指定できます。

# パフォーマンスの監視

[**監視**] ページでは、各種のシステム
オブジェクトのパフォーマンスを監視できます。ドライブ、プロセッサ、メモリなどの特定のハードウェア
コンポーネントを監視したり、システムの Web サーバによって転送されるプロセスやバイト/秒などの OS
コンポーネントを監視できます。[**監視**] ページには、カウンタのリアルタイム
データや履歴データを示すグラフが表示されます。

パフォーマンス
カウンタを監視するには、まずカウンタを選択して、監視対象カウンタのリストに追加する必要があります。カウンタを選択するときに、アイテムのポーリング間隔、パフォーマンスのしきい値、およびしきい値を何回超えたらアラートを生成するかを設定します。カウンタの選択についての詳細は、「パフォーマンス カウンタの設定」を参照してください。

**監視対象カウンタのパフォーマンス グラフを表示するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。新しいブラウザ
   ウィンドウにサーバ情報コンソールが開きます。
2. 左側のナビゲーション ペインで、[**監視**] をクリックします。

3. 必要に応じて、[**アクティブなパフォーマンス カウンタ**] をクリックします。
4. [**カウンタ**] ドロップダウン リストでパフォーマンス グラフを表示するカウンタを選択します。
5. [**リアルタイム データの表示**] を選択して、リアルタイム パフォーマンスのグラフを表示します。

   または

   [**履歴データの表示**] をクリックして、カウンタの選択時に ([履歴の保存] で)
   指定した期間のパフォーマンスを示すグラフを表示します。

パフォーマンス
グラフの横軸は経過した時間を表します。縦軸は測定単位を表します。たとえば、バイト/秒
(ファイル転送などを監視する場合)、パーセント (CPU 使用率などを監視する場合)、利用可能なバイト数
(ハード ドライブ容量などを監視する場合)
があります。線の高さは固定されていません。データの最大値と最小値に応じて変わります。あるカウンタでは縦軸が 1 ～ 100 を表し、別のカウンタでは 1 ～ 500,000
を表す場合があります。データの最大値と最小値の差が大きい場合は、データの小さい変化が平らな線で表現される可能性があります。

**注意**

- 別のカウンタを選択すると、グラフが更新され、測定単位がリセットされます。
- [**更新**]  をクリックすると、グラフがクリアされて再度作成されます。
- リストに含まれるカウンタによって生成されたアラートを受信した場合は、そのカウンタを右クリックし、[**承認**] をクリックしてアラートをクリアします。

**パフォーマンス カウンタの監視を停止するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。新しいブラウザ ウィンドウにサーバ情報コンソールが開きます。
2. 左側のナビゲーション ペインで、[**監視**] をクリックします。
3. 必要に応じて、[**アクティブなパフォーマンス カウンタ**] をクリックします。
4. [**監視されているパフォーマンス カウンタ**] でカウンタを右クリックし、[**削除**] をクリックします。

# 設定変更の監視

この製品は、監視エージェントがインストールされているデバイスのハードウェアまたはソフトウェアの構成が変更された場合にアラートを生成できます。構成変更により、デバイスのパフォーマンスや安定性が低下したり、標準インストールで問題が発生したりする可能性があります。本製品では、デバイスの重要な部分を監視することによって、総所有コスト (TCO) を削減できます。

アラートを生成するデバイスの構成変更には、以下があります。

- **アプリケーションのインストールまたはアンインストール**：
  アプリケーションをインストールまたは削除したユーザを確認できます。これは、ライセンスや従業員の生産性を追跡するときに役立ちます。[コントロール パネル] の
  [アプリケーションの追加と削除]
  に登録されているアプリケーションを監視します。その他のアプリケーションは無視されます。通知ログまたはアラートのポップアップ ウィンドウには、[アプリケーションの追加と削除]
  で使用されているアプリケーション名が表示されます。
- **メモリの追加または削除**：インストールされているメモリ量とメモリ
  タイプを検出および監視します。構成が変更されると、アラートが生成されます。
- **ハード ドライブの追加または削除**：
  サーバに搭載されているドライブのタイプとサイズを検出および監視します。構成が変更されると、アラートが生成されます。
- **プロセッサの追加、削除、または変更**：
  プロセッサの数、タイプ、および動作周波数を検出および監視します。構成が変更されると、アラートが生成されます。
- **ネットワーク カードの追加または削除**：デバイスのネットワーク インターフェイス
  カードの数とタイプを検出および監視し、構成が変更されるとアラートを生成します。

構成の変更によるアラートの記録は、サーバ情報コンソールでアラート
ログを表示して確認できます。詳細については、「アラート ログの表示」を参照してください。

# 接続の監視

ほとんどの場合、デバイスは危険な状況が発生するとユーザに通知します。たとえば、ハード
ディスクがいっぱいになった場合やファンが停止した場合などです。ただし、場合によっては、アラートの送信前にデバイスがオフラインなることがあります。たとえば、スイッチまたはルータによってネットワークトラフィックが中断された場合やデバイスで電源障害が発生した場合などです。

これらの状況に対応するため、本製品はデバイスを定期的に確認して、ネットワーク上で使用可能かどうかを判断します。デバイスが ping に応答しない場合は、、または次回 [**マイ デバイス**]
リストを更新したときに、そのサーバのヘルス ステータスが [危険] に変わります。

ターゲット指定したデバイスまたは [**すべてのデバイス**] グループ内のすべてのデバイスに対して ping を実行するように、デバイス監視を設定する必要があります。

**デバイス モニタをセット アップするには**

1. [**マイ デバイス**]
   リストで、監視するデバイスを選択します。[**すべてのデバイス**]、公開グループ、または非公開グループからサーバを選択できます。
2. [**ターゲット**] をクリックします。
3. 下のペインで、[**アクション**] をクリックして、[**デバイス モニタ**] をクリックします。
4. 現在監視されているデバイスのリストを表示するには、[**監視デバイスの表示**] をクリックします。
5. ping スイープの間隔 (分) と、本製品がデバイスとの通信を試行する回数を入力します。

6. アクションを [ターゲット デバイス] リストにあるデバイスに対して実行するか、[**すべてのデバイス**] グループにあるすべてのデバイスに対して実行するかを選択します。
7. すべてのデバイスの監視を停止するには、[**デバイスを Ping しない**] を選択します。
8. [**適用**] をクリックします。

最後にターゲット指定したデバイスのグループだけが監視されます。たとえば、ターゲット デバイス A とデバイス B を選択してデバイス監視を適用した場合、コア サーバはデバイス A とデバイス B に対してのみ ping を実行します。次にデバイス C とデバイス D を選択してデバイス監視を適用した場合、デバイス C とデバイス D だけが監視され、デバイス A とデバイス B は監視されなくなります。

# アラートの設定

## アラートの使用方法

デバイス上で問題またはその他のイベントが発生すると（デバイスのディスク領域の不足など）、System Manager
はアラートを送信します。これらのアラートは、アラートを呼び出す重要度レベルまたはしきい値を設定することで、カスタマイズできます。アラートをコンソールに送信し、特定のアクションを実行するようにアラートを設定できます。この章では、アラートの機能について説明します。

- アラートの表示方法
- アラートを生成するデバイス上の問題の種類
- イベントの重要度レベルの設定
- カスタム アラート ルールセットの設定プロセス
- 例：ディスク容量上の問題に対するアラート ルールセットの設定

### アラートの表示方法

この製品では、次の方法によって問題やその他のコンピュータ イベントを通知します。

- ログへの情報の追加
- 電子メールによる通知またはポケットベル メッセージの送信
- コア サーバまたは個別デバイス上でのプログラムの実行
- ネットワーク上の SNMP 管理コンソールへの SNMP トラップの送信
- デバイスの再起動とシャットダウン

コンピュータ
グループに割り当てられた特定のアラートによって、同時に多数の応答が生成される場合があることに注意してください。たとえば、「コンピュータ構成の変更」のアラートを設定し、それを電子メール
アクションに関連付けるとします。このアラートが設定されたコンピュータにソフトウェア配布パッチが適用されると、コア
サーバから多数の電子メールが生成されます。その数は、パッチが適用されたコンピュータの台数に等しく、電子メール
サーバに処理が集中してサーバが停止する可能性があります。このような場合は、このアラートを電子メールで送信するのではなく、コア ログに書き込むことによって処理することもできます。

### アラートを生成するデバイス上の問題の種類

この製品には、アラートを生成する多数のイベントのリストが含まれています。イベントの中には、すぐに対処が必要な問題もあれば、必ずしも問題ではないがシステム管理者に有益な情報となる構成上の変更などもあります。（詳細については、「設定変更の監視」を参照してください。）アラートは、デバイスに必要なハードウェアが設定されている場合のみ生成されます。たとえば、センサ読み取り値から生成されるアラートは、デバイスに正しいセンサが搭載されている場合のみ適用します。

監視が必要なイベントの種類には次のようなものがあります。

- **ハードウェアの変更**：
  プロセッサ、メモリ、ドライブ、カードなどのコンポーネントが追加または削除されました。
- **アプリケーションが追加または削除された**：
  デバイスにアプリケーションがインストールまたはアンインストールされました。
- **サービス イベント**：デバイス上でサービスが開始または停止しました。
- **パフォーマンス**：ドライブ容量、利用可能メモリなどのパフォーマンスしきい値を超えました。
- **IPMI イベント**： コントローラ、センサ、ログの変更など、IPMI
  デバイスで検出可能なイベントが発生しました。
- **モデム用途**：システム モデムが使用されているか、モデムが追加または削除されました。
- **物理セキュリティ**：検知されたシャーシ侵入、パワー
  サイクル、その他の物理的変更が行われました。
- **パッケージのインストール**：ターゲット コンピュータ上にパッケージがインストールされました。
- **リモート コントロール アクティビティ**：開始、停止、失敗などのリモート コントロール セッション
  アクティビティが発生しました。

アラートを生成するハードウェア監視は、デバイスにインストールされているハードウェアの機能とハードウェアの正しい構成に依存します。たとえば、S.M.A.R.T. 監視機能を持つハード
ドライブがデバイスにインストールされているが、S.M.A.R.T. 検出がデバイスの BIOS
設定で有効になっていない場合、またはデバイスの BIOS が S.M.A.R.T.
ドライブをサポートしていない場合、アラートは S.M.A.R.T. ドライブ監視からは生成されません。

## イベントの重要度レベルの設定

デバイス上の問題またはイベントは、以下に示す重要度レベルのうちの一部またはすべてに関連付けることができます。

- **情報**：
  製造元がシステムに導入したサポート構成の変更やイベントなど。この重要度レベルはデバイスのヘルスには影響しません。
- **OK**：現状を維持しても差し支えないことを表します。
- **警告**：問題がクリティカル ポイントに達する前にその問題を事前に警告します。
- **危険**： 問題にすぐ対処する必要があることを表します。
- **不明**：アラート
  ステータスが判別できないか、または監視エージェントがデバイスにインストールされていません。

イベントまたはサーバ上の問題の性質によっては、重要度レベルが適用されなかったり、重要度レベルが含まれないものがあります。たとえば、侵入検知イベントの場合、デバイスのシャーシは開いているか、閉じています。デバイスのシャーシが開いていると、警告の重要度でアラート
アクションが呼び出されます。
ディスク容量や仮想メモリなどのその他のイベントには、OK、警告、危険の 3
つの重要度レベルがあります。

一部のアラートについて、アラートを呼び出す重要度レベルまたはしきい値を設定できます。たとえば、[警告] アラートまたは [危険]
アラートの結果として実行されるアクションとして、それぞれ異なる操作を選択できます。[不明]
ステータスは、ステータスが判断できないということを表しているのみであるため、アラート
トリガには選択できません。

## カスタム アラート ルールセットの設定プロセス

アラート ルールセットを設定して、個別デバイスまたはターゲット
デバイスのグループに導入できます。コア
サーバにアラートを送信するには、管理対象デバイスに製品の監視コンポーネントをインストールしておく必要があります。（詳細については、「エージェントの構成」を参照してください。）

監視コンポーネントを管理デバイスにインストールすると、既定のアラート
ルールセットが組み込まれ、とコンソールにヘルス
ステータスが表示されます。この既定ルールセットには次のようなアラートが含まれます。

- ディスクが追加または削除された
- ディスク領域
- メモリ使用量
- 温度、ファン、電圧
- パフォーマンス モニタ
- IPMI イベント（適用するハードウェア）

既定のルールセットに加えて、カスタム アラート ルールセットを設定して導入できます。カスタム アラート アクションを特定のイベントに応答するように組み込むことができます。たとえば、ファンが停止した場合に、アラートを呼び出してハードウェア サポート グループに電子メールを送信できます。

アラート ルールセットの作成と導入の全体的なプロセスは次のようになります。

1. ルールセットを導入するデバイスを選択し、[**ターゲット**] をクリックしてこのデバイスを [**ターゲット デバイス**] リストに追加します。
2. 使用するアラート アクション ルールセットを作成します。これらのアクション
   ルールセットは、アラートがトリガするアクションの種類を定義します。（詳細については、「アラート アクションの設定」を参照してください。）
3. カスタム アラート
   ルールセットを作成します。こうすると、あらかじめ定義したアクションを選択することができます。（詳細については、「アラート ルールセットの設定」を参照してください。）
4. そのルールセットをターゲット デバイスに導入します。ルールセットを導入する前にターゲット
   デバイスを追加できます。（詳細については、「ルールセットの導入」を参照してください。）

次は、このプロセスの簡単な例です。

## 例：ディスク容量上の問題に対するアラート ルールセットの設定

1. 左側のナビゲーション ペインで、[**マイ デバイス**] をクリックして、[**すべてのデバイス**] グループをクリックします。
2. アラートを設定するデバイスを選択し、[**ターゲット**] をクリックしてこのデバイスを [**ターゲット デバイス**] リストに追加します。
3. [**アラート**] をクリックして、[**アクション ルールセット**] タブをクリックします。
4. [**アクション**] ドロップダウン リストで、構成するアクションを選択します（**電子メール/ページの送信**など）。[**新規**] をクリックし、[**名前**] フィールドに名前を入力して [OK] をクリックします。
5. [**アクション ルールセット**] ページに戻り、名前を付けたルールセットを選択して [**アクションの編集**] をクリックします。テキスト ボックスに必要に応じてデータを指定します。終了したら、[**保存**] をクリックします。
6. [**アラート ルールセット**] タブをクリックします。
7. [**新規**] をクリックし、[**名前**] フィールドに「ディスク容量の問題」などと入力し、[**説明**] フィールドに説明を入力して [**OK**] をクリックします。
8. 名前を付けたルールセットをクリックし、[**ルールセットの編集**] をクリックします。
9. [**新規**] ボタンをクリックします。
10. [**アラート タイプ**] ドロップダウン リストから [**ディスク領域**] をクリックします。
11. アラートを出すステータス :[**OK**]、[**警告**]、[**危険**] を確認します。（複数のステータスに同じアクションを設定する場合は、複数のステータスを選択します。各ステータスに異なるアクションを設定する場合は、ステータス レベルごとに異なるアクションがトリガされるように、各ステータスに別々の構成を作成します。）
12. [**アクション**] ドロップダウン リストから、手順 6 と 7 で指定した条件が満たされたときに実行するアクションを選択します。設定するアクションがリストにない場合は、[**アクション ルールセット**] ページでアクションを作成できます。（アラート アクション ルールセットを事前に作成していない場合は、リストには表示されません。）
13. [**アラート アクション**] ドロップダウン リストから、使用する構成を選択します。
14. またはコンソールの [**すべてのデバイス**] リストに表示されるサーバのヘルス ステータスにアラートを適用する場合は、[**デバイスのヘルスに影響**] を選択します。アラートの重要度レベルが [**情報**] のみの場合、アラートはデバイスのヘルスには影響しません。
15. [追加] をクリックします。
16. 手順 6 ～ 12 を繰り返してルールセットにアラートを追加します。
17. 終了したら、[**閉じる**] をクリックします。
18. ルールセット内の任意のアラート タイプを変更する場合、アラート タイプを選択して [**編集**] をクリックします。そしてタイプを変更したら、[**更新**] をクリックして [**閉じる**] をクリックします。
19. アラート ルールセットを定義したら、そのルールセットをターゲット デバイスに適用します。[**ルールセットの導入**] をクリックし、ルールセットを選択して [**導入**] をクリックします。

# アラート アクションの設定

[**アクション ルールセット**]
ページを使用して、アクションが選択されたときの動作に関する追加情報を設定します。しきい値を超えるとアラートが生成されます。アラートには、電子メールの送信などのアクションを関連付けることができます。各アクションには固有の構成があるので、アクションは個別に設定する必要があります。

**アクション ルールセットを作成するには**

1. 左側のナビゲーション ペインで、[**アラート**] をクリックして、[**アクション ルールセット**] タブをクリックします。
2. [**アクション**] ドロップダウン リストで、構成するアクションを選択します。アクションごとに、固有の構成のリストがあります。
3. [**新規**] をクリックし、[**名前**] フィールドに名前を入力して [**OK**] をクリックします。
4. [**アクション ルールセット**] ページに戻り、名前を付けたルールセットを選択して [**アクションの編集**] をクリックします。
5. [**プログラムをコアで実行**] または [**クライアントでのプログラム実行**] を選択した場合は、アラートに対して実行するプログラムへのパスを入力するか貼り付けて [**保存**] をクリックします。いずれかの**プログラム実行**アクションを選択した場合、デスクトップに予期したようにプログラムが表示されないことがあることに注意してください。プログラムが実行されるときに、そのプログラムは Windows のサービスとして起動されるので、普通のアプリケーションのように表示されません。このような方式で実行されるプログラムは、ユーザの操作が必要なユーザ インターフェイスを含まないものである必要があります。プログラムが実行しているかを確実に判断するには、Windows タスク マネージャのプロセスをチェックします。

   [**電子メール/ページを送信**] を選択した場合は、[**宛先**] フィールドに電子メールの受信者の電子メール アドレスを、[**送信者**] フィールドに有効な電子メール アドレスを、[**件名**] フィールドに件名を、[**本文**] フィールドにメッセージを入力し、メッセージの送信日時を選択して、[**SMTP サーバ**] フィールドに SMTP サーバの場所を入力します。メッセージを複数の受信者に送信する方法およびメッセージで変数を使用する方法については、[**ヘルプ**] ボックスをクリックしてください。終了したら、[**保存**] をクリックします。

   [**SNMP トラップの送信**] を選択した場合は、ホスト名を入力し、バージョンを選択して、[**コミュニティ文字列**] ボックスにコミュニティ文字列を入力します。次に [**保存**] をクリックします。

**注意**

- コンピュータ
  グループに割り当てられた特定のアラートによって、同時に多数の応答が生成される場合があります。たとえば、「コンピュータ構成の変更」のアラートを設定し、それを電子メール
  アクションに関連付けるとします。このアラートが設定されたコンピュータにソフトウェア配布パッチが適用されると、コア
  サーバから多数の電子メールが生成されます。その数は、パッチが適用されたコンピュータの台数に等しく、電子メール
  サーバに処理が集中してサーバが停止する可能性があります。このような場合は、このアラートを電子メールで送信するのではなく、コア ログに書き込むことによって処理することもできます。
- アラート
  アクションの中には、デバイスのヘルスに影響を与えないものもあります。たとえば、クライアント上でのプログラムの実行、シャットダウン/再起動、情報を伝えるだけのアラートなどがあります。ただし、これらのアクションが、デバイスのヘルスに影響を与える他のアラート
  アクションと組み合わされた場合、生成されたアラートはデバイス ヘルスに影響を与え、アラート ログに記録されます。
- SMTP アラートが正常に作動するためには、電子メールの [**送信者**] フィールドに有効な電子メール アドレスを入力する必要があります。
- バージョン 1 と識別された SNMP トラップは処理され、バージョン 3 と識別されたものはそのまま転送されます。
- SNMP トラップには、重要度レベルがトラップの [特定のトラップ タイプ] フィールドに報告されます。値は、「1」が不明、「2」が情報、「3」が OK、「4」が警告、「5」が危険です。

# アラート ルール セットの設定

[**アラート ルールセット**] ページでは、新しいアラート ルールセットを作成します。アラートを構成する前に、アラート アクションを構成する必要があります。(詳細については、「アラート アクションの設定」を参照してください。)

[**アラート ルールセット**] ページには、既定で 2 つのルールセットが表示されます。

- **コア アラート ルールセット** :
  このルールセットは、**デバイス監視**機能が有効になっている場合にアラートがコア サーバに送信されるようにします (「接続の監視」を参照)。このルールセットには、デバイス監視、AMT 回路ブレーカ アラート、および SOL (Serial Over LAN) セッションなどのアラート タイプを含む、あらかじめ定義されたアラート タイプのグループによって構成されています。コア アラート タイプのステータス、アクション、アラート アクション、およびヘルス設定は編集可能ですが、その他の変更を試みた場合は無視されます。

- **既定ルールセット**：
  このルールセットはすべての管理デバイスに導入され、大部分のネットワーク管理者にとって共通な複数のアラート タイプを含みます。このルールセットには、他のアラート
  タイプを追加したり、既定アラート
  タイプの設定を変更するなどの編集が可能です。このルールセットを編集すると、はっきりとルールセットの再導入を指定しなくてもすべての管理デバイスに変更内容が導入されます。

これらのルールセットに加えて、管理デバイスのターゲット グループに適用するためにカスタム ルールセットを作成することができます。このようなルールセットは、[**エージェントの構成**] に表示するために .XML 形式で生成する必要があります。

---

デバイス用のカスタム
ルールセットを作成するときには、デバイスに既定のルールセットが導入済みであると、アラート
ルールに重複または衝突が生じる可能性があることに留意してください。管理デバイスの構成時に既定のルールセットを導入してからカスタム
ルールセットを導入すると、両方のルールセットがそのデバイス上で実行されます。たとえば、両方のルールセットが同じアラート
タイプに対してアラートを生成して、異なるアクションをとった場合、結果としてアラート
アクションの重複が起こったり、予想外のアラート
アクションが発生したりすることがあります。いったん導入した後で既定のルールセットを削除することはできませんが、既定のルールセットの一部を変更したい場合は編集できます。

---

**アラート ルールセットを作成するには**

1. 左側のナビゲーション ペインで、[**アラート**] をクリックし、[**アラート ルールセット**] タブをクリックします (必要に応じて)。
2. [**新規**] をクリックし、[**名前**] フィールドに名前を、[**説明**] フィールドにアラートの説明を入力して [**OK**] をクリックします。
3. 名前を付けたルールセットをクリックし、[**ルールセットの編集**] をクリックします。
4. [**新規**] をクリックします。
5. [**アラート タイプ**] ドロップダウン
   リストから、アラートを受け取るコンポーネント、アクション、またはイベントのタイプを選択します。
6. アラートを出すそれぞれのステータス[**情報**]、[**OK**]、[**警告**]、[**危険**] をオンにします。たとえば、手順 5
   で選択したタイプが危険なしきい値を超えた場合にアラートを受け取るには、[**危険**] を選択します。

7. [**アクション**] ドロップダウン リストから、手順 5 と 6
   で指定した条件が満たされたときに実行するアクションを選択します。これらのアクションはあらかじめ定義しておきます。リストにないアクションが必要な場合は、[**アクション ルールセット**] ページでアクションを作成できます。

   **注意**：コンピュータ
   グループに割り当てられた特定のアラートによって、同時に多数の応答が生成される場合があります。たとえば、「コンピュータ構成の変更」アラートを設定し、それを電子メール
   アクションに関連付けるとします。このアラートが設定されたコンピュータにソフトウェア配布パッチが適用されると、コア
   サーバから多数の電子メールが生成されます。その数は、パッチが適用されたコンピュータの台数に等しく、電子メール
   サーバに処理が集中してサーバが停止する可能性があります。このような場合は、このアラートを電子メールで送信するのではなく、コア ログに書き込むことによって処理することもできます。

8. [**アラート アクション**] ドロップダウン リストで、構成をクリックします。使用可能な構成が 1 つしかない場合もあります (このリストの内容は、手順 7
   で選択したアクションによって異なります)。
9. またはコンソールの [**すべてのデバイス**] リストに表示されるサーバのヘルス
   ステータスにアラートを適用する場合は、[**デバイスのヘルスに影響**]
   を選択します。アラートの重要度レベルが [**情報**]
   のみの場合、アラートはデバイスのヘルスには影響しません。
10. [追加] をクリックします。
11. 手順 5 ～ 10 を繰り返してルール セットにアラートを追加します。
12. 終了したら、[**閉じる**] をクリックします。

アラート ルールセットを編集するには、ルールセットを選択し (手順 3 を参照)、[**ルールセットの編集**] をクリックして、上の手順を続行します。

ルールセットを作成または編集してから数分後に、ルールセット導入サービスによって、そのルールセットが既に導入されているすべてのコンピュータにおいて、自動的に更新が試行されます。あるいは、そのルールセットを即時に導入する場合は、[**ルールセットの導入**] タブをクリックして [**導入**] をクリックします。

# ルールセットの導入

[**ルールセットの導入**] ページを使用して、選択したアラートをターゲット デバイスに移動します。

ルールセットを管理デバイスに導入するには、まず管理エージェントをそのデバイスにインストールする必要があります。標準の管理エージェントを導入する場合は、既定のルールセットを導入します。エージェントのセットアップの終了後、新しいルールセットを更新または導入できます。まず、アラート ルールセットの導入先となるデバイスをターゲットに指定します。

**アラート ルールセットを導入するには**

1. 左側のナビゲーション ペインで、[**マイ デバイス**] をクリックして、[**すべてのデバイス**] グループをクリックします。
2. アラート ルールセットを導入するデバイスを選択し、[**ターゲット**] をクリックしてこのデバイスを [**ターゲット デバイス**] リストに追加します。
3. 左側のナビゲーション ペインで、[**アラート**] をクリックして、[**ルールセットの導入**] タブをクリックします。
4. [**アラート ルールセット**] ボックスで、導入するルールセットを選択します。
5. リンクをクリックしてターゲット デバイスのリストを表示します。このリストからデバイスを削除するには、サーバを右クリックして [**削除**] をクリックします。すべてのデバイスを削除するには、デバイス名のいずれかを右クリックして [.**リセット**] をクリックします。デバイスを追加するには、ターゲット デバイスのリスト (上記の手順 1 ～ 2) にそのデバイスを追加する必要があります。
6. [**ターゲット リスト**] ウィンドウを閉じ、[**導入**] をクリックして選択した構成をターゲット デバイスに導入します。

導入プロセスの一部として、導入されるルールセットとルールセットが導入されるデバイスのリストが XML ページとして作成されます。このレポートはコア サーバの ¥ldlogon¥alertrules ディレクトリに保存され、データベースに割り当てられている連番を使った名前が付きます。ルールセットの導入を行わずにこの XML ページだけを表示する場合は、[**XML の生成**] ボタンをクリックし、リンクをクリックして XML ファイルを表示します。

いかなる場合であっても、1 つの管理デバイスには 1 つのカスタム ルールセットのみが有効です。カスタム ルールセットを導入したデバイスに対して、2 つ目のルールセットを導入すると、最初のルールセットが 2 つ目のルールセットに上書きされます。

# デバイスのアラート ルールセットの表示

[**アラート ルールセット**] ページを使用して、選択したデバイスに割り当てられたアラート ルールセットのリストを表示したり、各アラートの詳細を表示します。

**アラート ルールセットを表示するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。新しいブラウザ ウィンドウにサーバ情報コンソールが開きます。
2. 左側のナビゲーション ペインで、[**ルールセット**] をクリックします。
3. [**アラート ルールセット**] タブをクリックします。

各ルールセットについて、次のような詳細が提供されています。これらの詳細の変更については、「アラートの使用方法」を参照してください。

- **状態変化** : アラートの状態が表示された状態に達すると、アラートが生成されます。

- **健全性に影響** :アラート
  ステータスがに表示されたときにサーバのヘルス状態に適用されるか、または
  [**すべてのデバイス**] リストに表示されたときに適用されるかを示します。
- **ルールセット名** : [アラート ルールセット] ダイアログで定義された、アラート
  ルールセットの名前。
- **アラート タイプ** : アラートの原因 (ハードウェア、ソフトウェア、イベントなど) の説明です。
- **アクションの構成** :[アクションの構成]
  ダイアログで定義されている、アラート生成時に発生するアクションです。
- **アラート ハンドラ** : 電子メール、SNMP
  トラップ、プログラムの実行など、生成されるアラートの種類。
- **インスタンス** : アラートのソースを表します。

また、[**アラート ログ**] ボタンをクリックして、デバイスのアラート
ログにアクセスしてログの詳細を表示できます。(詳細については、「アラート
ログの表示」を参照してください。)

# アラート ログの表示

[**アラート ログ**] ページでは、コア サーバに送信されたアラート (グローバル アラート ログ)
または管理デバイスに送信されたアラートを表示できます。ログは時刻順 (GMT)
に並べ替えられ、最新のアラートが一番上に表示されます。

アラート ログは次の列で構成されています。

- **アラート名** : [**アラートの構成**] ページで定義された、アラートに関連付けられている名前。
- **時刻** : アラートが生成された日時 (GMT)。
- **ステータス** : アラートのステータス。以下のいずれかが表示されます。
  - **不明** : ステータスを判断できません。
  - **情報** : 製造元がシステムに導入したサポート構成の変更やイベントなど。
  - **OK** : 現状を維持しても差し支えないことを表します。
  - **警告** : 問題がクリティカル ポイントに達する前にその問題を事前に警告します。
  - **危険** : 問題にすぐ対処する必要があることを表します。
- **インスタンス** : アラートのソースを表します。
- **デバイス名** :
  アラートが生成されたデバイスの名前。完全修飾ドメイン名である必要があります。(グローバル
  アラート ログのみ。)
- **IP アドレス** : アラートが生成されたデバイスの IP アドレス。(グローバル アラート ログのみ。)

---

デバイス名が完全修飾ドメイン名のように表示されない場合には、この製品がそのデバイスの完全修飾ドメイン名を解決できないことによります。

---

**グローバル アラート ログを表示するには**

1. 左側のナビゲーション ペインで、[**ログ**] をクリックします。

2. エントリを時間、名前、ステータス、またはインスタンス別に並べ替えるには、その列の見出しをクリックします。
3. 詳細なアラートの説明を表示するには、[**アラート名**] 列にあるエントリをダブルクリックします。.
4. ログ エントリを名前、ステータス、またはインスタンス別にリストするには、[フィルタ] ドロップダウン リストにあるフィルタ条件を選択します。たとえば、[**アラート名**] を選択して完全な名前 (Performance など) または * ワイルドカードを使って名前の一部 (Remote* など) を入力します。日付で検索するには、[**日付フィルタリングを有効にする**] を選択し、検索範囲の開始日および終了日を入力して [**検索**] をクリックします。
5. アラートのヘルス ステータスをクリアするには、[**アラート名**] 列の番号をクリックしてアラートを選択し、[**アラートをクリア**] をクリックして [**OK**] をクリックします。ログ エントリを削除するには、そのアラートを選択して [**エントリの削除**] をクリックします。
6. ログのすべてのエントリを削除するには、[**ログの消去**] をクリックします。

**特定のデバイスのアラート ログを表示するには**

1. [**マイ デバイス**] リストでデバイスをダブルクリックします。
2. 左側のナビゲーション ペインで、[**システム情報**] をクリックします。
3. [**ログ**] をクリックし、[**アラート ログ**] をダブルクリックします。
4. エントリを時間、名前、ステータス、またはインスタンス別に並べ替えるには、その列の見出しをクリックします。
5. 詳細なアラートの説明を表示するには、[**アラート名**] 列にあるエントリをクリックします。.
6. ログ エントリを名前、ステータス、またはインスタンス別にリストするには、ツールバーの [**フィルタ**] ボタンをクリックしてフィルタ条件を選択します。たとえば、[**アラート名**] を選択して完全な名前 (Performance など) または * ワイルドカードを使って名前の一部 (Remote* など) を入力します。選択したフィルタ オプションに関連付けられたアラートを表示するには、ツールバーの [検索] をクリックします。
7. 日付の範囲を指定してログ エントリを表示するには、[**すべての日付のイベントを表示**] チェックボックスの選択を解除して日付の範囲を選択します。[**更新**] をクリックしてその日付範囲の項目を表示します。

# ソフトウェア更新

System Manager には、管理ソフトウェア、オペレーティング システム ソフトウェア、およびデバイス ドライバの更新を検索できるソフトウェア更新ツールが含まれています。このような種類の更新をダウンロードし、適切な更新を導入およびインストールすることによって、影響を受けるデバイスを修正することができます (パッチとも呼ばれます)。

この章では次の内容について説明します。



## ソフトウェア更新の概要

ソフトウェア更新ツールにより、ネットワーク全体の管理デバイス上のソフトウェアを最新に維持できます。適切な更新ファイルのダウンロードおよび影響を受けるデバイスへの必要な更新の導入とインストールを行って、ソフトウェアを最新状態に維持するための繰り返し処理を自動化できます。

本製品は標準の役割ベース管理を使って、ユーザがソフトウェア更新ツールへアクセスできるようにします。役割ベース管理は、製品のアクセスおよびセキュリティ規準であり、管理者は、それに従ってツールやデバイスのアクセス制限を実行します。各ユーザには、どの機能が使用でき、どのデバイスを管理できるかを定義づける個別の権限とスコープが与えられます。管理者は、このような権限他のをユーザに割り当てます
(詳細については「役割ベース管理」を参照)。ソフトウェア更新ツールを使用するには、パッチ管理、基本 Web コンソール、およびレポート権限を持つユーザとしてログインする必要があります。

## サポートされているサーバ プラットフォーム

ソフトウェア更新では、標準のサーバ
プラットフォームのほとんどをサポートしており、次のオペレーティング
システムが稼動する管理サーバで更新をスキャンし、その更新を導入できます。

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4

- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional、Enterprise、Advanced)

## ソフトウェア更新ウィンドウについて

パッチ管理権限がある場合は、コンソールの左側のナビゲーション
ペインに**ソフトウェア更新**ツールが表示されます。**[ソフトウェア更新]**
をクリックすると、ウィンドウの右側にツールバーが 1 つと 2
つのペインが表示されます。左ペインには、ソフトウェア更新グループが階層型のツリー
ビューで表示されます。グループをクリックすると、右ペインにその内容が表示されます。右ペインでは、ソフトウェア更新定義の詳細が列リストに表示されます。一番上には、条件を指定してすばやく検索を行える**[検索]** ボタンがあります。**[検索]** ボックスでは、次の拡張文字はサポートされていません。<, >, ', ", !.

## ツール バー ボタン

- **更新 :[脆弱性設定の更新]**
  ダイアログを開きます。ソフトウェア更新情報を更新するプラットフォームおよび言語を指定できます。また、
  **[スキャン]**グループに更新を配置するかどうか、対応するパッチを同時にダウンロードするかどうか、パッチのダウンロード場所、およびプロキシ サーバ設定も指定できます。
- **ダウンロードのスケジュール :[スケジュールされているタスク]** ダイアログを開いてダウンロード
  タスクを表示します。このダイアログでタスク
  オプションを設定できます。**[保存]**をクリックすると、ダウンロード タスクが
  **[スケジュールされているタスク]** ウィンドウの **[脆弱性タスク]**タブに追加されます。
- **パッチ タスクをスケジュールする :[脆弱性スキャンのスケジュール]**
  ダイアログを開きます。タスク名を指定したりスキャナ オプションを設定したりできます。
- **表示されているすべての情報の更新**
  :右ペインのリストを、ダウンロードされた最新の更新情報で更新します。
- **削除 :[セキュリティとパッチ定義の消去]**ダイアログを開きます。コア
  データベースから脆弱性情報を削除するプラットフォームおよび言語を指定できます。

## 左側のペイン (ツリー ビュー)

[脆弱性スキャン] ウィンドウの左ペインには次のグループが表示されます。

- **スキャン**
  :管理デバイスでソフトウェア更新ツールを実行するときに検索されるすべての更新がリストされます。つまり、このグループに更新が含まれている場合は、次回のスキャン操作の要素になります。含まれていない場合は、次回のスキャンの要素になりません。

  [スキャン] は、[スキャンしない] および [未割り当て] とともに、3 種類の脆弱性状態の 1 つと見なされます。したがって、1 つのソフトウェア更新は 3 種類のグループの 1 つにのみ存在可能です。更新は、固有のアイコン([未割り当て] は ?のアイコン、[スキャンしない] は赤い X のアイコン、[スキャン]は通常の脆弱性アイコン)として認識されます。更新をあるグループから別のグループへ移動させると、自動的に状態が変更されます。

  あるグループから別のグループにソフトウェア更新を移動するには、その更新を右クリックし、移動先のグループを選択します。

  [スキャン]
  グループに更新を移動すると、次回のソフトウェア更新スキャンの特定の性質およびサイズを制御できます。

  **[脆弱性設定の更新]** ダイアログの **[新しい定義を [スキャン] グループに入れる]** オプションをオンにすると、更新時に新しい更新を [スキャン] グループに自動的に追加できます。

  **[スキャン] グループからソフトウェア更新を移動する場合の注意ソフトウェア更新** を [スキャン] グループから [スキャンしない] グループに移動すると、どのスキャン済みデバイスにこれらの更新が検出されたかに関するコアデータベース内の現在の情報が削除され、[ソフトウェア更新プロパティ] ダイアログおよびスキャン済みサーバの [サーバ情報] ダイアログのどちらからも参照できなくなります。削除した評価情報を復元するには、[スキャン] グループにそのソフトウェア更新を戻し、スキャンを再度実行します。

- **スキャンしない**
  :スキャナをデバイスで次回実行するときに検索されないソフトウェア更新がリストされます。既に説明したとおり、このグループ内の更新は、[スキャン] または [未割り当て] グループに含まれることはありません。更新をこのグループに移動すると、その更新をソフトウェア更新スキャンから一時的に削除できます。

- **検出** :スキャン ジョブに含まれているすべてのターゲット
  デバイスについて、前回のソフトウェア更新スキャンで検出されたソフトウェア更新がすべてリストされます。このグループの内容は、スキャンされたデバイスの数にかかわらず、前回のソフトウェア更新スキャンによって決定されます。

  [検出]
  リストは、前回のスキャンで検出されたすべてのソフトウェア更新から構成されます。[スキャン済み] 列と [検出]
  列は、スキャンされたデバイス数、およびソフトウェア更新が検出されたデバイス数を示すのに便利です。どのサーバで更新が検出されたかを確認するには、その定義を右クリックし、**[影響を受けるコンピュータを表示]** を選択します。特定のサーバの更新情報は、そのサーバの
  [サーバ情報コンソール] ダイアログでも確認できます。

  ソフトウェア更新は、[検出] グループから [未割り当て] または [スキャンしない]
  のいずれかのグループだけに移動できます。

- **未割り当て** :[スキャン] グループまたは [スキャンしない]
  グループのどちらにも属さないすべてのソフトウェア更新が一覧表示されます。基本的に、[未割り当て]
  グループは、収集された更新をスキャンするかどうかを決定するまで、それらのソフトウェア更新を待機させる領域です。

  既定では、収集されたソフトウェア更新は更新時に [スキャン] グループに追加されます。

  ソフトウェア更新は、[未割り当て] グループから [スキャン] または [スキャンしない]
  のいずれかのグループに移動できます。

- **OS 別で表示** :ダウンロードされたすべてのソフトウェア更新が、特定のデバイス
  オペレーティング
  システムのサブグループに整理されてリストされます。これらのサブグループは、OS
  カテゴリ別に更新情報を識別する際に役立ちます。これらの OS サブグループを使用して、OS 固有のスキャンのために一連のソフトウェア更新を [スキャン] グループにコピーできます。

  ソフトウェア更新は、[OS] グループから [スキャン]、[スキャンしない]、または [未割り当て]
  グループにコピーできます。また、更新は複数のプラットフォームや製品グループに同時に存在できます。

- **製品別で表示**
  :ダウンロードされたすべてのソフトウェア更新が、特定の製品サブグループに整理されてリストされます。これらのサブグループは、製品カテゴリ別に更新情報を識別する際に役立ちます。これらの製品サブグループを使用して、製品固有のスキャンのために更新を [スキャン]
  グループにコピーできます。

## 右側のペイン (リスト ビュー)

ウィンドウの左ペインでは、ソート可能な列に次のソフトウェア更新の詳細が表示されます。

- **ID** :ベンダ定義の固有の英数字コードで更新を識別します。
- **重要度**
  :更新の重要度レベルを示します。重要度には、[サービスパック]、[重要]、[高]、[中]、[低]、[該当なし]、[不明] があります。
- **タイトル** :更新の性質またはターゲットを簡単なテキスト文字列で説明します。
- **言語** :更新の影響を受ける OS の言語を示します。
- **公開日** :ベンダによって更新が公開された日付を示します。
- **サイレント インストール** :更新に対応するパッチ
  ファイルを、ユーザの介入なしに自動的にインストールするかどうかを示します。一部の更新には複数のパッチがあります。更新のパッチのうち自動的にインストールしないものがある場合は、[サイレント インストール] 属性を [いいえ] にします。
- **修復可能** :更新がパッチ
  ファイルの配布やインストールによって修復可能かどうかを示します。利用できる値は、次のとおりです。[はい]、[いいえ]、[一部
  (複数の検出ルールを含む更新については、検出されたすべての更新が修復可能とは限らない)]
  。

更新 ID をダブルクリックすると、そのプロパティ
ダイアログに詳細な情報が表示されます。[ソフトウェア更新プロパティ]
ダイアログから、更新の検出ルールを確認したり、対応するパッチ
ファイルをダウンロードしたり、ルールをクリックすることによってその詳細プロパティ
ダイアログを表示したりできます。

## ソフトウェア更新スキャンのためのデバイスの設定

管理デバイスで脆弱性をスキャンしてパッチ導入を受信するには、ソフトウェア更新エージェントをインストールしておく必要があります。

ソフトウェア更新エージェントを複数の管理デバイスに導入する最も簡単な方法は、ソフトウェア更新エージェントを選択して (既定の設定) 新しいエージェント構成を作成し、**[スケジュールされているタスク]** を使用して目的のターゲット デバイスの設定をスケジュールすることです。

ソフトウェア更新をサポートするようにデバイスを構成すると、ソフトウェア更新スキャンおよび修正
(つまり、パッチ導入とインストール) に必要なファイルがターゲット デバイスにインストールされます。

## ソフトウェア更新定義の更新

ネットワークは、ソフトウェア更新やバグ修正のような通常のメンテナンスの問題を常に抱えています。ソフトウェア更新ツールでは、LANDesk
でホストされているデータベースを介してソフトウェアを更新することによって、最新の既知のパッチ情報をすばやく簡単に収集できます。このサービスは、信頼されている業界およびベンダ
ソースからの既知の更新を統合します。

最新のパッチ情報を確立して管理すると、サポートするサーバ オペレーティング
システムごとに必要なソフトウェア更新の性質と程度をより理解することができます。最初のステップは
最新の既知の更新情報を更新することです。

即座にソフトウェア更新を設定して実行したり、指定した時刻に実行するかまたは再帰タスクとして実行
するスケジュールされた更新タスクを作成できます。

**ソフトウェア更新情報を更新するには**

1. 左側のナビゲーション ペインで、**[ソフトウェア更新]**
   をクリックします。ダイアログの詳細については、「[ソフトウェア更新]
   ウィンドウについて」を参照してください)。
2. **[更新]**ツール バー ボタンをクリックします。
3. 有効なコンテンツ サーバのリストからダウンロード場所を選択します。
4. ソフトウェア更新情報を更新するプラットフォームを選択します。リストから 1
   つ以上のプラットフォームを選択できます。選択したプラットフォームが多いほど、更新には時間
   がかかります。
5. ステップ 3
   で選択したプラットフォームについて、ソフトウェア更新情報を更新する言語を選択します。リスト
   から 1 つ以上の言語を選択できます。選択した言語が多いほど、更新には時間がかかります。
6. 既定の場所 ([スキャン] グループ) ではなく、[未割り当て]
   グループに新しいソフトウェア更新の定義 (データベースに存在しない更新)
   を自動的に配置するには、**[新しい定義を [スキャン] グループに入れる]**チェック
   ボックスの選択を解除します。
   - 実際のパッチ実行可能ファイルを自動的にダウンロードするには、**[上記で選択した定義
     のパッチをダウンロード]**チェック ボックスをオンにし、次のいずれかのダウンロード
     オプションをクリックします。
     **検出された定義のみが対象**
     :直前のソフトウェア更新スキャンで検出されたソフトウェア更新 (つまり、[検出]
     グループ内に現在ある更新) に対応するパッチだけをダウンロードします。
   - **参照されるすべての定義が対象** :[スキャン]
     グループ内に現在あるソフトウェア更新に対応するすべてのパッチをダウンロードします。
     この操作には時間がかかります。

パッチは、[脆弱性設定の更新] ダイアログの [パッチの設定]
セクションで指定した場所にダウンロードされます。次の「パッチのダウンロード場所を設定するには」の
手順を参照してください。

8. ネットワーク上に外部インターネット転送に使用されるプロキシ サーバ
   (ソフトウェア更新情報の更新およびパッチのダウンロードに必要) がある場合は、**[プロキシ設定]**
   タブをクリックし、**[プロキシ サーバを使用]**
   ボックスを選択します。サーバのアドレス、ポート番号、およびプロキシ
   サーバへのアクセスにログインが必要な場合は認証資格情報を指定します。
9. **[適用]**をクリックして、設定を保存します。
10. **[今すぐ更新]**をクリックしてソフトウェア更新を実行します。**[セキュリティおよびパッチ定義の更新]**
    ダイアログに、現在の操作とステータスが表示されます。

11. 更新が完了したら、**[閉じる]**をクリックします。更新が終了する前に **[キャンセル]**をクリックすると、その時点までに処理されたソフトウェア更新情報だけがコア データベースにダウンロードされます。残りの情報をすべて取得するには、更新を再実行する必要があります。

---

**注意**
:更新処理中にコンソールを閉じないでください。コンソールを閉じると、処理が中止されます。これは、スケジュールされたダウンロード タスクには該当しません。

---

同一コア サーバにSystem Manager と LANDesk® Management Suite がインストールされている場合、両方の製品は同じ設定を使ってどのタイプの脆弱性が更新されるか判断します。場合によっては、更新の実行中に System Manager から設定可能な更新のみを Management Suite で表示されることがあります。たとえば、Management Suite で更新オプションとしてセキュリティ侵害を選択して、System Manager でソフトウェア更新の更新を選択した場合、System Manager で更新を実行する時に更新された項目の中にソフトウェア更新とセキュリティ侵害の両方が表示されます。

**パッチのダウンロード場所を設定するには**

1. **[脆弱性設定の更新]** ダイアログの **[パッチ設定]** タブをクリックします。
2. パッチ ファイルのコピー先の UNC パスを入力します。既定の場所はコア サーバの ¥LDLogon¥Patch ディレクトリです。
3. ステップ 2 で入力した UNC パスがコア サーバ以外の場所である場合は、その場所の認証に有効なユーザ名とパスワードを入力します。

   このフォルダではファイルと Web の共有が有効になっていて、匿名アクセスも有効になっている必要があります。

4. サーバがダウンロードしたパッチを導入するためにアクセスできる Web URL を入力します。Web URL は、ステップ 2 で入力した UNC パスと一致している必要があります。
5. **[テストの設定]** をクリックすると、ステップ 4 で指定した Web アドレスに接続できたかどうかを確認できます。
6. UNC パス および Web URL を既定の場所に戻すには、**[パッチの設定のリセット]**をクリックします。既定の場所はコア サーバの ¥LDLogon¥Patch ディレクトリです。

## ソフトウェア更新ダウンロードのスケジュール設定

将来の指定した時刻に自動的に実行するか、または反復タスクとして実行するように、ソフトウェア更新をスケジュールされているタスクとして設定することもできます。この操作を行うには、**[ダウンロードのスケジュール]** ツール バー ボタンをクリックし、**スケジュールされているタスクのプロパティ** ダイアログでタスク名を指定してタスク オプションを設定します。**[保存]** をクリックすると、[スケジュールされているタスク] ウィンドウにタスクが表示されます。

スケジュールされている、ソフトウェアのすべての更新タスクでは、**[脆弱性設定の更新]**
ダイアログの現在の設定が使用されます。特定の更新ジョブの場所、プラットフォーム、言語、パッチ
ダウンロード サイト、またはプロキシ
サーバを変更する場合は、タスクのスケジュールが実行される前に、**[脆弱性設定の更新]**ダイアログで
それらの設定を変更する必要があります。

**ダウンロードのスケジュール タスクを設定するには**

1. 左側のナビゲーション ペインで、**[ソフトウェア更新]**をクリックします。
2. **[ダウンロードのスケジュール]**をクリックします。
3. **[スケジュールされているタスク]**ページで、スケジュールを構成します。
4. **[保存]**をクリックします。

**[ダウンロードのスケジュール]**をクリックすると、タスクが作成されます (ターゲット
デバイスはなく、スケジュールもされていません)。**[タスクのスケジュール]**手順をキャンセルする場合、そ
のタスクが既に作成されていて、**[マイ タスク]**リストにも表示されていることに注意してください。

## ソフトウェア更新および検出ルール情報の表示

LANDesk セキュリティ
サービスからの最新の情報を使用してソフトウェア更新情報を更新したら、コンソールにソフトウェア更新
リストを表示したり、プラットフォームや製品別にソフトウェア更新を表示したり、更新をさまざまなステー
タス
グループに移動したりできます。ウィンドウのさまざまなグループおよびそれらの使用方法の詳細につい
ては、この章で前述している「[ソフトウェア更新] ウィンドウについて」を参照してください。

ソフトウェア更新の詳細を表示するには、[ソフトウェア更新 ID] をダブルクリックして [プロパティ]
ダイアログを開きます。このダイアログの [検出ルール] リストでパッチ ファイル名をダブルクリックして
**[パッチのプロパティ]**ダイアログを開くと、検出ルールの詳細を表示できます (「[パッチのプロパティ]
ダイアログについて」を参照してください)。

この情報は、ネットワークでサポートしているサーバ
プラットフォームにどの更新が関連するか、更新の有無は検出ルールごとにどのようにチェックされるか
、入手可能なパッチはどれか、および影響を受けるデバイスにどのように修正を設定して実行するかを
決定する際に役立ちます。

スキャン済みデバイス固有のソフトウェア更新定義と検出ルール情報をコンソールから直接表示するこ
ともできます。これを実行するには、**[マイ デバイス]**
からサーバ情報コンソールにアクセスして、左側のナビゲーション ペインで **[ソフトウェア更新]**
をクリックします。

## ソフトウェア更新情報の消去

ソフトウェア更新情報が使用環境に適切でなくなった場合、ソフトウェア更新ウィンドウ (およびコア
データベース) からソフトウェア更新情報を削除できます。

ソフトウェア更新情報を削除すると、対応する検出ルール情報もデータベースから削除されます。ただし、実際のパッチ実行可能ファイルはこの処理で削除されません。パッチ ファイルは、通常コア サーバにあるローカル リポジトリから手動で削除する必要があります。

**ソフトウェア更新情報を消去するには**

1. **[消去]**ツール バー ボタンをクリックします。ダイアログの詳細については、「[セキュリティとパッチ定義の消去] ダイアログについて」を参照してください。
2. ソフトウェア更新情報を削除するプラットフォームを選択します。リストから 1 つ以上のプラットフォームを選択できます。

   更新情報が複数のプラットフォームに関連付けられている場合に更新情報を削除するには、関連付けられているすべてのプラットフォームを選択する必要があります。

3. 上で指定したプラットフォームに関連付けられている、更新情報を削除する言語を選択します。

   Windows プラットフォームを選択した場合は、どの言語の更新情報を削除するか指定する必要があります。UNIX プラットフォームを選択した場合は、すべての言語の更新情報を削除するために [言語選択なし] オプションを指定する必要があります。

4. **[削除]**をクリックします。

## ソフトウェア更新のためのデバイス スキャン

ソフトウェア更新の評価は、デバイスに現在インストールされているバージョンのオペレーティング システムに固有のファイルおよびレジストリ キーを、判明している最新のソフトウェア更新に照合して確認し、サーバの更新の必要性を明らかにすることを意味します。既知の (業界ソースから更新された) ソフトウェア更新情報を確認してスキャン対象の更新を決定すると、ソフトウェア更新スキャナ エージェントがインストールされている管理デバイス上で、カスタマイズされた評価を行うことができます(デバイスの脆弱性スキャンおよびパッチ導入の設定については、この章で前述している「デバイスのソフトウェア更新スキャンの設定」を参照してください)。

ソフトウェア更新スキャナの実行時にはいつも、スキャン グループの内容が読み取られ、これらに固有の更新についてスキャンされます。更新についてサーバをスキャンする前には必ず、そのグループにスキャン対象のソフトウェア更新だけが含まれていることを確認してください。スキャン グループにソフトウェア更新を追加したりこのグループからソフトウェア更新を削除したりして、スキャンのサイズと性質をカスタマイズできます。

## ソフトウェア更新スキャナの実行

ソフトウェア更新スキャナは、コンソールからデバイスに対してスケジュールされたスキャン
タスクとしてプッシュすることもできます。

**ソフトウェア更新スキャン タスクを作成するには**

1. 左側のナビゲーション ペインで、**[ソフトウェア更新]**をクリックします。
2. 最新のソフトウェア更新定義に更新済みであることを確認します。
3. [スキャン] グループに、スキャン対象の更新だけが含まれていることを確認します。
4. **[パッチ タスクのスケジュール]**ツール バー
   ボタンをクリックします。ダイアログの詳細については、「[脆弱性スキャンのスケジュール]
   ダイアログについて」を参照してください。
5. スキャンに固有の名前を入力します。同じ名前のタスク
   スクリプトが既に存在する場合は、既存のスクリプトを上書きするかどうかを選択できます。
6. ターゲット デバイスに進行状況のダイアログを表示するかどうかを指定します。エンド
   ユーザがスキャンをキャンセルできるように、スキャナ ダイアログに [キャンセル]
   ボタンを表示するかどうかを指定することもできます。
7. ターゲット
   デバイスでソフトウェア更新スキャナの実行が完了したときにソフトウェア更新スキャナのダイア
   ログをどのように閉じるかを指定します。エンド
   ユーザに入力を求めるか、指定したタイムアウト時間の経過後にダイアログを閉じるように設定
   できます。
8. **[OK]**をクリックします。
9. 下部ペインのタスクを選択して (**[脆弱性タスク]**の下)、[編集] をクリックします。ターゲット
   パラメータとスケジュール パラメータを設定し、**[保存]**をクリックします。

## 検出した更新の表示

検査対象のソフトウェア更新のいずれかについて、ソフトウェア更新スキャナによっていずれかのターゲット デバイスで更新が検出されると、その情報がコア
サーバにレポートされ、**[検出]**リストに追加されます。

ソフトウェア更新スキャン実行後に検出された更新を表示するには、次のいずれかの方法を実行します
。

## 検出されたグループ別に表示

ソフトウェア更新ウィンドウで**[検出]**
グループを選択して、前回のスキャンで検出されたすべての更新の完全なリストを表示します。

## 個々のデバイス別に表示

**[マイ デバイス]** でデバイス名をダブルクリックしてから**[ソフトウェア更新]**
をクリックして、そのデバイスのソフトウェア更新評価情報の詳細を表示します。

## パッチのダウンロード

パッチを検出されたソフトウェア更新を持つデバイスに導入するには、最初に、ご使用のネットワーク上のローカル パッチ リポジトリにパッチ実行可能ファイルをダウンロードする必要があります。パッチ
ファイルの既定のダウンロード先は、コア サーバの /LDLogon
ディレクトリです。この場所は、**[脆弱性設定の更新]** ダイアログの **[パッチの設定]** タブで変更可能です。

---

**パッチのダウンロード先およびプロキシ サーバの設定**
パッチ ダウンロードでは常に、**[脆弱性設定の更新]** ダイアログの
**[パッチの設定]**タブに現在設定されているダウンロード先の設定値が使用されます。また、ご使用のネットワークがプロキシ サーバを使用してインターネットにアクセスしている場合は、パッチ
ファイルをダウンロードする前に、**[脆弱性設定の更新]** ダイアログの **[プロキシ設定]** タブでプロキシ
サーバの設定値を設定する必要があります。

---

製品によって、最初に [パッチのプロパティ] ダイアログに表示されている URL からパッチ
ファイルのダウンロードが行われます。接続を確立できない場合または何らかの理由でパッチを入手できない場合は、信頼できる業界ソースからのパッチを含む、会社によってホストされているデータベースである LANDesk セキュリティ サービスよりパッチがダウンロードされます。

一度に 1
つずつパッチをダウンロードすることも、一連のパッチを同時にダウンロードすることもできます。

**1 つのバッチをダウンロードするには**

1. ソフトウェア更新の名前をダブルクリックして、その **[プロパティ]** ダイアログを開きます。
2. **[検出ルール]** セクションで、ダウンロードする検出ルールのパッチ ファイルを選択して
   **[選択されているパッチのダウンロード]** をクリックします。
3. ダウンロード動作およびステータスが **[パッチをダウンロード中]**
   ダイアログに表示されます。**[キャンセル]** をクリックすると、ダウンロード
   プロセス全体をいつでも終了できます。
4. ダウンロードの終了時には、**[閉じる]**ボタンをクリックします。

**複数パッチをダウンロードするには**

スケジュールされている、ソフトウェアのすべての更新タスクでは、**[脆弱性設定の更新]**ダイアログの現在の設定が使用されます。特定の更新ジョブの場所、プラットフォーム、言語、パッチ ダウンロード
サイト、またはプロキシ
サーバを変更する場合は、タスクのスケジュールが実行される前に、**[脆弱性設定の更新]**
ダイアログでそれらの設定を変更する必要があります。

1. 左側のナビゲーション ペインで、**[ソフトウェア更新]**をクリックします。
2. **[ダウンロードのスケジュール]** をクリックします。
3. **[スケジュールされているタスク]**ページで、スケジュールを構成します。
4. **[保存]**をクリックします。

### パッチ ファイルの削除

パッチ ファイルを削除するには、通常はコア サーバの LDLogon ディレクトリにあるパッチ リポジトリからパッチを手作業で削除します。

## ソフトウェア更新の修正

ソフトウェア更新定義の更新、スキャン
グループへのスキャン対象更新の配置、管理デバイスでのソフトウェア更新スキャンの実行、注意の必要なソフトウェア更新の判断、および必要なパッチのダウンロードがすべて完了すると、次のステップとして、影響を受けるデバイスに必要なパッチを導入しインストールすることによってソフトウェア更新での修正を実行します。

個々のソフトウェア更新単位で修正が実行されます。言い換えると、個々のソフトウェア更新について、必要なパッチ ファイルを導入しインストールする修正タスクを作成するということです。

ソフトウェア更新スキャンと同様、修正もソフトウェア更新スキャナ
エージェントが設定されたデバイス上でのみ有効です。詳細については、この章で前述している「デバイスのソフトウェア更新スキャンの設定」を参照してください。

Linux の修正がサポートされています。ソフトウェア更新ツールを使って Linux
デバイスの更新を検出しておき、その更新による修正の対策を各自で判断することができます。その場合は、利用している Linux ディストリビューションのサポート購読を使って必要な RPM
をダウンロードし、デバイスに RPM を導入できます。

---

**警告** :多くのパッチは完了後自動的にデバイスを再起動します。

---

**カスタム修正スクリプトを作成するには**

1. 左側のナビゲーション ペインで、**[ソフトウェア更新]**をクリックします。
2. **[検出]**
   グループを選択して、前回のスキャンで検出されたソフトウェア更新を表示します。必ずしもこのグループを選択する必要はありません。まだスキャンされていない、または検出されていない更新についてカスタム修正スクリプトを作成する場合は、他の脆弱性グループをクリックしてその内容を表示し、特定の脆弱性を選択できます。
3. 定義を右クリックして **[影響を受けるデバイスの表示]**
   を選択し、このソフトウェア更新に影響を受けるデバイスを表示します。
4. 定義を右クリックして **[修正タスクの作成]** を選択します。
5. （オプション）**[タスク名]**テキスト ボックスの名前を変更します。
6. オプションを選択して**[OK]**をクリックします。

- **影響を受けるコンピュータをターゲット カートにコピーする**
  :ソフトウェア更新の影響のあるコンピュータを修正のためにターゲット
  カートにコピーします。
- **実行中に進行状況を表示する** :スキャナの実行中、エンド ユーザ
  デバイス上に情報を表示します。スキャナのアクティビティを表示する場合や、このダイアログ内のその他の表示および対話オプションを設定する場合、このオプションをオンにします。このオプションをオンにしないと、このダイアログのその他のオプションは設定に使用できなくなり、スキャナはデバイス上で透過的に実行されます。
- **スキャン ダイアログを閉じる前にユーザ入力が必要** :
  スキャナの表示ダイアログが閉じる前に、エンド
  ユーザにプロンプトを表示する場合は、このオプションを選択します。このオプションをオンにすると、エンド
  ユーザが何も入力しないと、ダイアログは開いたままになり、他のスケジュールされているタスクがタイムアウトする原因になることがあります。
- **タイムアウト後、自動的にダイアログ ボックスを閉じます**
  :指定した時間後にスキャナの表示ダイアログが閉じるようにするには、このオプションを選択します。

# スクリプト

## スクリプトの管理

本製品では、スクリプトを使用してデバイスのカスタム
タスクを実行します。スクリプト作成ダイアログを完了すると、.INI 拡張子が付いた Windows INI
フォーマットの ASCII テキスト ファイルが生成されます。これらのスクリプトは、コア サーバの ¥Program Files¥LANDesk¥ManagementSuite¥Scripts
フォルダに保存されます。スクリプトのファイル名は、コンソールのスクリプト名になります。[**スクリプト**] ウィンドウ (左側のナビゲーション ペインにある [**スクリプト**] をクリック) を使って、ローカル スケジューラ スクリプトを Windows デバイスのために作成するか、自分のスクリプト ファイルを作成して Scripts
フォルダに保存できます。

[**スクリプト**] ウィンドウでは、スクリプトは次のカテゴリに分類されます。

- **[マイ スクリプト]**: このグループに関連付けられたスクリプトです。
- **すべての他のスクリプト**: コア サーバにあるすべてのスクリプトです。
- **ユーザ スクリプト** (管理者にのみ表示される):
  ユーザ全員によって作成されたスクリプト。このスクリプトは、作成者でソートされています。

[**マイ スクリプト**]
の項目の下にグループを作成すると、スクリプトをさらに詳細に分類できます。新しいローカル
スケジューラ スクリプトを作成するには、[**ローカル**] ボタンをクリックします。

スクリプトを作成したら、スクリプトのショートカット メニューの [ **スケジュール**] をクリックします。[**マイ デバイス**] ウィンドウでタスクを実行するターゲット デバイスを指定し、[**スケジュールされているタスク**] ウィンドウでタスクを実行するスケジュールを設定できます。タスクのスケジュールの詳細については、「タスクのスケジュール」セクションを参照してください。

### Management Suite の 旧バージョンを使用しているユーザのスクリプトとタスクのオーナーシップについての変更

Management Suite バージョン 8.70
以前では、すべてのスクリプトはグローバルに設定されていたため、ユーザ全員がすべてのスクリプトを表示できました。本バージョンより、スクリプトはそのスクリプトの作成者と管理者にしか表示できなくなりました。

[**スクリプト**] ウィンドウには [ステート] 列があります。[ステート] 列には、
ユーザ全員がスクリプトを表示できる場合は [公開]
、スクリプトの作成者または管理者しか表示できない場合は [非公開]
と表示されます。ユーザは自分で作成したスクリプトを右クリックして、[非公開] または [公開]

をクリックしてスクリプトのステートを変更できます。管理者は、すべてのスクリプトのステートを変更できます。

[DOS PE] が既定です。その他の PE を選択すると、コマンド スクリプトを作成できなくなります。Windows および Linux PE では、キャプチャまたは導入スクリプトのみを生成できます。

Linux PE を選択した場合は、[LANDesk] または [その他] イメージング ツール
オプションからのみ選択できます。Windows PE を選択した場合は、[LANDesk]、[その他]、および [Microsoft* XImage] から選択できます。

## ローカル スケジューラ スクリプトの作成

ローカル
スケジューラは、デバイスで実行するサービスです。これは標準の管理エージェントの一部として、エージェント構成を導入した際にインストールされます。通常、ローカル
スケジューラは、定期的なインベントリ スキャナを実行するなど Management Suite
のタスクを扱います。ソフトウェアや OS の導入など、ローカル スケジューラではなくコア
サーバによって扱われます。ローカル
スケジューラは、デバイスで定期的に実行する独自のタスクをスケジュールできます。作成したローカル スケジューラ スクリプトは、他のスクリプトと同様に管理デバイスに導入できます。

ローカル スケジューラは、各タスクに ID 番号を割り当てます。ローカル スケジューラ
スクリプトは、本製品が使用するデフォルトのローカル スケジューラ スクリプトとは異なる ID
範囲を持ちます。各デバイスに対して、1 つのカスタム スケジューラ
スクリプトしかアクティブにできません。新しいスクリプトを作成してデバイスに導入する場合は、ローカル インベントリ スキャンのスケジュールなど、デフォルトのローカル スケジュール
スクリプトに影響することなく、古いスクリプト (カスタム ローカル スケジューラ ID 範囲にあるスクリプト) が置き換えられます。

スクリプトのスケジュール
オプションを選択するときは、さまざまなオプションの厳密度に留意してください。たとえば、曜日に月曜日を選択し、月の日に 17 日を選択すると、タスクが月の 17
日目の月曜日にだけ実行され、実行頻度が非常に低くなります。

即座にまたは任意の時間に、ローカル コンピュータ上で restartmon.exe
を実行する作成するスクリプトを作成することができます。特定のコンピュータからのレポートが停止している場合は、LDClient フォルダにある restartmon.exe
を使ってコレクタとすべての監視プロバイダを再開させることができます。このユーティリティは、レポート機能がインストールされていて、レポート機能が中断されているコンピュータ用です。このユーティリティを使って、デバイスを再起動せずにコレクタとプロバイダを再開します。

1. 左側のナビゲーション ペインで、[**スクリプト**] をクリックします。
2. [**ローカル**] をクリックします。
3. [スクリプト名] に名前を入力します。
4. [**追加**] をクリックして、スクリプトのオプションを定義します。

5. 前述のように、ローカル スケジューラのオプションを構成します。終了したら、[**保存**] をクリックします。
6. [**保存**] をクリックして、スクリプトを保存します。
7. [**マイ スクリプト**] グループでそのスクリプトを選択し、[**スケジュール**] をクリックすると作成したスクリプトがデバイスに導入されます。

## 帯域幅オプションについて

ローカル スケジューラ
コマンドを構成する場合、タスクを実行するために管理デバイスに必要な最小の帯域幅を指定できます。タスクを実行する時間が来ると、ローカル スケジューラ タスクを実行している各デバイスが、小さな ICMP ネットワーク
トラフィックを指定したコンピュータに送信し、転送パフォーマンスを評価します。テストのターゲット コンピュータが利用できない場合は、タスクは実行されません。

次の帯域幅オプションを選択できます。

- **RAS:**デバイスのターゲット コンピュータへのネットワーク接続が、少なくとも RAS またはダイアルアップである場合にタスクが実行されます。通常、このオプションの選択は、デバイスが何らかのネットワーク接続を持つ場合に常にタスクを実行することを意味します。
- **WAN:**デバイスのターゲット コンピュータへの接続が、少なくとも WAN 速度である場合にタスクが実行されます。WAN 速度は、LAN のしきい値より遅い非 RAS 接続で定義されます。
- **LAN:**デバイスのターゲット コンピュータへの接続が LAN 速度設定を超える場合に、タスクが実行されます。LAN 速度は、既定で 262,144 bps と定義されます。

## スクリプト タスクのスケジュール

[**スケジュールされているタスク**]
ウィンドウには、スケジュールされたタスクのステータスが、タスクの実行中および完了時に表示されます。スケジューラ サービスとデバイスが通信する方法は 2 つあります。

- 標準の管理エージェント (既にデバイスにインストールされている必要がある) を介して。
- ドメインレベルのシステム アカウントを介して。選択したアカウントには、サービスとしてのログイン権限が必要であり、またサービス設定ユーティリティで認証資格が指定されている必要があります。スケジューラ アカウントの設定の詳細については、「スケジューラ サービスの設定」を参照してください。

LANDesk と一緒に、選択したコンピュータでインベントリ
スキャンを実行するなどの定期的なメンテナンス
タスクを実行するためにスケジュールできる、いくつかの標準スクリプトがインストールされます。
左側のナビゲーション ペインで [**スクリプト**] をクリックし、[**すべての他のスクリプト**] をクリックすると、これらのスクリプトが表示され、スケジュールを設定できます。

**タスクをスケジュールするには**

1. 左側のナビゲーション ペインで、[**スクリプト**] をクリックします。
2. クリックしてスクリプト グループへ移動します。
3. スクリプトをクリックし、[**スケジュール**] をクリックします。
4. タスクの名前を入力し、[**OK**] をクリックします。
5. [**カスタム スクリプト タスク**] タブで [**すべてのタスク**] をクリックし、手順 3 で名前を付けたタスクをクリックして [**編集**] をクリックします。
6. カスタム スクリプト タスクのページに記入します。ページで解らないところがあれば [ヘルプ] をクリックしてヘルプを表示するか、ヘルプの「タスク スケジューラ」を参照してください。

[**スケジュール**] をクリックすると、タスクが作成されます (ターゲット デバイスはなく、スケジュールもされていません)。この [スケジュールされているスケジュール] の手順をキャンセルしても、タスクは既に作成されており、[タスク] リストに表示されていることに注意してください。

## 既定のスクリプトの使用方法

本製品には出荷時に 2 つの既定のスクリプトが含まれています。これらのスクリプトを使用すると、一部の一般的なタスクの完了が容易になります。これらのスクリプトは、[**スクリプト**] ウィンドウ (左側のナビゲーションペインで [**スクリプト**] をクリック)] の下にある「Generic sample dir command script」、「PXE representative deployment」、および「PXE representative removal」は例外です。!

- **インベントリ スキャナ** :選択したデバイス上でインベントリ スキャナを実行します。このスクリプトには、スクリプト ファイルの作成方法を説明したドキュメントが含まれています。コマンドおよびパラメータの正しい使用方法の詳細については、このスクリプト ファイルを読むか印刷してください。
- **Restore client records:**選択したデバイスでインベントリ スキャナを実行しますが、スキャナが、デバイスを構成したコアにレポートを送信します。データベースをリセットする必要がある場合は、このタスクにより、複数のコア環境で、デバイスを正しいコア データベースに追加できます。

# タスクのスケジュール

- カスタム タスク グループ
- [ターゲット デバイス] ページ
- [タスクのスケジュール] ページ
- [カスタム スクリプト] ページ

**スケジュールされているタスク**
ツールは、エージェント構成、ソフトウェア更新、スクリプト、およびデバイス検出で共通しています。下のペインで特定の機能ページに合わせてタスクがフィルタされ、関連するタスクのみが表示されます。たとえば、[**デバイス検索**] ツールを開いた場合、検索タスクが下のペインの [**検索タスク**]
タブに表示されます。他のすべてのタスクは**スケジュールされているタスク**
ツールから表示できます。ここでは、構成をすぐに実行するか、将来のある時点で繰り返しまたは一回のみ実行するかをスケジュールできます。

[**スケジュールされているタスク**] ページの左ペインには次のタスク グループが表示されます。

- **マイ タスク** :
  スケジュールを行ったタスクです。ユーザと管理ユーザだけがこれらのタスクを表示できます。
- **すべてのタスク** : ユーザ タスクと「public」とマークしたタスクの両方です。
- **共通タスク**
  :ユーザが「共通」とマークしたタスクです。このグループからタスクの編集またはスケジュールする人がそのタスクの所有者となります。タスクは [共通タスク] グループに残り、そのユーザの [ユーザ タスク] グループにも表示できます。
- **ユーザ タスク** (管理ユーザのみ) : ユーザが作成したタスク。

[**マイ タスク**、[**共通タスク**]、または [**すべてのタスク**]
をクリックすると、右ペインに次の情報が表示されます。

- **タスク** : タスク名。
- **開始** : タスクの実行がスケジュールされている時刻。タスク名をクリックして [**編集**]
  をクリックすると、開始時間を編集したり、スケジュールをやり直すことができます。
- **ステータス** : 全体的なタスク ステータス。詳細は、右ペインの [ステータス]
  列に表示されます。右ペインの列にはタスク
  ステータスが、[処理中]、[すべて完了]、[完了したものはありません]、[失敗]
  のいずれかで表示されます。
- **配布パッケージ** :
  タスクを配布するパッケージ名。このフィールドはソフトウェアの配布に適用されます。
- **配信方法** :タスクが使用する配信方法。このフィールドはソフトウェアの配布に適用されます。
- **所有者** : このタスクが使用しているスクリプトの作成者の名前。

スケジュールされているタスクをダブルクリックすると、右ペインに次のサマリ情報が表示されます。

- **名前** : タスクの状態名。
- **数量** : タスクの状態ごとのデバイス数。

- **割合** : タスクの状態ごとのデバイスの割合。

デバイスにタスクをスケジュールする前に、デバイスが適切なエージェントを持っていて、インベントリデータベース内にある必要があります。サーバ構成は例外です。サーバ構成は標準の管理エージェントを持たないデバイスをターゲットに選択できます。タスクは [タスク] タブでスケジュールをやり直したり(編集)、削除することができます。タスクをスケジュールしたら、[タスク]
タブでタスクのステータスを確認してください。

タスクを編集するには、編集するタスクを選択して [**編集**]
をクリックします。タスクが開き、そのタスクに適切な編集オプションが表示されます。

## カスタム タスク グループ

「**マイ タスク**」、「**すべてのタスク**」、および「**共通タスク**」のタスク タイプに対してカスタム
グループを作成できます。カスタム
グループを使用すると、脆弱性をスキャンしたり、スクリプトを実行したりするなど、関連したタスクをグループ化できます。グループおよびサブグループは 20 レベルまで設定できます。

1. **カスタム タスク グループを作成するには**左側のナビゲーション
   ペインで、[**スケジュールされているタスク**] をクリックします。

2. 左ペインでグループを作成する [タスク タイプ] をクリックします。
3. ツールバーの [**新しいグループ**] をクリックします。
4. [**グループ名**] テキスト ボックスに名前を入力し、[OK] をクリックします。

カスタム グループを作成したら、タスクまたは別のグループをリストから選択してツールバーの [**移動**]
をクリックすることによって、グループに移動またはコピーできます。

## [ターゲット デバイス] ページについて

このページで、設定しているタスクのデバイス ターゲットを追加できます。また、ターゲット
デバイス、クエリ、およびこのタブ上のタスクのデバイス グループを表示することもできます。複数の LANDesk 管理製品がインストールされている場合、1 つの製品のコンソールで作成したデバイス
グループを、他のすべてのコンソールでも表示できます。このページはデバイス検索タスクには必要ありません。

- **ターゲット一覧の追加** : [**マイ デバイス**]
  から以前にターゲット一覧に置いたデバイスを追加します。
- **クエリの追加** : 以前に作成したクエリの名前をターゲットに指定します。
- **削除** : 選択したターゲットを削除します。

このページにはターゲット デバイス グループが表示されますが、コア サーバに LANDesk Management Suite がインストールされている場合にのみグループが表示されることに注意してください。Server Manager, System Manager を実行している場合、または Management Suite で Web コンソールを実行している場合、デバイス
グループはグループとしてターゲットされません。グループを選択してターゲットとすると、そのグループにある個々のデバイスがターゲット デバイス リストに追加され、[**ターゲット グループ**] ではなく [**ターゲット デバイス**] の下に表示されます。

## [タスクのスケジュール] ページについて

スケジューラには、次のオプションを持つ [**スケジュールされているタスク プロパティ**] タブがあります。

- **未スケジュール**：(既定) 後でスケジュールできるように、[タスク] リストのタスクを未スケジュールのままにしておきます。
- **すぐに開始**：
  できるだけ速やかにタスクを実行します。その他の設定によって、タスクの開始までに 1 分かかる場合もあります。
- **スケジュールされた時刻に開始**
  :指定した時間にタスクを開始します。このオプションをクリックする場合は、次の情報を入力してください。
  - **日付**：
    タスクを開始する日付。ロケールの設定によって、日付順序は「日/月/年」または「月/日/年」になります。
  - **時刻**：タスクを開始する時刻です。
  - **実行周期**：タスクを繰り返し実行する場合は、[**時間単位**]、[**日単位**]、[**週単位**]、[**月単位**] のいずれかをクリックします。[**月単位**] を選択して、月によっては存在しない日付 (31 日など) を選択した場合、その日付が存在する月のみにタスクが実行されます。
- **このデバイスをスケジュールする**：タスクを初めて実行するときは、既定の [待機中または作業中] のままにする必要があります。以降に実行するときには、[すべて]、[成功しなかったデバイス]、または [タスクの実行を試行しなかったデバイス] から選択します。これらのオプションについては、後で詳細に説明します。
  - **成功しなかったデバイス**：
    最初にタスクを完了しなかったすべてのデバイス上でタスクを実行する場合のみ、これを選択します。これは、[成功] 状態を持つデバイスは除外します。このタスクは、[待機中] または [アクティブ] を含む、その他すべての状態のデバイス上で実行されます。タスクをできるだけ多くの不成功デバイス上で実行する必要があるが、タスクをデバイスごとに一度、正しく完了する必要のある場合には、このオプションを使用を検討してください。
  - **待機中または作業中**：
    処理を待機しているまたは現在処理中のデバイスでタスクを実行する場合、これを選択します。

- **すべて** :
  状態に関係なく、すべてのデバイス上でタスクを実行する場合に、これを選択します。できるだけ多くのデバイス上で実行する必要のあるタスク、特に繰り返しタスクがある場合は、このオプションの使用を検討してください。
- **タスクの実行を試行しなかったデバイス**
  :最初にタスクを完了せず、タスクを失敗しなかったデバイス上でタスクを実行する場合のみ、これを選択します。これは、[オフ]、[ビジー]、[失敗]、または [キャンセルされました] 状態のデバイスは除外します。ターゲットとして重要ではないタスクを失敗した多数のターゲット デバイスがある場合には、このオプションの使用を検討してください。

## [カスタム スクリプト] ページについて

- **現在選択しているカスタム スクリプト** : スケジュールするスクリプトを選択します。

# レポート

## レポートについて

System Manager
には、ネットワーク上の被管理デバイスに関する重要な情報を提供するさまざまな特別レポートを生成するのに使用するレポート ツールが含まれています。

System Manager では、コア
データベースにデバイスを追加し、これらのデバイスのハードウェアおよびソフトウェア
データを収集するためにインベントリ スキャン
ユーティリティを使用します。デバイスのインベントリ表示から取得したインベントリ
データは、表示および印刷できます。また、このインベントリ
データを使用してクエリを定義したり、デバイスをグループ化できます。レポート
ツールは、スキャンしたこのインベントリ データを収集し、見やすいレポート
フォーマットに整理することで、このデータを有効に活用します。

あらかじめ定義されているサービス
レポートやインベントリ資産レポートを使用することもできます。レポートを実行したら、コンソールからレポートを表示できます。

Server Manager と Management Suite を共にインストールしている場合は、Server Manager
で実行するレポートには、サーバのみが含まれています。その他のデバイスを除外するようにクエリが設定されている場合を除いて、クエリを実行する場合は、サーバとデバイスの両方を取得します。

特定のコンピュータからのレポートが停止している場合は、LDCLIENT フォルダにある restartmon.exe を使ってコレクタとすべての監視プロバイダを再開させることができます。このユーティリティは、レポート機能がインストールされていて、レポート機能が中断されているコンピュータ用です。このユーティリティを使って、デバイスを再起動せずにコレクタとプロバイダを再開します。

### レポート グループとあらかじめ定義されたレポートについて

レポートは、[**レポート**] ウィンドウ (左側のナビゲーション ペインで [**レポート**] をクリック )
でグループ化されます。管理者はすべてのレポート グループの内容を表示できます。System Manager
には、レポートと呼ばれる特別な役割が含まれていて、他者に対して
レポートの表示を許可しますが、別の管理機能に対するアクセスは提供しません。(詳細については、「役割ベース管理」を参照してください。)レポート権限を持つユーザもレポートを参照して実行できますが、ユーザのスコープに含まれているデバイスだけで実行できます。

[**レポート**] ウィンドウには、次のレポート グループがあります。

- ハードウェア
- ソフトウェア

# レポートの表示

[**レポート**] ウィンドウから任意のレポートを実行できます。

[**レポート**] ウィンドウで、特定のレポート グループをクリックして、
実行するレポートをクリックします。**レポート ビュー**にレポート データが表示されます。

## [レポート ビュー] ウィンドウについて

レポートを使用すると、クライアント
コンピュータの資産を示すグラフをすばやく表示できます。レポートは、スキャナがデータベースに格納するデータから作成されます。ブラウザからレポートを表示したり、印刷したりできます。

**レポートを表示するには**

1. 左側のナビゲーション ペインで、[**レポート**]
   をクリックします。レポートのカテゴリは右ペインに表示されます。レポートの一覧を表示するには、カテゴリの見出しをクリックします。各レポートの横にあるアイコンはレポートのタイプを示しています。

    グラフ アイコンが示されているレポートは、円グラフまたは棒グラフ (2 次元または 3 次元) で表示されます。グラフでは、色の付いている棒や円の各要素をクリックすると、概要にドリルダウンできます。

    文書アイコンが示されているレポートは、テキストで表示されます。

2. レポートを表示するには、レポート名をクリックします。
3. ハードウェアまたはソフトウェアのスキャン日の概要を表示するには、開始日と終了日をクリックして期間を設定し、[**実行**] をクリックします。

ディスク領域の概要レポートには、Windows ベースのデバイスのデータのみが含まれます。

レポートを印刷するには、印刷するページを右クリックして [**印刷**] をクリックします。[印刷] ダイアログの [**印刷**]
をクリックします。レポートが複数のページにわたる場合は、ページごとに右クリックして印刷する必要があります。

**レポートを配布するには**

- レポートを電子メールで送信する場合は、レポートを .PDF
  ファイルに印刷してから電子メールに添付して送ることをお勧めします。

コンソールでは、レポートは円グラフまたは棒グラフで表示されます。グラフのタイプを設定するには、レポート グラフ内のドロップダウン リストをクリックして、グラフのタイプを変更します。

インタラクティブ バー、および多数のレポートに表示される円グラフを表示するためには、Macromedia Flash Player* 7 がインストールされている必要があります。

# クエリ

## クエリの使用方法

クエリとは、コア データベース用にカスタマイズされた検索方法です。この製品は、コア データベースでデバイスのデータベース
クエリを作成するツール、および別のディレクトリにあるデバイスの LDAPクエリ
を作成する方法を提供します。コア データベース クエリは、コンソールの [**クエリ**] ビューで作成します。System Manager 公開クエリは LANDesk® Management Suite で、両方が使用されている場合は LANDesk® Management Suite が System Manager 公開クエリで、それぞれ可視状態となります。LDAP クエリは、**ディレクトリ マネージャ** ツールで作成します。

このセクションでは次の内容について説明します。

- クエリの概要
- クエリ グループ
- データベース クエリの作成
- クエリの実行
- クエリのインポートとエクスポート

### クエリの概要

クエリを使用すると、特定のシステム条件またはユーザ条件に基づいてコア データベース内にあるデバイスを検索して整理することによって、ネットワークを管理できます。

たとえば、プロセッサのクロック周波数が 166 MHz より低いデバイスや、RAM が 64 MB より少ないか、またはハード ドライブが 2 GB より少ないデバイスのみをキャプチャするクエリを作成して実行できます。それらの条件を表す 1 つ以上のクエリ文を作成し、標準的な論理演算子を使用して文を相互に関連付けます。クエリを実行すると、クエリの結果を印刷し、一致するデバイスにアクセスして管理できます。

### クエリ グループ

クエリは、[**マイ デバイス**] ビュー内でグループに関連付けることができます。これらは動的グループと呼ばれ、動的グループの内容は、その動的グループに関連したクエリの結果です。たとえば、同じ地理的エリアのすべてのデバイスから構成されるグループは、メモリ、ハード ディスク サイズなどのクエリに関連付けることができます。

クエリ グループおよびクエリを [すべてのデバイス] ビューに表示する方法、クエリ グループやクエリを使った操作の詳細については、「**アクションのためのデバイスのグループ化**」を参照してください。

# データベース クエリの作成

**[新しいクエリ]**
ダイアログを使用して、属性、関係演算子、および属性の値を選択してクエリを作成します。インベントリ属性を選択し、受け入れ可能な値に関連付けて、クエリ文を作成します。クエリ文を他の文またはグループと関連付ける前に、作成したクエリ文同士を論理的に関連付け、グループとして評価されるようにします。

**データベース クエリを作成するには**

1. コンソールの [**クエリ**] ビューで、[**新規**] をクリックします。
2. インベントリ属性リストから**コンポーネント**を選択します。
3. [**ステップ 1: 検索条件**] で [**編集**] をクリックします。
    1. このリストをドリル
       ダウンして、検索条件とする属性を選択します。たとえば、特定の種類のソフトウェアを実行するすべてのクライアントを検索するには、Computer.Software.Package.Name を選択します。
    2. 属性を選択すると、一連のフィールドがウィンドウの右側に表示されます。これらのフィールドから演算子と値を選択し、検索条件を完成させます。たとえば、Internet Explorer 5.0 を実行するすべてのクライアントを検索する場合、属性は "Computer.Software.Package.Name"、演算子は "="、値は "Internet Explorer 5" になります。
    3. ウィンドウの下部で、[追加] をクリックして空のフィールドに検索条件を入れます。
    4. 別の検索条件を作成し、最初の条件にブール値演算子 (AND や OR) を追加することによって、クエリを絞り込むこともできます。各ボタンを使用して、作成した条件の追加、削除、置換、グループ化、グループ解除を実行します。
    5. 終了したら、[OK] をクリックします。
5. [**ステップ 2: 表示する属性**] で [**編集**] をクリックします。
    1. このリストをドリル
       ダウンし、クエリ結果リストに表示する属性を選択します。クエリで返されるクライアントの識別に役立つ属性を選択してください。表示する属性が見つからない場合は、[カスタム属性] ダイアログで追加できます。ただし、これらの属性をクエリ ダイアログに表示するには、コンピュータに割り当てておく必要があります。
       **注意**：Oracle データベースを使用している場合、インベントリ スキャナで最初から定義されている属性 (たとえば、Computer.Display Name、Computer.Device Name、Computer.Device ID、Computer.Login Name など) を少なくとも 1 つ選択してください。
    2. 属性の選択後、[**追加**] をクリックしてウィンドウの下にある空のフィールドに移動します。クエリ結果リストを表示するには、[件数を含める] をクリックします。
    3. さらに属性を追加する場合はこのプロセスを繰り返します。属性を削除するには [**削除**] ボタンを使用し、属性の順序を変更するには [**上へ移動**] または [**下へ移動**] をクリックします。
    4. 指定するアクションに対してクエリの結果をタッゲット指定可能にするには、[**結果をターゲット指定可能にする**] をクリックします。

5. 終了したら、[OK] をクリックします。
6. （オプション）[**ステップ 3: 属性順に結果並べ替え**] で、[**編集**] をクリックし、クエリ結果の表示順をカスタマイズします。
7. あとで再び同じクエリを実行する場合は、[**クエリの保存**] をクリックしてクエリに独自の名前を付けます。保存する前にクエリを実行すると、クエリ パラメータは失われ、同じクエリを再び実行するにはクエリを作成しなおす必要があります。
8. [**ステップ 4: クエリの実行**] で、[**クエリの実行**] をクリックします。

**表示順序でのクエリ文の実行**
グループを作成していない場合は、このダイアログに一覧表示されたクエリ文は下から上に向かって実行されます。関連するクエリ項目は、グループとして評価されるようにグループ化されていることを確認してください。グループ化されていない場合は、クエリの結果が、期待したものと異なる場合があります。

## クエリの実行

**クエリを実行するには**

1. 左側のナビゲーション ペインで、[クエリ] をクリックします。
2. クエリを選択して [**実行**] をクリックします。

   または

   実行する前にクエリに変更を追加するには、クエリをダブルクリックし、[**編集**] をクリックします。ステップ 1 ～ 3 を変更し、[**クエリの実行**] をクリックします。

   **注意** : クエリに変更を追加した後、変更内容を保存する場合は [**クエリの保存**] をクリックするか、[**名前を付けてクエリを保存**] をクリックして変更後のクエリに新しい名前を付けます。この操作はクエリを実行する前に行います。クエリを実行する前に変更を保存しないと、クエリの変更は保存されません。

3. 結果 (一致したデバイス) は、[**すべてのデバイス**] ビューの右側のペインに表示されます。

## クエリのインポートとエクスポート

インポートおよびエクスポートを使用すると、クエリをあるコア データベースから別のコア データベースに転送できます。エクスポートされたクエリは .XML ファイルとして保存されます。

**クエリをインポートするには**

1. インポートされるクエリを置くクエリ グループを右クリックします。
2. ショートカット メニューの [**インポート**] を選択します。
3. インポートするクエリに移動し、選択します。
4. [**開く**] をクリックして、[**すべてのデバイス**] ビューで選択したクエリ グループにクエリを追加します。

**クエリをエクスポートするには**

1. エクスポートするクエリを右クリックします。
2. ショートカット メニューの [**エクスポート**] を選択します。
3. クエリを XML ファイルとして保存する場所に移動します。
4. クエリの名前を入力します。
5. [**保存**] をクリックして、クエリをエクスポートします。

# カスタム クエリについて

デバイスにインストールされているハードウェアやソフトウェアについてインベントリの詳細が必要な場合には、カスタム クエリが役立ちます。カスタム
クエリを使用すると、類似のインベントリを持つコンピュータのリストを作成できます。また、カスタム
クエリは、グループやスコープを定義するためにも使用されます。

[**カスタム クエリ**] ページ (左側のナビゲーション ペインで [**クエリ**] をクリック)
には、保存されているクエリのリストが表示されます。保存されているクエリを実行するには、クエリを選択してから、[実行] を選択します。

---

クエリ
リストが複数のページに及ぶ場合は、ページの上部にある矢印を使ってページを移動してください。各ページに表示する項目数を入力して、[**設定**] をクリックします。

---

# カスタム クエリの作成

デバイスにインストールされているハードウェアやソフトウェアについてインベントリの詳細が必要な場合には、カスタム クエリが役立ちます。カスタム
クエリを使用すると、類似インベントリを持つデバイスのリストを作成できます。たとえば、すべてのデバイスを 750MHz
以上のプロセッサにアップグレードする場合、データベース内のすべてのデバイスに対し、プロセッサ動作周波数が 750MHz 未満という条件でクエリを実行できます。また、カスタム
クエリは、グループやスコープを定義するためにも使用されます。

インベントリ スキャナがデータベースに格納した、「属性」
と呼ばれる任意のインベントリ項目、およびカスタム属性についてクエリを実行できます。

## クエリの管理

[**クエリ**]
ビューでクエリを管理します。このビューを使用して、クエリの作成、編集、削除を次のように行います。

- 既存のクエリを実行するには、そのクエリを選択して [**実行**] をクリックします。
- 新しいクエリを作成するには、[新規]
  をクリックします。クエリを作成して保存すると、その名前がこのページのリストに表示されます。

- リスト内のクエリを編集するには、そのクエリをダブルクリックします。[**クエリの編集**] ページが表示され、編集可能なクエリ パラメータが表示されます。
- 最新のクエリを編集するには、[**現在のクエリの編集**] をクリックします。
- クエリを削除するには、そのクエリを選択して、[削除] をクリックします。

クエリの作成手順は、次の 4 つのステップで構成されています。

1. **検索条件の作成** : クエリのベースとなる一連のインベントリ属性を指定します。
2. **表示する属性の選択** : IP アドレスやコンピュータのデバイス名など、ユーザが知りたい属性が結果に表示されるように、クエリを絞り込みます。
3. **属性により結果をソートする (オプション)** : クエリ結果をどのようにソートするかを指定します (ステップ 2 で、クエリ結果に 2 種類以上の属性を表示するように選択した場合のみ)。
4. **クエリの実行** : 作成したクエリを実行します。また、後で使用するためにクエリを保存したり、やり直すためにすべてのクエリ情報を消去したりすることもできます。

# ステップ 1:検索条件の作成 (必須)

検索条件は、クエリの基準となるインベントリ属性と関連値のセットです。1 つの検索条件を使用することも、複数の条件をまとめてクエリのベースにすることもできます。

[**クエリの編集**] ページでは次の手順を実行します。[**クエリの実行**] ビューで、[**新規**] をクリックするか、既存のクエリを選択して [**編集**] をクリックします。

**検索条件を作成するには**

1. **ステップ 1** で、[**編集**] をクリックします。データベースに現在あるすべてのインベントリ データのリストを示すウィンドウが表示されます。
2. このリストをドリルダウンして、検索条件とする属性を選択します。たとえば、特定の種類のソフトウェアを実行するすべてのクライアントを検索するには、Computer.Software.Package.Name を選択します。
3. 属性を選択すると、一連のフィールドがウィンドウの右側に表示されます。これらのフィールドから演算子と値を選択し、検索条件を完成させます。たとえば、Internet Explorer 5.0 を実行するすべてのクライアントを検索する場合、属性は "Computer.Software.Package.Name"、演算子は "="、値は "Internet Explorer 5" になります。
4. ウィンドウの下部で、[追加] をクリックして空のフィールドに検索条件を入れます。
5. 別の検索条件を作成し、最初の条件にブール値演算子 (AND や OR) を追加することによって、クエリを絞り込むこともできます。各ボタンを使用して、作成した条件の追加、削除、置換、グループ化、グループ解除を実行します。
6. 終了したら、[OK] をクリックします。

サーバのヘルス状態についてのクエリ (Computer.Health.State) を実行および保存する場合は、データベースの状態が数字で表されることに注意します。検索条件を作

成するときは次の表を使用してください。たとえば、ヘルス状態が「不明」のコンピュータを検出する検索条件を作成するには、演算子「NOT EXIST」を使用します。

| ヘルス状態 | 演算子 |
|---|---|
| 不明 | NOT EXIST |
| 標準 | 2 |
| 警告 | 3 |
| 重要 | 4 |

# ステップ 2:表示する属性の選択 (必須)

ステップ 2
では、クエリ結果で返されたコンピュータの識別に使用する属性を選択します。たとえば、ステップ 1 で設定した検索条件に合致する各コンピュータを物理的に探すために結果を利用する場合、各コンピュータの表示名 (Computer.DisplayName) や IP アドレス (Computer.Network.TCPIP.Address) などの属性を指定します。

[**クエリの編集**] ページでは次の手順を実行します。

**表示する属性を選択するには**

1. **ステップ 2** で、[**編集**] をクリックします。データベースに現在あるすべてのインベントリデータのリストを示すウィンドウが表示されます。
2. このリストをドリルダウンし、クエリ結果リストに表示する属性を選択します。クエリで返されるクライアントの識別に役立つ属性を選択してください。表示する属性が見つからない場合は、[カスタム属性] ダイアログで追加できます。ただし、これらの属性をクエリダイアログに表示するには、コンピュータに割り当てておく必要があります。

   **注意：** Oracle データベースを使用している場合、インベントリスキャナで最初から定義されている属性 (たとえば、Computer.Display Name、Computer.Device Name、Computer.Device ID、Computer.Login Name など) を少なくとも 1 つ選択してください。

3. 属性の選択後、[>>] をクリックしてウィンドウ右側の空のフィールドに移動します。クエリ結果リストを表示するには、[件数を含める] をクリックします。
4. さらに属性を追加する場合はこのプロセスを繰り返します。属性を追加または削除するには矢印ボタンを使用し、属性の順序を変更するには [上へ移動] または [下へ移動] をクリックします。

5. 指定するアクションに対してクエリの結果をタッゲット指定可能にするには、[**結果をターゲット指定可能にする**] をクリックします。
6. 終了したら、[OK] をクリックします。

クエリ結果リストに列の見出しを追加することもできます。

**列の見出しを変更するには (オプション)**

1. **ステップ 2** で、[**編集**] をクリックします。
2. 下のボックスで列の見出しをクリックし、[編集] をクリックします。見出しを編集して Enter キーを押します。必要に応じて繰り返します。
3. [**OK**] をクリックします。

クエリ作成プロセスでの次のステップはオプションで、2
つ以上の列のあるクエリ結果にのみ適用されます。そのため、この段階でクエリを保存してください。クエリを保存するには、ページの上部にある [クエリの保存]
をクリックします。ウィンドウが表示され、このクエリの名前を入力するように求めるプロンプトが表示されます。名前を入力し、ウィンドウの右上隅にある [保存] をクリックします。

# ステップ 3:属性により結果をソートする (オプション)

この操作は、ステップ 2 で 2
つ以上の属性および列見出しを定義しており、これらの列のいずれかで結果をアルファベット順または番号順に並べ替える場合にのみ必要です。

たとえば、クエリ結果を、返されたコンピュータのそれぞれの IP アドレスおよびプロセッサ タイプという 2 つの異なる属性の順番に表示するように指定したとします。この場合、ステップ 3 では結果をプロセッサ タイプのアルファベット順に並べ替えることができます。

ステップ 3 を実行しないと、ステップ 2 で選択した最初の属性順に自動的に並べ替えが行われます。

**属性により結果をソートするには**

1. **ステップ 3** で、[**編集**] をクリックします。ウィンドウが表示され、**ステップ 2** で選択した属性が示されます。
2. 並べ替えに使用する属性を選択し、[>>] をクリックして空のテキスト ボックスに移動します。
3. [**OK**] をクリックします。

# ステップ 4:クエリの実行

クエリを作成すると、これを実行したり、保存したり、消去して最初からやり直したりすることができます。

後で使用するためにクエリを保存するには、[**保存**] ツール バー
ボタンをクリックします。保存したクエリは [**カスタム クエリ**]

ページに一覧表示されます。クエリが別のクエリの更新バージョンである場合は、[名前を付けて保存] ツール バー ボタンをクリックして新しい名前を付けます。

既定では、保存されているクエリは保存したユーザにのみ表示されます。保存する前に [**公開クエリ**] をオンにしておくと、保存されたクエリはすべてのユーザに表示されます。クエリを公開できるのは、公開クエリ管理権限がある管理者のみです。

複数の製品ファミリの製品がインストールされている場合、クエリは製品間で共有されます。あるクエリを 1 つの製品のコンソールで保存すると、ほかの製品のコンソールにも表示されるようになります。

このクエリの結果を表示するには、[**実行**] ツールバー ボタンをクリックします。

[**クエリの編集**] ページからクエリのパラメータをクリアするには、[**クリア**] ツールバー ボタンをクリックします。クエリがあらかじめ保存されている場合は、現在のページから消去されますが [**カスタム クエリ**] リストに残ります。

# クエリ結果の表示

クエリ結果は、クエリ作成過程で指定した検索条件に一致した項目です。結果が予想と異なっている場合は、[**クエリの編集**] ページに戻って情報を絞り込んでください。

ドリルダウンして、クエリ結果リスト内のいずれかのデバイスに関する詳細情報を表示するには、クエリ データをダブルクリックするか、クエリ データを右クリックして表示されたメニューで [**コンピュータの表示**] をクリックします。

[**クエリ結果**] ページで [**CSV 形式で保存**] ツールバー ボタンをクリックすると、結果をスプレッドシートまたは別のアプリケーションと互換性のある形式でエクスポートできます。

クエリ結果を印刷するには、[クエリ結果] ページの [**印刷ビュー**] をクリックします。

# ドリルダウン クエリ結果の表示

クエリ結果は、クエリ作成過程で指定した検索条件に一致した項目です。結果が予想と異なっている場合は、[**クエリの編集**] ページに戻って情報を絞り込んでください。

ドリルダウンして、クエリ結果リスト内のいずれかのデバイスに関する詳細情報を表示するには、クエリ データをダブルクリックするか、クエリ データを右クリックして表示されたメニューで [**コンピュータの表示**] をクリックします。

# クエリ結果の CSV ファイルへのエクスポート

クエリ結果のデータをスプレッドシート アプリケーションで表示するには、データを CSV (コンマ区切り値) ファイルとしてエクスポートします。[**クエリ結果**] ページで [**CSV 形式で保存**] ツール バー

アイコンをクリックし、情報を CSV ファイルとして保存します。これで、この CSV ファイルのインポートおよびこのファイルを使用した作業に Microsoft Excel* などのアプリケーションを使用できます。

# クエリの列の見出しの変更

1. 既存のクエリを開くか、新しいクエリを作成します。
2. 下のボックスで列の見出しをクリックし、[編集] をクリックします。見出しを編集して **Enter** キーを押します。必要に応じて繰り返します。
3. [**OK**] をクリックします。

# クエリのエクスポートおよびインポート

作成したクエリはすべてエクスポートおよびインポートすることができます。クエリはすべて、XML ファイルとしてエクスポートします。同じクエリ ファイル名を 2 回以上エクスポートすると、既存のファイルが上書きされます。これを避けるには、エクスポートしたファイルを別の場所にコピーしてください。

エクスポートおよびインポートの機能は、次のいずれかの場合に役立ちます。

- 使用しているデータベースを再インストールする必要がある場合、エクスポート/インポート機能を使用すると、既存のクエリを保存して新しいデータベースで使用できます。

  たとえば、クエリのエクスポート後、これらをデータベースの再インストールによる影響を受けないディレクトリに移動できます。データベースの再インストール後、Web サーバ上のクエリ ディレクトリにクエリを戻し、これらを新しいデータベースにインポートできます。
- エクスポート/インポート機能を使用して、クエリを他のデータベースにコピーできます

  たとえば、クエリを Web サーバ上のクエリ ディレクトリにエクスポートしてから、電子メールや FTP で他の人に送信できます。受信者は、これらのクエリを別の Web サーバ上のクエリ ディレクトリに配置し、別のデータベースにインポートできます。また、ドライブをマップして、別の Web サーバ上のクエリ ディレクトリにクエリを直接コピーすることもできます。

**クエリをエクスポートするには**

エクスポートするクエリが格納されているデータベースに接続中に、次の手順を実行します。

1. 左側のナビゲーション ペインで、[**クエリ**] をクリックします。
2. [**カスタム クエリ**] ページで、エクスポートするクエリの名前をクリックします。[**編集**] をクリックします。
3. [**クエリの編集**] ページで、[**エクスポート**] ツールバー ボタンをクリックしてクエリをディスクにエクスポートします。

4. [**クエリがエクスポートされました**]
   ページで、そのクエリを右クリックして、選択済みのディレクトリに XML
   ファイルとしてダウンロードします。このクエリは XML ファイルになります。

同じクエリ ファイル名を 2
回以上エクスポートすると、既存のファイルが上書きされます。これを避けるには、エクスポートしたファイルを別の場所にコピーしてください。

最終的にクエリをデータベースにインポートして戻す場合は、Web サーバによって認識されているクエリディレクトリに移動する必要があります。このディレクトリは、既定では「c:¥inetpub¥wwwroot¥LANDesk¥LDSM¥queries」です。

**クエリをインポートするには**

インポートするクエリが格納されているデータベースに接続中に、次の手順を実行します。

1. 左側のナビゲーション ペインで、[クエリ] をクリックします。
2. [**カスタム クエリ**] ページで、[**新規**] をクリックします。
3. [**クエリの編集**] ページで、[**インポート**] ツールバー ボタンをクリックします。
4. インポートするクエリを選択します。インポートする前にこのクエリのパラメータを確認する場合は、[表示] をクリックします。
5. [**クエリの編集**] ページで、[**インポート**] をクリックしてクエリをロードします。
6. クエリのロード後、スクロール ダウンし、[クエリの保存]
   をクリックしてこのデータベースに保存します。

# インベントリの管理

インベントリ スキャン ユーティリティを使用して、コア
データベースにデバイスを追加したり、デバイスのハードウェアおよびソフトウェア
データを収集したりできます。このユーティリティは、インベントリ
データの表示、印刷、およびエクスポートやクエリの定義、デバイスのグループ化、および特別レポート
の生成などにも使用できます。

このセクションでは次の内容について説明します。



# インベントリ スキャンの概要

デバイス セットアップ機能でデバイスを構成すると、インベントリ
スキャナがデバイス上にインストールされるコンポーネントに含まれます。クライアント構成を作成する際
に、インベントリ スキャナをデバイス上で実行するタイミングを指定できます。

インベントリ
スキャナはデバイスが初期設定されると自動的に実行されます。スキャナの実行可能ファイルの名前は
、Windows では LDISCAN32.EXE、Linux では LDISCAN です。インベントリ
スキャナはハードウェアおよびソフトウェア データを収集し、コア
データベースに入力します。その後、デバイスが起動されるたびにハードウェア
スキャンが実行されますが、ソフトウェア スキャンはユーザが指定した間隔で実行されます。ソフトウェア
スキャンの設定を指定するには、コア サーバで [**スタート**]、[**プログラム
ファイル**]、[LANDesk、[LANDesk Configure Services] の順にクリックします。

インベントリ サービスの設定の詳細については、付録 C の「インベントリ
サービスの設定」を参照してください。

最初のスキャンの終了後、コンソールからスケジュールされたタスクとしてインベントリ
スキャンを実行できます。インベントリ スキャンをリモート
サーバに対してスケジュールするには、リモート
デバイス上で標準管理エージェントを実行しておく必要があります。

---

**注意**：検索機能を使用してコア データベースに追加されたデバイスのインベントリ データは、コア
データベースにスキャンされていません。完全なインベントリ
データをデバイスごとに表示するには、各デバイス上でインベントリ
スキャンを実行する必要があります。

---

次の場合にインベントリ データを表示し使用できます。

- 特定のインベントリ属性を表示するために [**すべてのデバイス**] リストをカスタマイズする。

- コア データベースで特定のインベントリ属性のあるサーバのクエリを実行する。
- の管理タスク処理のためにデバイスをグループ化する。
- インベントリ属性に基づいて特別レポートを生成する。
- デバイス上のハードウェアおよびソフトウェアの変更をトラックし、変更時にアラートまたはログ ファイル エントリを生成する。

インベントリ スキャナの動作の詳細については、次の各セクションを参照してください。

## デルタ スキャン

デバイス上で最初のフル スキャンが終了すると、インベントリ
スキャナを次回実行した際にデルタ変更のみをキャプチャしてコア データベースに送信します。Windows レジストリからソフトウェア情報を収集するには、スキャナ オプション /RSS を使用します。

## フル スキャンの強制

デバイスのハードウェアおよびソフトウェア データのフル スキャンを強制するには、既存の差分スキャン ファイルを削除し、**Configure LANDesk Software Services** アプレットの設定を変更します。

1. サーバから **invdelta.dat** ファイルを削除する。最新のインベントリ スキャンのコピーは、ハード ドライブのルートに invdelta.dat
   という名前の隠しファイルとしてローカルに保存されています(LDMS_LOCAL_DIR
   環境変数によりこのファイルの場所が決定されます)。
2. 「**/sync**」オプションをインベントリ スキャナ ユーティリティのコマンド ラインに追加する。コマンド ラインを編集するには、[**スタート**]、[**プログラム**]、[**LANDesk Management**]
   の順にクリックします。次に [**インベントリ スキャン**] ショートカット
   アイコンを右クリックし、[**プロパティ**]、[**ショートカット**] の順に選択して**ターゲット**
   パスを編集します。
3. コア サーバで、[**スタート**]、[**プログラム**]、[**LANDesk**]、[**LANDesk Configure Services**]
   の順にクリックします。
4. [**インベントリ**] タブをクリックし、[**詳細設定**] をクリックします。
5. [**Do Delta** (デルタ)] 設定をクリックします。[**値**] ボックスに「**0**」と入力します。
6. [**OK**] を 2 度クリックし、サービスを再起動するかどうかをたずねるメッセージに対して [**はい**] をクリックします。

## スキャン圧縮

既定では、Windows インベントリ スキャナ (LDISCAN32.EXE) によって実行されるインベントリ
スキャンは圧縮されています。スキャナは、おおよそ 8:1 の圧縮比率でフル スキャンおよびデルタ スキャンを圧縮します。スキャン結果は、最初にメモリ内でビルドされてから圧縮され、より大きなパケット サイズを使用してコア
サーバに送信されます。スキャン圧縮には、より少ないパケットおよび帯域幅が使用されます。

## スキャンの暗号化

インベントリ スキャンは、暗号化されています (TCP/IP スキャンのみ)。インベントリ スキャンの暗号化を無効にするには、LANDesk Configure Services アプレットの設定を変更します。

1. コア サーバで、[**スタート**]、[**プログラム**]、[**LANDesk**]、[**LANDesk Configure Services**] の順にクリックします。
2. [**インベントリ**] タブをクリックし、[**詳細設定**] をクリックします。
3. [**Disable Encryption** (暗号化を無効にする)] 設定をクリックします。[**値**] ボックスに「**1**」と入力します。
4. [**設定**] をクリックし、[**OK**] をクリックします。
5. [**OK**] をクリックし、サービスを再起動するかどうかをたずねるメッセージに対して [**はい**] をクリックします。

# インベントリ データの表示

インベントリ スキャナがデバイスのスキャンを終了すると、コンソールにシステム情報を表示できます。

ハードウェア、デバイス ドライバ、ソフトウェア、メモリ、環境情報などのデバイス インベントリがコア データベースに保存されます。このインベントリは、デバイスの管理や設定、およびシステム問題をすばやく識別するために使用できます。

インベントリ データは次の方法で表示できます。

- サマリ インベントリ
- フル インベントリ
- 属性プロパティの表示
- システム情報

作成したレポートでもインベントリ データを表示できます。詳細については、「レポート概要」を参照してください。

## サーバ情報コンソールからのサマリ インベントリの表示

サマリ インベントリはサーバ情報コンソールの [**概要**] ページにあり、デバイスの基本的な OS 設定およびシステム情報についての要約が記載されています。

**注意**：検索ツールを使用してデバイスをコア データベースに追加した場合、このインベントリ データはコア データベースにスキャンされていません。サマリ インベントリ機能を問題なく完了させるために、このサーバでインベントリ スキャンを実行する必要があります。

**サマリ インベントリを表示するには**

1. コンソールの [**すべてのデバイス**] ビューで、デバイスをダブルクリックします。

2. 左側のナビゲーション ペインで、[**システム情報**] をクリックし、[**システムの概要**] をクリックします。

## Windows 2000/2003 サーバの概要データ

この情報は、Windows 2000/2003 サーバのサマリ インベントリを表示する場合に表示されます。

- **ヘルス** : サーバの現在のヘルス状態。
- **タイプ** : アプリケーション、ファイル、電子メールなどのサーバの種類。
- **製造元** : サーバの製造元。
- **機種** : サーバの機種型。
- **BIOS バージョン** : ROM BIOS のバージョン。
- **オペレーティング システム**: サーバ上で実行中の Windows または Linux OS : 2000、2003、または Red Hat。
- **OS バージョン** : サーバ上で実行中の Windows 2000/2003 または Linux OS のバージョン番号。
- **CPU** : サーバ上で実行されているプロセッサのタイプ。
- **脆弱性スキャナ** : インストールされているエージェントのバージョン。
- **インベントリ スキャナ** :インストールされているエージェントのバージョン。
- **監視** :インストールされている監視スキャナのバージョン。
- **前回の再起動** :サーバが最後に再起動された時間。
- **CPU 使用率** : プロセッサの現在の使用率。
- **使用されている物理メモリ** : サーバ上で使用可能な RAM 容量
- **仮想メモリ使用量** : RAM およびスワップ ファイル メモリなどのサーバで利用可能なメモリ容量
- **ディスク領域使用量**: 使用されているドライブ領域の割合。ハード ドライブが複数ある場合は、各ドライブが一覧されます。

IPMI 対応サーバの場合は、IPMI 固有の追加データが表示されます。Linux サーバの場合は、[概要] ビューにも同様の情報が表示されます。

# フル インベントリの表示

フル インベントリには、デバイスのハードウェアおよびソフトウェア コンポーネントの完全なリストがあります。このリストにはオブジェクトおよびオブジェクト属性が含まれています。

**フル インベントリを表示するには**

1. コンソールの [**すべてのデバイス**] ビューで、デバイスをクリックします。
2. [**プロパティ**] タブで、[**インベントリの表示**] をクリックします。.

# 属性プロパティの表示

インベントリのリストからデバイスのインベントリ オブジェクトの属性プロパティを表示できます。属性プロパティは、インベントリ

オブジェクトの性質や値を示します。また、新しいカスタム属性を作成したり、ユーザ定義属性を編集したりできます。

属性プロパティを表示するには、左ペインの属性をクリックします。

Internet Explorer 内でこの情報を印刷するには、フレーム内で右クリックし、[印刷] をクリックします。Mozilla 内で印刷するには、フレーム内で右クリックし、[**This Frame** (このフレーム)]、[**Save Frame As** (名前を付けてフレームを保存)] の順にクリックして [**保存**] をクリックし、アプリケーション内でファイルを開いて [**印刷**] をクリックします。

## システム情報

サーバ情報コンソールで、デバイスのシステム情報を表示および変更できます。[**ハードウェア**]、[**ソフトウェア**]、[**ログ**]、および[**その他**] カテゴリ内の情報は、保存されているデータまたはリアルタイム データです。情報リンクをクリックすると、選択したコンポーネントの詳細を表示できます。必要に応じて、しきい値の設定、情報の入力を行うことができます。

1. コンソールの [**すべてのデバイス**] ビューで、デバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[**システム情報**] をクリックします。
3. グループを展開して表示する情報リンクをクリックします。

# インベントリ オプションのカスタマイズ

コンソールには、インベントリ オプションをカスタマイズする際に使用できるサービス設定ユーティリティが含まれています。多くの場合、既定のオプションを使用できますが、オプションを変更する必要がある場合にはこのユーティリティを実行できます。Configure Services アプレットを起動するには、コア サーバ上で [**スタート**]、[**プログラム ファイル**]、[**LANDeskConfigure Services LANDesk**]、[] の順にクリックします。(このユーティリティのファイル名は svccfg.exe です。)

サービス設定ユーティリティを使って設定します。

- データベース名、ユーザー名、およびパスワード
- デバイス ソフトウェアのスキャン間隔、メンテナンス、インベントリ スキャン保存日数、およびクライアント ログイン履歴の長さ
- 重複デバイス ID の処理
- スケジューラ構成 (スケジュールされているジョブとクエリ評価の間隔を含む)
- カスタム ジョブ構成 (リモート実行タイムアウトを含む)

詳細については、サービス設定ユーティリティの各タブで [**ヘルプ**] をクリックしてください。

# LDAPPL3.TEMPLATE ファイルの編集

LDAPPL3.TEMPLATE ファイルには、特にスキャナのインベントリ パラメータに関連する情報が含まれています。このテンプレート ファイルを LDAPPL3.INI

ファイルと併用すると、デバイスのソフトウェア
インベントリを識別します。このファイルは、エージェント構成の一部として管理 Windows
デバイスに保存されます。このパラメータは、エージェント構成の [インベントリ] タブに設定されます。

---

Linux デバイスでは、類似した構成ファイル (/etc/ldappl.conf)
にスキャナのパラメータ情報が含まれています。このファイルを編集してスキャナの動作を変更できます
。ファイルには Linus スキャナの動作を変更する方法についての指示が含まれています。

---

テンプレート ファイルの [LANDesk Inventory] セクションを編集すると、スキャナがソフトウェア
インベントリを識別する方法を決めるパラメータを設定できます。既定では、LDAPPL3.TEMPLATE
はコア サーバの LDLogon 共有にあります。

次の表に従って、テキスト エディタの [LANDesk Inventory] セクションを編集します。

| オプション | 説明 |
|---|---|
| Mode | スキャナがデバイス上でソフトウェアをスキャンする方法を決めます。既定は Listed です。設定は次のとおりです。<br><br>• **Listed:**LDAPPL3 にリスト済みファイルを記録します。<br>• **Unlisted:** LDAPPL3 には定義されていないが ScanExtensions 行にリスト済みの拡張子を持つすべてのファイルの名前および日付を記録します。このモードでは、ネットワーク上で許可されていないソフトウェアを検索できます。<br>• **All:** リスト済みおよび非リストのファイルを検索します。 |
| Duplicate | ファイルの複数のインスタンスを記録します。値を OFF に設定して最初のインスタンスのみを記録するか、ON に設定して検出されたすべてのインスタンスを記録します。既定は ON です。 |
| ScanExtensions | スキャンするファイルの拡張子 (.EXE、.COM、.CFG など) を設定します。ファイルの拡張子が複数ある場合は、スペースを使用して区切ります。既定では、スキャンされるのは「.EXE」のみです。 |
| バージョン | LDAPPL3 ファイルのバージョン番号です。 |
| レビジョン | LDAPPL3 ファイルのレビジョン番号で、将来の互換性の確認に役立ちます。 |
| CfgFiles 1-4 | 指定したファイルの日付、時刻、ファイルサイズ、および内容を記録します。すべてのローカル ドライブを除外する場合は、ドライブ文字 (たとえば C:) を省略できます。4 つの行のそれぞれに複数のファイルを指定できますが、1 行の長さは 80 文字に制限されています。<br><br>同じ行にあるパス名はスペースで区切ります。 |

| オプション | 説明 |
| --- | --- |
| | スキャナは、現在のファイルのデータおよびサイズを、以前にスキャンしたファイルのデータおよびサイズと比較します。そのデータとサイズが一致しないと、スキャンは新しいレビジョンとしてそのファイルの内容を記録します。 |
| ExcludeDir 1-3 | 特定のディレクトリをスキャンから除外します。すべてのローカル ドライブを除外する場合は、ドライブ文字 (たとえば C:) を省略できます。列挙は 1 から始まり、各行は ″¥″ で終わる必要があります。 |
| MifPath | MIF ファイルが格納される、クライアントのローカル ドライブ上の場所を指定します。既定の場所は、c:¥DMI¥DOS¥MIFS です。 |
| UseDefaultVersion | TRUE に設定されると、LDAPPL3 のファイル名とファイル サイズ エントリのうちファイル名のみが一致していれば、スキャナは一致を報告します (バージョンは EXISTS として報告されます)。このオプションは、不明なアプリケーションでもファイル名が同じであれば一致と見なす可能性があります。配布されている LDAPPL3.TEMPLATE ファイルでは、このパラメータは FALSE に設定されています。つまり、正確に一致しなければエントリは追加されません。このパラメータがなければ、既定で TRUE になります。 |
| SendExtraFileData | TRUE に設定されると、追加のファイル データがコア サーバに送信されます。既定は FALSE です。つまり、既定では、パス、名前、およびバージョンのみがコア データベースに入力されます。 |

**LDAPPL3.TEMPLATE ファイルを編集するには**

1. コア サーバから ¥Program Files¥LANDesk¥ManagementSuite¥LDLogon ディレクトリに移動して、メモ帳などのテキスト エディタで LDAPPL3.TEMPLATE を開きます。
2. 更新するパラメータまでスクロールして変更します。
3. ファイルを保存します。

## アプリケーション リストの更新

アプリケーション リストのデータである DEFAULTS.XML は、コア データベースに保存されます。よく使用されるソフトウェア アプリケーションの名前およびバージョン番号は非常に頻繁に変更されるので、LANDesk では新しい DEFAULTS.XML を年に数回公開します (前バージョンの LANDesk ソフトウェアでは、このファイルは LDAPPL.INI と呼ばれていました)。

**アプリケーション リストを更新するには**

1. 新しい DEFAULTS.XML または LDAPPL3.TEMPLATE ファイルを http://www.landesk.com/support/downloads からダウンロードします。ファイルをダウンロードするには、製品を選択して [**Software update**] をクリックします。
2. ファイルを LDLOGON ディレクトリに保存します。
3. 「アプリケーション リストの公開」の手順に従って新しい LDAPPL3.INI を公開します。

## アプリケーション リストの公開

アプリケーション リストを公開すると、DEFAULTS.XML 内の最新のアプリケーション リストがデータベースにインポートされ、アプリケーション リストと LDAPPL3.TEMPLATE の内容が結合されて LDAPPL3.INI ファイルが更新されます。¥Program Files¥LANDesk¥ManagementSuite ディレクトリにあるスタンドアロン ユーティリティ COREDBUTIL.EXE を使用すると、これらの手順が自動的に実行されます。

**アプリケーションのリストを公開するには**

1. CoreDBUtil.exe を起動します。
2. [**アプリケーション リストの公開**] ボタンをクリックします。

LDAPPL3.TEMPLATE または DEFAULTS.XML の更新版を変更またはダウンロードした場合は、アプリケーション リストを公開する必要があります。

# ハードウェア構成

## Intel* AMT サポート

System Manager は、Intel* Active Management Technology (Intel* AMT)
を使用するデバイスをサポートしています。AMT はリモート
デバイスの管理を可能にするハードウェアとファームウェアの機能であり、オペレーティング
システムまたはデバイスの電源の状態に関係なく、デバイスのアクセスにアウトオブバンド (OOB)
通信を使用します。

本製品は Intel AMT のバージョン 1 および 2 をサポートしています。Intel AMT 2
デバイスのプロビジョニング手順には、バージョン 1
の時にはなかった新しい機能が含まれています。バージョン 2
でのプロビジョニングの詳細については、「Intel AMT
デバイスの設定」を参照してください。本セクションの情報は、特に明記されていない限り両方のバージョンに当てはまります。

ハードウェア構成ツールには、Intel AMT デバイスの管理用に次のような機能があります。

- プロビジョニング ID (PID および PPS) の自動生成 (バージョン 2)
- 管理デバイスのユーザ名およびパスワードの変更
- 回路ブレーカ ポリシーの設定および有効化 (バージョン 2)
- エージェント プレゼンス監視の設定および有効化 (バージョン 2)

### 管理エージェントがある場合とない場合のデバイスの管理方法

デバイスに Intel AMT が構成されている場合、デバイスに LANDesk
エージェントがインストールされていなくても、ある程度の管理機能が利用できます。ネットワークに接続されていてスタンバイ電源が入っていれば、デバイスを検出してインベントリに追加し、ネットワーク上の他のデバイスとともに管理することができます。

デバイスに Intel AMT
が搭載されていて管理エージェントがインストールされていない場合は、非管理デバイス検出で検出され、インベントリ データベースに移動される場合があります。この場合は [マイ デバイス]
リストに表示されます。ただし、System Manager の管理オプションの多くは利用できません。LANDesk
エージェントをインストールすると、これらのオプションが使用可能になります。Intel AMT
で構成されているデバイスで使用可能な管理機能には、次のようなものがあります。

- **インベントリの概要** :
  デバイスの電源が入っていない場合でも、そのデバイスの通常のインベントリ
  データのサブセットをクエリしたり、リアルタイムで表示したりすることができます。
- **イベント ログ** : Intel AMT
  特有のイベントについて、そのイベントの重要度および説明を示すログをリアルタイムで表示できます。

- **リモート ブート マネージャ**： デバイスのオペレーティング
  システムや電源の状態に関わらず、電源サイクルおよび複数の起動オプションをリモート管理コンソールから開始できます。使用可能なオプションは、そのデバイス上でサポートされるオプションに依存します。一部のデバイスは起動オプションの一部をサポートしません。
- **脆弱性スキャンの強制と OS ネットワークの無効化**：
  デバイスで悪意のあるソフトウェアが実行されている可能性がある場合、次回再起動時に脆弱性スキャンを実行できます。必要に応じて、デバイスのネットワーク アクセスをオペレーティング システム
  レベルで無効にし、不要なパケットがネットワークに広がらないようにすることができます。

管理オプションの詳細については、「Intel AMT デバイスの管理」を参照してください。

## Intel AMT バージョン 1 機能の提供要件

デバイスを Intel AMT デバイスとして検出するにはまず、そのデバイスで Intel AMT
構成画面にアクセスし、製造元の既定のパスワードをセキュア
パスワードに変更しておく必要があります。(Intel AMT
構成画面へのアクセス方法の詳細については製造元のマニュアルを参照してください。)この手順を行わないと、デバイスは検出されますが Intel AMT デバイスとして認識されず、Intel AMT
デバイスとして検出させた場合に表示されるインベントリ サマリ情報を表示できません。

コア サーバが検出した Intel AMT
デバイスを認証するには、ユーザ名/パスワードの資格情報がサービス設定ユーティリティで設定した資格情報と一致している必要があります。資格情報は Intel AMT 構成画面で変更できます。

Intel AMT デバイスを管理するためにコア
データベースに追加すると、そのデバイスが既にプロビジョニングされているかどうかに関わらず、System Manager
はサービス設定ユーティリティで選択したモードに自動的にデバイスをプロビジョニングします。Small Business モードはネットワーク インフラクストラクチャ
サービスなしでセキュアではない基本的な管理機能を提供し、Enterprise
モードは大企業向けで、DHCP、DNS、TLS 証明機関サービスを使って管理デバイスとコア
サーバ間のセキュアな通信を確実にします。

Intel AMT デバイスを Enterprise モードで提供した場合、コア
サーバは安全な通信のためにデバイスに証明書をインストールします。別のコア
サーバが管理するデバイスの場合、いったん提供を解除してから新しいコア
サーバで再度提供を行う必要があります。そうしないと、新しいコア
サーバに一致する証明書がないので、デバイスの Intel AMT
アクセスは応答しません。同様に、他のコンピュータがそのデバイスの Intel AMT
機能にアクセスしようとしても、一致する証明書がないのでアクセスできません。

# Intel* AMT デバイスの設定

Intel AMT
機能を持つデバイスは、初めてセットアップして電源を入れる時に設定する必要があります。初期設定プロセスには、許可されたユーザのみが Intel AMT
管理機能へアクセスできるようにする、いくつかのセキュリティの手順があります。

Intel AMT デバイスは、ネットワーク上のプロビジョニング サーバと通信します。このプロビジョニング サーバは、ネットワーク上の Intel AMT デバイスからのメッセージをリッスンして、そのデバイスの OS の状態に関係なくアウトオブ バンド通信を使って IT
スタッフがサーバを管理できるようにします。!ProductName! は、Intel AMT 用のプロビジョニング サーバとして機能し、セットアップ時にデバイスのプロビジョニングをアシストする機能も持っています。これで、追加の !ProductName! 管理エージェントの有無にかかわらず、これらのデバイスを管理できます。

このセクションでは、新しい Intel AMT (バージョン 2)
デバイスを構成するための推奨プロセスの概要を説明します。このプロセスでは、System Manager を利用して 1 対のプロビジョニング ID (PID と PPS) を作成します。これらの ID は、デバイスの [Intel AMT 構成画面に入力すると、ID を認識しているプロビジョニング
サーバへの安全な接続を確実に行うので、Intel AMT デバイスが最初のプロビジョニング
プロセスを正常に完了できます。

---

Intel AMT バージョン 1 機能を持つデバイスは、類似のプロセスを利用していましたが、PID と PPS キーは利用していませんでした。詳細は本セクションの終わりにある注意を参照してください。

---

## Intel AMT 2 デバイスのプロビジョニング

Intel AMT 2 デバイスを受け取ると、IT
技術者はコンピュータを組み立てて電源を入れます。デバイスに電源が入った後で、技術者は BIOS ベースの Intel ME (Management Engine) 構成画面にログインして、既定のパスワード (admin) を堅牢なパスワードに変更します。これで、Intel AMT 構成画面にアクセスできるようになります。

Intel AMT 構成画面では、次のようなプロビジョニング準備情報を入力します。

- PID (provisioning ID: プロビジョニング ID)
- PPS (pre-provisoning passkey: プロビジョニング準備パスキー)、別名 PSK (pre-shared key: 共有準備キー)
- プロビジョニング サーバの IP アドレス
- プロビジョニング サーバとの通信用ポートとしてポート 9882
- Enterprise モードの選択
- Intel AMT デバイスのホスト名

PPS はプロビジョニング
サーバと管理デバイスに認識されている必要がありますが、セキュリティ上の理由からネットワークで送信することはできません。PPS は (Intel AMT 構成画面に) デバイスに手動で入力して、この場合 System Manager 用のコア サーバでもあるプロビジョニング

サーバに格納する必要があります。PID/PPS ペアは System Manager
によって生成されて、データベースに格納されます。プロビジョニングで使用するために、生成された ID
ペアのリストを印刷できます。

IT 技術者はプロビジョニング サーバとして System Manager コア サーバの IP
アドレスを入力して、ポート 9982 を指定します。そうでない場合、デフォルトで Intel AMT
デバイスは構成サーバがポート 9971
をリッスンしている場合に受け取ることができる通常のブロードキャストを送信します。

Intel AMT
構成画面へアクセスするためのデフォルトのユーザ名とパスワードは、「admin」と「admin」です。これらはプロビジョニング
プロセス中に変更できます。ユーザ名は同じでもかまいませんが、パスワードは堅牢なものに変更しなければなりません。下の手順で説明されているように新しいユーザ名とパスワードの組み合わせが、System Manager
に付属するサービス設定ユーティリティの中に入力されます。各デバイスが設定された後なら、個々のデバイスごとにユーザ名/パスワードを変更できますが、プロビジョニングのためには [Configure Service] にあるユーザ名/パスワードを使用します。

Intel AMT
構成画面に上記情報を入力すると、デバイスはネットワークに初めて接続したときに「hello」メッセージを送信し、プロビジョニング サーバとの通信を試みます。このメッセージをプロビジョニング
サーバが受信すると、管理デバイスとの接続をサーバが確立した時にプロビジョニング
プロセスが始まります。

コア サーバが「hello」メッセージを受信して PID/PPS キーを検証すると、Intel AMT
デバイスをプロビジョンして、TLS モードにします。TLS (Transport Layer Security)
モードは、プロビジョニングが完了した時点でコア
サーバと管理サーバ間の安全な通信チャネルを確立します。このプロセスには、デバイスの UUID
と暗号化された資格情報を使ったデータベース内のレコード作成も含まれます。データベース内にデバイスのデータがある場合、そのデバイスは非管理デバイスのリストに表示されます。

Intel AMT デバイスがコア サーバによってプロビジョニングされると、Intel AMT
機能を使ってのみ管理できるようになります。非管理デバイスのリストから選択して、管理デバイスに追加することができます。また、System Manager
管理エージェントをデバイスに導入して、より多様な管理機能を使うことも可能です。

System Manager を使った Intel AMT 2 デバイスの推奨プロビジョニング
プロセスは、次のとおりです。項目 1 と 2 に固有の説明は、次の手順で説明されています。

1. サービス設定ユーティリティを実行して、Intel AMT
   デバイスのプロビジョニング用の新しい堅牢なパスワードを指定します。(下記の手順を参照。)
2. System Manager を使って、Intel AMT プロビジョニング ID (PID と PPS)
   のバッチを生成して、キーのリストを印刷します。(下記の手順を参照。)
3. デバイスの BIOS から Intel ME
   構成画面にログインして、既定のパスワードを堅牢なパスワードに変更します。

4. Intel AMT 構成画面にログインします。印刷したプロビジョニング ID のリストから、PID/PPS キーのペアを 1 つ入力します。コア サーバ (プロビジョニング サーバ) の IP アドレスを入力して、ポート 9982 を指定します。プロビジョニングに Enterprise モードが選択されていることを確認します。Intel AMT デバイスのホスト名を入力します。
5. BIOS 画面を終了すると、デバイスは「hello」メッセージを送信し始めます。
6. コア サーバが「hello」メッセージを受信して生成されたキーのリストに対して PID/PPS を確認します。一致するキー ペアがあれば、デバイスを TLS モードにプロビジョニングします。
7. デバイスが非管理デバイス検出リストに追加されます。
8. デバイスを選択して、管理デバイスに追加します。デフォルトではエージェントなしのデバイスとして管理されますが、管理エージェントをそのデバイスに導入することも可能です。

### Configure Service で Intel AMT ユーザ名とパスワードを設定するには

1. コア サーバで、[スタート]、[LANDesk]、[Configure Services] の順にクリックします。
2. [**Intel AMT 構成**] タブをクリックします。
3. [現在の Intel AMT 資格情報] のユーザ名とパスワードに「admin」と入力します。
4. [新しい Intel AMT 資格情報の提供] に新しいユーザ名 (オプション) と堅牢なパスワードを入力します。
5. [**OK**] をクリックします。

プロビジョニング ID のバッチを生成する前に、ここにユーザ名とパスワードを入力する必要があります。

### Intel AMT プロビジョニング ID のバッチを生成するには

1. コア サーバで、左側のナビゲーション ウィンドウにある [ハードウェア構成] をクリックします。
2. [AMT] を展開し、ツリーを [プロビジョニング][AMT ID 生成] までドリルダウンします。
3. 生成する ID の数を入力します (通常プロビジョニングを予定しているデバイス数)。
4. PID に異なる接頭辞を使用する場合には、[PID 接頭辞] テキスト ボックスに入力します。この接頭辞には、ASCII 文字セットの大文字アルファベットと数字のみが使えます。最大で 7 文字まで接頭辞に入力できます。
5. 生成 ID のグループを特定するバッチ名を入力します。
6. [生成された AMT ID を表示する] を選択すると、リスト内の生成された ID が表示されます。このボックスを選択しない場合、ID は生成されてデータベースに保存されますが、ここには表示されなくなります。
7. [ID 生成] をクリックします。
8. ID が生成された後に [ID リストの印刷] をクリックすると、ID リストの新しいウィンドウが開かれます。(現在リストに表示されている ID のみが新しいウィンドウに表示されます。)ブラウザの印刷機能を使ってリストを印刷します。
9. 前に生成された ID を表示するには、[バッチ名] ボックスを空白にしたままで [バッチ ID の表示] をクリックします。
10. あるバッチの生成された ID を表示するには、[バッチ名] テキスト ボックスにバッチ名を入力してから [バッチ ID の表示] をクリックします。

一度に任意の個数のプロビジョニング キーが生成できます。このキーは、今後新しい Intel AMT デバイスのプロビジョニングを行うときの参考としてデータベース内に格納されます。デバイスのプロビジョニングが完了して、プロビジョニング キーが消費されると、[AMT ID 生成] ページの消費済み ID が暗色表示されるので、どの ID が使用済みなのか追跡できます。

PID 接頭辞はその ID が PID であると判別しやすくするために追加されます。接頭辞の使用は必須ではありません。0 ～ 4 文字の使用を推奨しますが、最大で 7 文字まで接頭辞に使用できます。

プロビジョニング キーのバッチを特定するには、バッチ名を指定します。これは、ID を適用するデバイスを示す説明的な名前です。たとえば、会社の各部門ごとにバッチを生成して、それぞれのバッチを「Development」、「Marketing」、「Finance」などと名付けることができます。後で生成された ID を表示するには、バッチ名を入力してから [バッチ ID の表示] をクリックすると、該当する ID のみのリストが表示されます。

## 堅牢なパスワード

Intel AMT で安全な通信を有効にするには、堅牢なパスワードの使用が必要です。パスワードは次の条件を満たしている必要があります。

- 8 文字以上
- 1 文字以上の数字 (0-9) を含む
- 1 文字以上の英数字でない ASCII 文字 (!、&、% など) を含む
- ラテン文字の大文字と小文字の両方または非 ASCII 文字 (UTF+00800 以上) を含む

## プロビジョニング プロセス中のエラー

正しくペアになっていない PID と PPS を入力すると (たとえば PPS が別の PID とペアになっている)、アラート ログにエラー メッセージが表示されて、そのデバイスではプロビジョニングができなくなります。そのデバイスを再起動してから、Intel AMT 構成画面で正しい PID/PPS のペアを再入力する必要があります。

PID を入力した時 Intel AMT 構成画面にエラーメッセージが表示される場合、PID が誤って入力されています。その PID が正しいか確認するためににチェックサムが実行されます。

## Intel AMT 1.0 デバイスの検索

デバイス検索スキャンを実行すると、Intel AMT バージョン 1 デバイスが検出されて、[非管理] デバイス リスト内の [Intel AMT] フォルダに追加されます。デバイスは、製造元が設定した元のユーザ名とパスワードを置換して安全なユーザ名とパスワードに構成されている場合に、Intel AMT デバイスとして認識されます。

Intel AMT 構成画面で安全なユーザ名とパスワードを追加する時に、Intel AMT 2 デバイスの場合と同様に、プロビジョニング サーバの IP アドレスを入力してポート 9982

を指定することもできます。しかし、Intel AMT 1 デバイスのプロビジョニングには PID/PPS ペアは使われていません。プロビジョニング サーバの IP アドレスを指定すると、コア サーバがプロビジョニング サーバとして機能し、デバイスをエージェントなしのデバイスとして管理できます。

Intel AMT バージョン 1 ではバージョン 2 と同レベルのセキュリティは用いられていません。Intel は、バージョン 1 デバイスは外部から切り離された安全なネットワークで設定することを推奨しています。設定が完了した後で、バージョン 1 デバイスを管理する比較的安全でないネットワークに移動することができます。

# Intel* AMT デバイスのユーザ名とパスワードの変更方法

新しい Intel AMT (バージョン 1) デバイスのプロビジョニングには、セキュアなユーザ名とパスワードが必要です。System Manager で管理するデバイスの場合、Intel AMT 構成画面に入力したユーザ名とパスワードは、System Manager サービス設定ユーティリティで入力したものと同一である必要があります。サービス設定ユーティリティ内のユーザ名とパスワードはデータベースに保存されていて、Intel AMT デバイスのプロビジョニングでは全体的に適用されます。

Intel AMT で安全な通信を有効にするには、堅牢なパスワードの使用が必要です。パスワードは次の条件を満たしている必要があります。

- 8 文字以上
- 1 文字以上の数字 (0-9) を含む
- 1 文字以上の英数字でない ASCII 文字 (!、&、% など) を含む
- ラテン文字の大文字と小文字の両方または非 ASCII 文字 (UTF+00800 以上) を含む

プロビジョニングの後も IT メンテナンスの一部として定期的にユーザ名とパスワードを変更してください。各 Intel AMT デバイスに対して別々のユーザ名/パスワードの組み合わせを使用することも、複数のデバイスに 1 つのユーザ名/パスワードの組み合わせを使用することもできます。[ハードウェア構成] ページで入力した新しいユーザ名/パスワードの組み合わせはデータベースに保存され、System Manager が管理する Intel AMT デバイスとセキュアな通信を行うために使用されます。

**Intel* AMT デバイスのユーザ名とパスワードを変更するには**

1. コア サーバで、左側のナビゲーション ウィンドウにある [ハードウェア構成] をクリックします。
2. [AMT] を展開し、[構成] までドリルダウンします。
3. [すべてのデバイス] リストでユーザ名とパスワードを変更する 1 つ以上のデバイスを選択します。ツールバーの [ターゲット] をクリックします。
4. 下部ウィンドウにユーザ名を入力してから、パスワードの入力と確認入力を行います。

5. [ターゲット デバイス] をクリックしてから [適用] をクリックします。

   単一デバイスまたは同一リスト内の複数デバイスに対して、そのデバイスを選択して [選択したデバイス] をクリックしてから [適用] をクリックします。

# 回路ブレーカ ポリシーの設定

Intel AMT* 2.0 には、Intel AMT 2.0 の機能を持つデバイスでネットワーク セキュリティ ポリシーを施行する回路ブレーカが含まれています。管理デバイスの回路ブレーカ ポリシーは、**ハードウェア構成** ツールを使って選択および適用できます。

回路ブレーカ ポリシーが Intel AMT デバイスに適用されると、着信および送信ネットワーク パケットが定義されたポリシーに従ってデバイスによりフィルタされます。ネットワーク トラフィックがフィルタで定義されているアラート条件に一致するとアラートが生成され、デバイスのネットワーク アクセスがブロックされます。その後デバイスは、そのポリシーに従って修正されるまで、ネットワークから隔離されます。

System Manager には、Intel AMT デバイスに適用できる、あらかじめ定義された回路ブレーカ ポリシーが含まれています。各ポリシーには、許可しないネットワーク トラフィックの種類およびトラフィックがフィルタの条件と一致した場合にとるアクションを定義する一連のフィルタが含まれています。ポリシーを選択および適用するには、以下の手順に従います。

1. 1 つ以上の管理デバイスをターゲットにします。
2. 適用する回路ブレーカを選択します。必要に応じてポリシーを編集します。
3. ポリシーをターゲット デバイスに適用します。

回路ブレーカ ポリシーが管理デバイスでアクティブである場合は、デバイスはすべての着信および送信ネットワーク トラフィックを監視します。フィルタの条件が検出された場合は、以下のアクションが実行されます。

1. 管理デバイスにより ASF アラートがコア サーバに送信され、エントリがアラート ログに追加されます。
2. コア サーバにより、どのポリシーに違反しているかが判断され、管理デバイスのネットワーク アクセスをシャット ダウンします。
3. デバイスが回路ブレーカ修正キュー (**ハードウェア構成**ツール) にリストされます。
4. デバイスのネットワーク アクセスを復元するために、管理者は適切な修正手順に従い、デバイスを修正キューから削除する必要があります。この操作により、デバイスの元の回路ブレーカ ポリシーが復元されます。

この手順の詳細については、次のセクションが説明します。

# 回路ブレーカ ポリシーの選択および適用

System Manager に含まれている、Intel AMT
デバイスに適用できる、あらかじめ定義された回路ブレーカ
ポリシーは、以下の通りです。ポリシーは、ポート番号、パケット
タイプ、および特定時間内のパケット数などのパラメータで定義されています。ポリシーを有効にすると、選択したデバイスの Intel AMT に登録されます。ポリシーは、管理デバイスの CircuitBreakerConfig フォルダに XML ファイルとして保存されます。

- **BlockFTPSrvr:**このポリシーは、FTP ポート経由のトラフィックを阻止します。パケットが FTP ポート 21 で送信または受信されると、パケットはドロップされ、ネットワーク アクセスが停止されます。
- **LDCBKillNics:** このポリシーは、次の管理ポートを除くすべてのネットワーク ポートのトラフィックをブロックします。

| ポートの説明 | 番号の範囲 | トラフィックの方向 | プロトコル |
|---|---|---|---|
| LANDesk 管理 | 9593-9595 | 送信/受信 | TCP、UDP |
| Intel AMT 管理 | 16992-16993 | 送信/受信 | TCP のみ |
| DNS | 53 | 送信/受信 | UDP のみ |
| DHCP | 67-68 | 送信/受信 | UDP のみ |

このポリシーがデバイスに対して実際に適用されるのは、コア サーバが管理デバイスのネットワーク アクセスをシャット
ダウンするときです。デバイスが修正キューから削除されると、元のポリシーがデバイスに再度適用されます。

- **LDCBSYNFlood:**このポリシーは、SYN のサービス拒否 (Denial-Of-Service) 攻撃を検出します。1 分間に最高 10,000 の TCP パケットが許可され、SYN フラグがオンになります。その値を超えるとネットワーク アクセスが停止されます。
- **UDPFloodPolicy:**このポリシーは、UDP のサービス拒否 (Denial-Of-Service) 攻撃を検出します。0 ～ 1023 のポートで 1 分間に最高 20,000 の UDP パケットが許可されます。その値を超えるとネットワーク アクセスが停止されます。

**回路ブレーカ ポリシーを選択するには**

1. 左側のナビゲーション ペインで、[**ハードウェア構成**] をクリックします。
2. [**AMT**] をクリックし、ツリーを [**CB ポリシー**] までドリルダウンします。
3. デバイスのリストで、ポリシーを適用するデバイスを選択します (複数のデバイスを選択するには、[Ctrl] または [Shift] キーを押しながらクリックします)。

4. ツールバーの [**ターゲット**] をクリックして、デバイスを [**ターゲット デバイス**] リストに追加します。
5. 下のペインで、ポリシーをドロップダウン リストから選択します。
6. [**ターゲット デバイス**] をクリックし、[**適用**] をクリックします。

## 修正キューにあるデバイスに対するネットワーク アクセスを復元する

回路ブレーカ ポリシーによってデバイスのネットワーク
アクセスが停止されている場合、そのデバイスは修正キューにリストされます。
デバイスは、リストから削除されてそのデバイスのアクティブ
ポリシーが復元するまで、リストに残ります。デバイスをリストから削除する前に、デバイスがキューにリストされる原因となった問題を解決する必要があります。たとえば、FTP
トラフィックが検出された場合、デバイスで FTP
トラフィックを阻止するために適切なアクションがとられているかを確認する必要があります。

**デバイスを修正キューから削除するには**

1. 左側のナビゲーション ペインで、[**ハードウェア構成**] をクリックします。
2. [**AMT**] をクリックし、ツリーを [**CB 修正**] までドリルダウンします。
3. 元の回路ブレーカ ポリシーを復元するデバイスを選択し、[**削除**] をクリックします。

# Intel* AMT エージェント プレゼンス構成

Intel* AMT 2.0 には、管理デバイスにおけるソフトウェア エージェントの存在を監視できるエージェント プレゼンス セキュリティ ツールが含まれています。エージェント
プレゼンス監視機能を有効にすると、デバイスの管理エージェントが継続して実行され、エージェントが停止した場合にはほかのソフトウェア
ベースのエージェントが問題を検出できないときでもアラートで通知されます。

System Manager は Intel AMT エージェント プレゼンスを採用して 2
つのエージェントを監視します。監視するエージェントは標準の管理エージェントおよび監視サービスです。これは、正常の監視通信が利用できない場合などに便利です。たとえば、デバイスの通信レイヤーが機能していない、または監視エージェント自体が停止している場合などが考えられます。既定で、エージェント プレゼンスはその監視プロセスも監視し、プロセスが停止した場合はアラートで通知されます。

エージェント
プレゼンス監視は、デバイスの管理エージェントからの「ハートビート」メッセージをリッスンするタイマーを設定し、エージェントが実行されていることを確認します。ハートビート
メッセージを受信していないためタイマーの期限が切れた場合、アラートは Intel AMT によりコア
サーバに送信されます。

エージェント プレゼンス構成をセットアップするとデバイスのエージェントが Intel AMT
に登録され、ハートビートは直接 Intel AMT
へ送信されるようになります。ハートビートが停止すると、Intel AMT
によりアウトオブバンド通信を通じてデバイス エージェントが応答していないというアラートがコア

サーバへ送信されます。Intel AMT により、プラットフォーム イベント トラップ (PET) アラートがステータスの変更についての説明と一緒にコア サーバへ送信されます。既定では、このアラートはデバイスのヘルスと共にログされます。このアラートが受信されたときに開始する別のアラート アクションを設定することもできます (アラート アクションの設定については、「アラート アクションの設定」を参照してください)。

エージェント プレゼンス監視を設定すると、2 つのエージェントの監視を有効または無効にし、以下の値を設定できます。

- **ハートビート**:ハートビート信号間の最大間隔 (秒)。この制限時間内に新しいハートビートが受信されない場合、エージェントが応答していないと判断されます。既定の値は、標準の管理エージェントで 120 秒、監視サービスで 180 秒です。最低値はいずれの場合も 30 秒です。
- **起動時** :オペレーティング システムの起動後、エージェントからハートビートを受信するまでの最大間隔 (秒)。この制限時間が経過すると、エージェントが応答していないと判断されます。エージェント プレゼンスはエージェントがインストールされている Intel AMT で設定します。そのため、エージェントが実行されてから最初のハートビートが送信されるまで、若干の時間がかかることがあります。既定の値は 360 秒で、最低値は 30 秒です。

**Intel AMT エージェント プレゼンス構造を編集するには**

1. 左側のナビゲーション ペインで、[**ハードウェア構成**] をクリックします。
2. [**AMT**] を展開し、ツリーを [**AP 構成**] までドリルダウンします。
3. Intel AMT 2.0 デバイスでエージェント プレゼンス監視を無効にするには、[**エージェントの存在監視を有効にする**] チェックボックスをオフにします。
4. 特定のエージェントに対する監視を無効にするには、該当のエージェント名の横にあるチェックボックスをオフにします。(これらのチェックボックスが両方ともオフになっていても、エージェント プレゼンスによるエージェント プレゼンス自体の監視プロセスは、エージェント プレゼンスが有効になっている限り、継続して監視されます。)
5. ハートビート間の最大間隔を変更するには、[**Heartbeat**] テキスト ボックスに新しい値を入力します (最低 30 秒間)。
6. デバイスでオペレーティング システムの起動後エージェントによって最初のハートビートが送信されるまでの最大待機時間を変更するには、新しい値を [**開始時刻**] テキスト ボックスに入力します (最低 30 秒間、120 秒間を推奨します)。

# IPMI サポート

System Manager には、Intelligent Platform Management Interface (IPMI) 1.5 および 2.0 のサポートが組み込まれています。IPMI は、管理可能なハードウェアにアクセスするためのメッセージとシステム インターフェイスを定義するために、Intel、* H-P、* NEC、* および Dell *

が開発、規格化した仕様です。IPMI には、コンピュータのオン/オフまたは OS の動作状態に関係なく、多くの機能へのアクセスを可能にする監視と復旧機能が含まれています。

IPMI 監視は、BMC (Baseboard Management Controller) が処理しています。BMC は、スタンバイ電源で動作し、システムのヘルスステータスを自動的にポーリングします。イベントのログ記録、アラートの生成、システム電源のオフまたはリセットなどの自動復旧アクションの実行など、BMC が障害の発生を検知したときに IPMI が行う処理を設定できます。

システム上で BMC を検知するように、SMBIOS 2.3.1 以降をインストールしておく必要があります。BMC が検知されないと、レポートやエクスポートなどにおける IPMI 情報を確認できなくなる場合があります。

IPMI は、温度や電圧、ファン、電力供給、シャーシ侵入などの物理ヘルス特性を監視するのに使用されるハードウェアへの共通インターフェイスを定義します。ヘルス監視に加え、IPMI には、自動アラート、自動システムシャットダウンと再起動、リモート再起動と電源制御機能、資産追跡などのその他のシステム管理機能が含まれています。

オペレーティング システムの状態によって、IPMI 対応デバイスに対する System Manager メニューオプションが若干異なります。

## IPMI 対応デバイス機能の管理

監視機能は、監視対象のデバイスの状態や、デバイスに何がインストールされているかによって異なります。Baseboard Management Controller (BMC) を搭載した IPMI 対応デバイスへの管理者コンソールからの監視には、いくつかの制限があります。たとえば、BMC の設定後に管理エージェントを追加することはできません。これには、デバイスの電源がオフまたは OS が機能していない場合のアウト オブ バンド管理が含まれます。管理エージェントをインストールし、BMC が存在し、デバイスの電源がオンになり、OS が機能していると、すべての管理機能が使用可能になります。以下のテーブルは、これらの異なる構成で使用できる機能を比較したものです。

| | BMC のみ* | BMC + エージェント | エージェント (IPMI なし) |
|---|---|---|---|
| アウト オブ バンド 管理の有効化 | /X= | /X= | |
| イン バンド管理の有効化 | | /X= | /X= |
| デバイスが検出可能** | /X= | /X= | /X= |
| 環境センサーの読み取り | /X= | /X= | ハードウェア依 |

| | BMC のみ* | BMC + エージェント | エージェント (IPMI なし) |
|---|---|---|---|
| | | | 存 |
| リモートでの電源のオン/オフの切り替え | /X= | /X= | /X= |
| イベント ログの読み取り/クリア | /X= | /X= | |
| アラートの構成 | /X= | /X= | /X= |
| OS 情報の読み取り | | /X= | /X= |
| 安全なシャットダウン | | /X= | /X= |
| SMBIOS 情報 (プロセッサ、スロット、メモリ) の読み取り | | /X= | /X= |
| IP シンク (OS と BMC 間) | | /X= | |
| ワッチドッグ タイマ | | /X= | |
| BMC によるコア サーバとの通信 | /X= | /X= | |
| ローカル System Manager コンポーネントとコア サーバの通信 | | /X= | /X= |
| すべての System Manager 管理機能 | | /X= | |

*標準 BMC。mini BMC は、Baseboard Management Controller を小型化したバージョンです。mini BMC では上記の機能が備えられていますが、以下のような制約があります。

- Serial Over LAN (SOL) リダイレクションをサポートしていません。
- BMC 管理に対して 1 人のユーザ名しか指定できません。

- BMC との通信用に 1 つのチャンネルしか使用できません。
- システムのイベント ログ (SEL) のレポジトリが小規模です。

** BMC が構成済みでない場合、BMC は IPMI 検出のために本製品が使用する ASF ping に応答しません。つまり、通常のコンピュータとして検出されることになります。管理エージェントを導入するときに、サーバ構成実行ファイルがシステムをスキャンして IPMI を検出し、BMC を構成します。

## 他の IPMI ドライバとの競合

System Manager と共に管理するデバイス上に IPMI ドライバを含む別の管理ソフトウェアをインストールした場合、IPMI 管理機能を持つ Management Suite エージェントを導入する前にこれらの製品をアンインストールする必要があります。

たとえば、Microsoft* Windows* Server 2003 には IPMI サポート機能が含まれています。これは Windows Management Instrumentation (WMI) プロバイダと IPMI ドライバを含む Windows Remote Management (WinRM) のインストールによって導入されます。しかし、System Manager ではこの IPMI ドライバのインストールをサポートしておらず、自身の IPMI ドライバをインストールします。WinRM が System Manager で管理するデバイス上にインストールされている場合、最初に WinRM を Windows の [プログラムの追加と削除] からアンインストールする必要があります ([スタート]、[コントロール パネル]、[プログラムの追加と削除]、[Windows コンポーネントの追加と削除]、[管理とモニタ ツール] の順にクリックして、[ハードウェア コンポーネント] のチェックボックスを外し、[OK] をクリックします)。

# IPMI BMC 構成

[IPMI BMC 構成] ページでは、IPMI対応デバイスとの通信の設定をカスタマイズします。次に説明する機能は、インバンドデバイスで使用できます。デバイスがアウト オブ バンドの場合は、電源構成とBMC ユーザ設定のみを使用できます。

---

**警告** : IPMI 仕様を熟知しており、これらの設定に関係するテクノロジを理解しているユーザ以外は、IPMI 設定の変更は行わないでください。これらの設定オプションを誤って使用すると、System Manager が IPMI 対応デバイスと正しく通信できなくなる場合があります。

---

次の構成オプションを使用できます。

- ワッチドッグ タイマ
- 電源構成
- ユーザ設定
- BMC パスワード
- LAN 構成
- SOL 構成
- IMM 構成の変更

## ウォッチドッグ タイマの設定の変更

IPMI には、BMC ウォッチドッグ
タイマのインターフェイスがあります。このタイマは、定期的に期限切れになるように設定したり、期限がくると特定のアクション (パワー サイクルなど) を起動するように設定したりすることができます。System Manager
は、期限切れにならないように定期的にタイマをリセットするように設定されています。デバイスが利用不可になると
(電源がオフになっているまたはハングしているなど)、タイマはリセットされずに期限切れとなり、アクションが起動されます。

タイマが期限切れになるまでの時間を指定し、期限切れになった際のアクションを選択できます。何のアクションもとらない、デバイスのハード リセット
(シャットダウンしてから再起動)、正常にデバイスの電源をオフにする、パワー サイクル
(正常に電源をオフにしてから再起動する) を実行する、などを選択できます。

また、生成されるネットワーク トラフィックの量を減らすウォッチドッグ タイマ有効時に BMC の ARP
(Address Resolution Protocol : アドレス解決プロトコル)
メッセージのブロードキャストを停止することもできます。ARP を中断した場合、ウォッチドック
タイマが期限切れになると、自動的に再開します。

**ウォッチドッグ タイマの設定を変更するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。
3. [IPMI BMC 構成] を展開し、[ウォッチドック タイマ] をクリックします。
4. [ウォッチドッグ タイマをオンにする] を選択してタイマを有効にします。
5. タイマをチェックする頻度を指定します (秒または分)。
6. ウォッチドッグ タイマが期限切れになった際に起動するアクションを選択します。
7. ウォッチドッグ タイマ有効時に BMC の ARP
   メッセージのブロードキャストを停止する場合は、[BMC ARP を停止] を選択します。
8. [**適用**] をクリックします。
9. ウォッチドッグ タイマの設定を変更している場合、[既定値の復元]
   をクリックすると既定の設定に戻すことができます。

## 電源構成の設定変更

IPMI
が有効なコンピュータで電源供給が停止した場合、電源復旧時に実行する動作を指定できます。電源が停止したときの状態にコンピュータを復元することを推奨しますが、電源をオフの状態のままにしたり、常にコンピュータを起動する設定を選択することも可能です。

**電源構成の設定を変更するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。

2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。
3. [IPMI BMC 構成] を展開し、[電源構成] をクリックします。
4. 電源が復旧した際のオプションを選択します。
5. [**適用**] をクリックします。
6. 電源構成の設定を変更している場合、[既定値の復元] をクリックすると既定の設定に戻すことができます。

## BMC ユーザ設定の変更

System Manager は、BMC に固有の (他の System Manager ユーザ名と区別された) ユーザ名とパスワードの組み合わせで BMC に認証されます。System Manager では最初のユーザ名が予約されており、必ず BMC の通信に使用されます。BMC で他のユーザ名の定義が許可されている場合は、BMC 認証のためのユーザ名とパスワードを定義できます。

また、個々のユーザの権限レベルも指定できます。アドバンスト IMM の場合、各チャネルのプロトコル権限レベル (telnet、http、および https) の指定もできます。

---

**警告**： この設定への変更には十分注意してください。誤った設定により、本製品とデバイスの BMC 通信が無効になることがあります。

---

**BMC ユーザ設定を変更するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。
3. [IPMI BMC 構成] を展開し、[ユーザ設定] をクリックします。
4. ユーザ名のデータをクリアするには、インデックス番号をクリックしてから [クリア] をクリックします。
5. ユーザ名を追加または変更するには、インデックス番号をクリックして [編集] をクリックします。
6. ユーザ名を入力します。
7. パスワードを設定するには、[パスワードの設定] チェックボックスを選択して、パスワードを入力し、入力の再確認を行います。
8. LAN およびシリアル アクセスの権限レベルを選択します。
9. [変更内容の保存] をクリックします。

## BMC パスワードの変更

System Manager は、既定のユーザ名 (ユーザ 1) とパスワードを使用してデバイスの BMC に認証します。ユーザ名を変更することはできませんが、パスワードは変更できます。このパスワード設定を変更すると、変更内容はデータベースと BMC に保存されます。

**既定の BMC パスワードを変更するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。

3. [IPMI BMC 構成] を展開し、[パスワード] をクリックします。
4. 新しいパスワードを入力し、確認します。
5. [**適用**] をクリックします。

## LAN 構成の変更

IPMI メッセージは、デバイスのシステム インターフェイスに加え、LAN インターフェイスを使って直接 BMC から送信できます。LAN 通信を有効にすることにより、コア
サーバはデバイスの電源がオフになっている場合でも、IPMI
専用のアラートを受信できるようになります。デバイスに有効なネットワーク
アドレスがあってネットワークに物理的に接続しており、デバイスの主要電源が接続したままの状態である限り、コア サーバはデバイスとの通信を維持できます。

---

**警告** :BMC との LAN
通信またはシリアル通信のカスタム構成を設定する場合、この設定への変更には十分注意してください。誤った設定により、本製品とデバイスの BMC 通信が無効になることがあります。

---

LAN チャネルが定義されている場合、デバイスの BMC に既定の設定を使用するか、IP
アドレスとゲートウェイ設定を変更することができます。これらのオプション使って、各プラットフォーム イベント トラップ (PET) イベントに対して、BMC による SNMP トラップの送信先を設定します。

また、LAN 経由でアラートを送信するための SNMP
コミュニティ文字列を変更することができます。このような設定を行う場合、SNMP 認証で使う SNMP コミュニティ文字列を指定する必要があります。個々の構成に対して、トラップ送信先情報を編集して、トラップの送信先と送信方法、通知するかどうかを指定します。

**LAN チャネル構成のプロパティを設定するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。
3. [IPMI BMC 構成] を展開し、[LAN 構成] をクリックします。
4. LAN 通信のドロップダウン リストから [常に利用可能] を選択して、BMC
   へのアクセスを開いたままにします。[無効] を選択すると、デバイスがアウトオブバンドの時に BMC への LAN アクセスがなくなります。
5. チャネルに対するユーザの権限レベルを選択します。[管理者レベル]
   はすべてのコマンドにアクセスがあり、[ユーザ レベル] は読み取り専用アクセスに制限されます (ユーザ レベルを選択すると、機能セットが制限されます)。
6. [BMC ARP の電源を永久にオフにします] を選択して、BMC から ARP (Address Resolution Protocol : アドレス解決プロトコル)
   メッセージをオフにします。これによりネットワークのトラフィックを減少させられますが、デバイスがアウトオブバンドの時に BMC での通信が妨げられます。
7. [ARP の応答をオフにする] を選択して、OS が利用できない時に BMC がARP
   メッセージの応答を送信するのを止めさせます。この設定を有効にすると、デバイスがアウトオブバンドの時に BMC での通信が妨げられます。

8. BMC が OS チャネルと同期している場合、LAN チャネルの IP
   設定は自動的に設定されます。そうでない場合には、[IP 設定]
   タブのチェックボックスが有効になっています。このボックスを選択したままにしておいて DHCP
   設定を自動的に取得するようにするか、またはボックスのチェックマークを外して静的設定を使ってテキスト
   フィールドを編集することもできます。通常は自動設定を使用することが推奨されます。
9. [LAN でアラートを送信] タブをクリックして、SNMP コミュニティ文字列設定を設定します
   (詳細は下記を参照)。
10. [適用] をクリックして変更内容を保存します。

**[LAN でアラートを送信] プロパティを変更するには**

1. [LAN 構成] ページを開きます (上記手順 1-3)。
2. [LAN でアラートを送信] タブをクリックします。
3. [有効] チェックボックスを選択して、SNMP アラートの送信を有効にします。
4. SNMP 認証で使用する [SNMP コミュニティ文字列] を指定します。
5. トラップ送信先を設定するには、インデックス番号をダブルクリックして [プロパティ]
   ダイアログを開きます。
6. BMC のアラートの送信先 IP アドレス、対応する MAC アドレスを指定します。
7. 試行回数、試行の頻度、および使用する優先ゲートウェイを指定します。
8. アラートを受領確認するには (確認を選択するとネットワーク
   トラフィックの量が増加します)、[アラートを受領確認します] チェックボックスを選択します。
9. [**OK**] をクリックします。
10. すべての設定が完了したら、[LAN 構成] ページで [適用] をクリックします。

## Serial Over LAN (SOL) 構成の変更

SOL (Serial Over LAN) 構成オプションを使って、BIOS POST メッセージのシリアル
ポートへの転送など、特別な用途のためにシリアル
モデムの設定をカスタマイズします。モデム接続経由でダイアルするのに BMC
が必要な場合には、初期化文字列とダイアル文字列などの特別なモデム設定を指定する必要があります。

シリアル モデムの設定については、デバイス ボードの BIOS
およびジャンパ設定を構成する必要があります。詳細については、それぞれのデバイスのマニュアルを参照してください。

---

**警告** :BMC との LAN
通信またはシリアル通信のカスタム構成を設定する場合、この設定への変更には十分注意してください。誤った設定により、本製品とデバイスの BMC 通信が無効になることがあります。

---

**SOL 構成の設定を変更するには**

1. [**マイ デバイス**] ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、[ハードウェア構成] をクリックします。

3. [IPMI BMC 構成] を展開し、[SOL 構成] をクリックします。
4. [シリアルオーバー LAN 通信をオンにする] を選択して SOL を有効にします。
5. [SOL のアクティブ化に必要なユーザ レベル] で最低レベルを選択します。
6. デバイスのハードウェア構成に適切な [SOL セッションのボー レート] を選択します。
7. [**適用**] をクリックします。

## IMM 構成の変更

**[IMM 構成]** ページは、拡張 IMM アドイン カードが装備された IPMI 対応デバイスでのみ表示されます。このページのオプションを使うと、IMM 対応デバイスで使用するプロトコルと機能の有効/無効を切り替えられます。これらの設定に変更を加える前に、製造元の IMM のマニュアルをよく読んでください。

**IMM 構成の設定を変更するには**

1. **[マイ デバイス]**ビューで、設定するデバイスをダブルクリックします。
2. サーバ情報コンソールの左側のナビゲーション ペインで、**[ハードウェア構成]**をクリックします。
3. **[IPMI BMC 構成]**を展開し、**[IMM 構成]**をクリックします。
4. 有効にするプロトコルと機能のチェックボックスを選択して、必要な設定を加えます。オプションは、次のとおりです。
   - KVM
   - SNMP
   - telnet
   - SMTP アラート
   - HTTP
   - HTTPS
5. **[適用]**をクリックします。

## Dell* DRAC デバイスの管理

本製品には、Dell* DRAC (Remote Access Controller) のあるデバイスとの管理統合機能が含まれています。DRAC は、Dell のデバイス上の IPMI 対応サーバ管理ハードウェアに対するインターフェースを提供するリモート ハードウェア コントローラです。DRAC には IP アドレスが割り当てられており、デバイス検索時とデバイス管理時に DRAC デバイスを特定するために使用されます。

Dell DRAC のあるデバイスは、他の IPMI 対応デバイスと同様の機能性で管理することが可能です。デバイスが検出されて管理デバイスのリストに追加されたとき、他の IPMI 対応デバイスと同様に管理されます。また、System Manager にはユニークな Dell DRAC の機能があります。

OpenManage Server Administrator は、Dell DRAC デバイスの管理用に Dell より提供されている Web ベースのコンソールです。通常これは、ブラウザに DRAC の IP

アドレスを入力し、ユーザ名とパスワードを使ってログインしてアクセスします。Dell DRAC デバイスが System Manager で管理されている場合、このユーティリティを System Manager インターフェースから直接開くこともできます。

さらに、System Manager では OpenManager Server Administrator へのアクセス用ユーザ名とパスワードの管理も行うことができ、またサーバ情報コンソールにこのユーティリティからの 3 つのログを表示します。

**Dell DRAC デバイス用の OpenManage Server Administrator を開くには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [ハードウェア] を展開してから [Dell DRAC] をクリックします。デバイスの IP アドレスと他の特定情報が表示されます。
3. [Dell DRAC ユーティリティを起動] をクリックして、新しいウィンドウにそのデバイスの OpenManage Server Administrator を開きます。

## Dell DRAC のログは System Manager で利用可能です。

OpenManage Server Administrator ユーティリティの 3 つのログは、System Manager サーバ情報コンソールに表示されます。

- **Dell DRAC ログ** : ログイン アクティビティ、セッション ステータス、ファームウェアの更新ステータス、DRAC と他のデバイス コンポーネントとの通信など、Server Administrator が記録するすべてのイベントを追跡します。System Manager に表示される情報には、イベントの重要度、説明、エラーの推奨修正方法などが含まれます。
- **Dell DRAC コマンド ログ** : Server Administrator に発行されるすべてのコマンドを追跡します。実行されたコマンド、実行者、実行日時が表示され、ログイン試行とログアウト試行、およびアクセス エラーも含まれます。
- **Dell DRAC トレース ログ** : アラート、ページング、または DRAC からのネットワーク接続などネットワーク通信イベントに関する詳細の追跡に役立ちます。

**Dell DRAC デバイスのログを表示するには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [ログ] を展開します。
3. [Dell DRAC ログ]、[Dell DRAC コマンド ログ]、または [Dell DRAC トレース ログ] をクリックします。

## Dell* DRAC 対応デバイスのユーザ名の管理方法

OpenManage Server Administrator インターフェースにアクセスするには、そのデバイスで定義されているユーザ名とパスワードを使ってログインします。デフォルトの **root**

ユーザは、リストの最初のユーザであり、削除することはできません。しかし、パスワードを変更することはできます。15 人までユーザを追加できます。DRAC のユーザ名には異なるアクセス
レベルを付与できますが、System Manager は管理者レベルのユーザ名のみを定義できます。

**DRAC が有効なデバイスのユーザ名とパスワードを追加または編集するには**

1. [すべてのデバイス] リストでデバイスをダブルクリックします。
2. サーバ情報コンソールで [ハードウェア構成] をクリックします。
3. ハードウェア構成コンソールで [Dell DRAC 構成] を展開してから [Dell DRAC ユーザ] をクリックします。現在定義済みのユーザのリストが表示されます。
4. ユーザのパスワードを変更するには、ユーザ番号をクリックし、[パスワードを変更] をクリックします。新しいパスワードの入力と確認入力を行ってから、[適用] をクリックします。(複数のユーザに同じパスワードを割り当てるには、Ctrl キーを押しながらクリックするか、Shift キーをクリックしながら選択します。)
5. ユーザを追加するには、[ユーザの追加] をクリックします。ユーザ名とパスワードを入力し、そのパスワードの確認入力を行ってから、[適用] をクリックします。ユーザがリストに追加されます。

   **注意**:
   既にリスト内にあるユーザ名を入力した場合には、指定した新しいパスワードがそのユーザ名の既存のパスワードを上書きするので、リストに同じユーザ名で 2 人目のユーザが追加されることはありません。

6. ユーザを削除するには、ユーザ番号をクリックして [ユーザの削除] をクリックし、それから [OK] をクリックします。(複数のユーザを削除には、Ctrl キーを押しながらクリックするか、Shift キーをクリックしながら選択します。)

このリストのすべてのユーザは、OpenManage Server Administrator に管理者レベルのアクセス権があります。

# コア データベースのインストールとメンテナンス

## コア データベースのインストール

本製品の既定のインストールは、コア サーバの Microsoft MSDE
データベースをインストールします。これは System Manager に対して使用できる唯一のデータベース
オプションで、インストールできるコア データベースは 1 つだけです。データベースはスタンドアローン
サーバのみにインストールする必要があります。

データベース スキーマは Microsoft SQL Server 2000 の SP4
をサポートしています。すべてのデータベース サーバに MDAC 2.8
がインストールされている必要があります。

コア
サーバにインストールされているデータベースは、新しいデータベースである必要があります。System
Manager を以前 LANDesk® Management Suite または Server Manager
がインストールされていたサーバにインストールする場合、既存のデータベース構造を System Manager
のインストールに使用することはできません。

LANDesk Configure Services
ユーティリティには、各種のサービスを設定できるインターフェイスがあります。このユーティリティの
[全般] タブには、現在のサーバ名、データベース名、およびコア
データベースへのアクセスに必要なユーザ名/パスワードが表示されます。これらの資格情報は、コア
データベースにアクセスするすべてのサービスが使用しています。System Manager は 1 つのコア
データベースしか使用できないので、サーバ名またはデータベース名を変更する必要はありません。資
格情報は必要に応じて変更できます。詳細については、「付録 C : サービスの設定」を参照してください。

# 付録 A :システム要件とポートの使用

コアには、静的 IP アドレスが必要です。



## 管理コア サーバ

管理コア サーバでは、次のオペレーティングシステムがサポートされています。

- Microsoft Windows 2000 Server (SP4)
- Microsoft Windows 2000 Advanced Server (SP4)
- Microsoft Windows 2003 Server Standard Edition (SP1)
- Microsoft Windows 2003 Server Enterprise Edition (SP1)

## サーバ サポート (エージェント)

- Microsoft Windows 2000 Server (SP4)
- Microsoft Windows 2000 Advanced Server (SP4)
- Microsoft Windows 2000 Professional (SP4)
- Microsoft Windows 2003 Server Standard Edition x86 (SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (SP1)
- ~~Microsoft Windows XP Professional (SP2)~~
- ~~Microsoft Windows XP Professional x64 (SP2)~~
- Windows Small Business Server 2000 (SP4)
- Windows Small Business Server 2003 (SP1)
- Red Hat Enterprise Linux v3 (ES) 32-bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32-bit - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32-bit - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32-bit - U2

- Red Hat Enterprise Linux v4 WS EM64t – U2
- SUSE* Linux Server 9 ES 32-bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE* Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

## ブラウザ

- Microsoft Internet Explorer 6.x (SP1)
- Mozilla 1.7 以降
- Firefox 1.5 以降

## データベース

- MSDE (SP4)

### Microsoft Data Access Component

- MDAC 2.8 以降

2 つ以上の LANDesk
管理製品で同じデータベースを使用する場合、両方の製品を同じ「コア」コンピュータにインストールする必要があります。複数の製品を同じ「コア」コンピュータ上にインストールする場合、同じデータベースを使用する必要があります。両方の製品で同じデータベースを使用する場合、両方の製品のバージョンを 8.70 にする必要があります。

# ポートの使用

## はじめに

ファイアウォール (またはトラフィックをフィルタするルータ)
のある環境で本製品を使用する場合、この製品が正しく機能するためには、ファイアウォールまたはルータの設定を調整する必要があります。このセクションでは、製品の各種コンポーネントによって使用されるポートについて説明します。ここで説明する内容は、ルータおよびファイアウォールを設定する際に必要になる情報で、各サブネット内でローカルにのみ使用するポートについての説明は除外します。

## ファイアウォール規則の基礎知識

この情報はファイアウォール規則の設定に関するものです。ファイアウォール規則の設定という主題に馴染みがないユーザは、このセクションを読んで、主なコンセプトの基礎を理解してください。

## ファイアウォール規則

「ポートを開く」というのは、正確な表現ではありません。単にファイアウォールに行って任意のポートを開くことはできません。ポートを開くとは、ファイアウォール規則を設定することを端的に示した表現です。ファイアウォール規則では、ファイアォールを通過することを許可するトラフィックと許可しないトラフィックを規定します。ファイアウォール規則は、ポート番号上のトラフィックをフィルタするだけではありません。規則は、プロトコル、発信元のポート番号と宛先のポート番号 (インバウンド/アウトバウンド)、送信元の IP アドレスと送信先の IP アドレスなどに基づいて設定できます。

一般的なファイアウォール規則を以下に示します。「TCP ポート 9535 上の インバウンド トラフィックを許可します。」本製品を使用するためには、リモート コントロールをサポートするためにこの規則が必要になります。この規則は、次の 3 つの要素に基づきます。

1. プロトコル (TCP または UDP)
- ポート番号
- 方向 (インバウンドまたはアウトバウンド)

ファイアウォール規則を設定するためには、これらの 3 つの要素が必須となります。

## 発信元と宛先ポート、および動的ポート

TCP または UDP 通信には、常に 2 つのポートが関係します。すべての TCP パケットまたは UDP パケットは、発信元ポートから宛先ポートに送られます。ファイアウォール規則は、発信元ポートまたは宛先ポート、あるいはその両方のポートに基づいて設定できます。このようにドキュメント内に一覧されるポートは、常に宛先ポートです。

5007 (インベントリ サービスが使用) などのよく知られたポートは、通信の片側のみを表します。通信のもう一方の側では、動的ポートを使用します。動的ポートは、オペレーティング システムによって 1024 ～ 5000 の範囲に自動的に割り当てられます。

## ファイアウォールと UDP トラフィック

TCP トラフィックがファイアウォールを通過することを許可するには (たとえば、ポート 5007 へのインバウンドの TCP 接続を許可するには)、ひとつの規則で十分です。TCP 接続を確立すると、データは双方向に接続を通過できます。

UDP トラフィックは、コネクションレスであるため、これとは異なります。たとえば、コア サーバは、既定で、タスクの開始前に UDP ポート 38293 でデバイスに対して「ping」します。ポート 38293 への送信 UDP パケットを許可するファイアウォール規則では、パケットはコア サーバからファイアウォールの外のデバイスにパケットを送ることができます。ただし、デバイスの応答パケットは送れません。

ポート 38293
への送信パケットと受信パケットの両方を許可するファイアウォール規則では、よく知られたポートを通信の片側のみがリッスンするため、どちらか一方の通信が動作しなくなります。もう一方の側の通信は動的ポートを使用します。コア サーバの送信パケットは動的ポートからポート 38293
に送られるため、デバイスの応答パケットは、ポート 38293 からポート 38293
でなく、同じ動的ポートに送られます。 両方向の通信を許可するには、発信元ポートまたは宛先ポートを 38293 に設定した UDP パケットを許可する規則が必要になります。このような規則は、すべての UDP ポートへのインバウンド
パケットを許可するため、通常、イントラネットでは使用されますが、外部のファイアウォールでは使用されません。

こうした理由から、一般に UDP
トラフィックは「ファイアウォールに適していない」とみなされます。もう一度先ほどの例を考えてみると、UDP ポート 38293 に代わってTCP ポート 9595
を使用できます。ファイアウォールを越えてデバイスを管理するときには、TCP
ポートを使用するように製品を構成することを検討するはずです。

## 使用されるポート

| ポート | 方向 | プロトコル | サービス |
|---|---|---|---|
| 31770 | コンソールからデバイスへ、デバイスからコアへ | TCP | コンソールとデバイス間の通信 |
| 9595, 9594 | コンソールからデバイスへ | TCP | サーバ構成 |
| 9595 | コンソールからデバイスへ | UDP | 検索 |
| 623 | コンソールからデバイスへ | UDP | ASF、IPMI 検索 |
| 5007 | コンソールからデバイスへ | TCP | インベントリ |
| 9535 | コンソールからデバイスへ | TCP | リモート コントロール |
| 139, 145 | コンソールからデバイスへ | TCP | ファイルとプリンタの共有 |

| ポート | 方向 | プロトコル | サービス |
|---|---|---|---|
| 137, 138 | コンソールからデバイスへ | UDP | ファイルとプリンタの共有 |

本製品でノードを管理するには、インストール済みの標準の管理エージェントでノードを検索する必要があります。検索には、UDP ポート 9595
が使用されます。手動で個々のデバイスをコンソールに追加することもできますが、このためには、デバイスが UDP ポート 9595
の「ping」に応答する必要があります。コンソールとデバイスの間の通信は、TCP ポート 31770 と 6787 を使用します。後者のポート上のトラフィックは、HTTP ベースです。ASF (Alert Standard Forum)
検索の場合、UDP ポート 623 が使用されます。また、リモート コントロールについては、TCP ポート 9535 を使用します。IPMI 検索は、ASF 検索とリンクされていて、同じポート (UDP/623) を使用します。

# 付録 B : コア サーバのライセンス認証

コンソールを使用するには、まずコア サーバの使用開始ユーティリティを使用してコア
サーバのライセンス認証を行う必要があります。この操作は、通常は追加ライセンスを購入するたびに
一度だけ実行する必要があります。コア サーバの使用開始
ユーティリティは、次のことを実行するために使用します。

- 使用開始時に新しいサーバのライセンスを認証する
  既存のコア

サーバを更新する、試用ライセンスから通常のライセンスに切り替える、Management Suite
にアップグレードする、または Server Manager。
45 日の試用ライセンスで新しいサーバのライセンスを認証する

[**スタート**]、[**プログラム**]、[**LANDesk**]、[**コア サーバの使用開始**]
の順にクリックし、ユーティリティを起動します。コア
サーバがインターネットに接続していない場合は、このセクションの「手動によるコア
サーバのライセンス認証とノード カウント データの確認を参照してください。

各コア サーバは、そのコア サーバに固有の認可された証明書を持つ必要があります。複数のコア
サーバは、同じ LANDesk アカウントに対してノード
カウントを検証することはできますが、同じ認可証明書を共有することはできません。
このユーティリティは、System Manager インストール後の最初の再起動時に自動的に実行されます。

定期的に、コア サーバはノード カウントの検証情報を「¥Program Files¥LANDesk¥Authorization
Files¥LANDesk.usage」ファイル内生成します。このファイルは、定期的に LANDesk Software ライセンス
サーバに送信されます。このファイルは XML
形式で、電子署名が済んでおり、暗号化されています。このファイルに手動で変更を加えると、ファイル
の内容と LANDesk Software ライセンス サーバに対する次の利用状況レポートが無効になります。

コア サーバは、HTTP で LANDesk Software ライセンス サーバと交信します。プロキシ
サーバを使用している場合は、ユーティリティの [**プロキシ**]
タブをクリックし、プロキシ情報を入力します。コア
サーバがインターネットに接続している場合、ライセンス
サーバとの交信は自動で行われ、手動による操作は必要ありません。コア
サーバが接続されていない場合は、再起動時に [**Close**]
をクリックし、認証ファイルを「licensing@landesk.com」へ電子メールで送信してください。

---

コア サーバの使用開始
ユーティリティは、ダイアルアップによるインターネット接続を自動で起動しません。ダイアルアップ接続を
手動で起動してライセンス認証ユーティリティを実行した場合は、ライセンス認証ユーティリティはダイア
ルアップ接続を使用して利用状況のレポートを送信することができます。

コア サーバがインターネットに接続していない場合は、このセクション内で後でふれるようにノード
カウントを手動で検証して送信することができます。

---

## LANDesk Software アカウントを使ったサーバのライセンス認証

標準ライセンスで新しいサーバのライセンスを認証する前に、LANDesk Software 製品と購入したノード数についてライセンスを認証するアカウントを LANDesk Software でセットアップする必要があります。サーバのライセンスを認証するには、アカウント情報 (ユーザ名とパスワード) が必要となります。この情報がない場合は、LANDesk Software のセールス担当者までお問い合わせください。

製品をインストールしてからコア サーバのライセンスを認証するまでの間に、コア サーバの日時を変更しないでください。変更するとライセンス認証に失敗します。その場合は、製品をアンインストールしてから再インストールする必要があります。

**サーバのライセンスを認証するには**

1. [**スタート**]、[**プログラム**]、[**LANDesk**]、[**コア サーバの使用開始**] の順にクリックします。ユーザ名およびパスワードは入力されています。
- 使用するコア サーバの [**ユーザ名**] と [**パスワード**] を入力します。
- [**ライセンス認証**] をクリックします。

## 試用ライセンスによるサーバのライセンス認証

45 日の試用ライセンスにより、LANDesk Software ライセンス サーバを使ってサーバのライセンスが認証されます。45 日の評価期間が終了すると、コア サーバにログインすることができなくなり、インベントリ スキャンの受け入れが停止されます。ただし、ソフトウェアやデータベースの既存のデータは失われません。45 日の試用期間中やその終了後に、コア サーバの使用開始 ユーティリティを使って、LANDesk Software アカウントを使用する標準のライセンスに切り替えることができます。試用ライセンスが無効となった場合は、標準のライセンスへの切り替えにより、コア サーバのライセンスが再度認証されます。

**45 日間の評価用ライセンスで認証するには**

1. [**スタート**]、[**プログラム**]、[**LANDesk**]、[**コア サーバの使用開始**] の順にクリックします。
2. [**45 日間の評価用ライセンスでこのコア サーバを認証する**] をクリックします。
3. [**評価**] をクリックします。

## 既存のアカウントの更新

更新オプションにより、利用状況の情報が LANDesk Software ライセンス サーバに送信されます。インターネットに接続している場合は、利用状況のデータが自動で送信されます。そのため、通常はノード カウント検証の送信にこのオプションを使用しないでください。このオプションを使って、LANDesk Software アカウントに対応するコア

サーバを変更することもできます。このオプションは、試用ライセンスから標準ライセンスへの変更にも使用できます。

**既存のアカウントを更新するには**

1. [**スタート**]、[**プログラム**]、[**LANDesk**]、[**コア サーバの使用開始**] の順にクリックします。
2. [**LANDesk ユーザ名とパスワードを使ってこのコア サーバを更新する**] をクリックします。
3. 使用するコア サーバの [**ユーザ名**] と [**パスワード**] を入力します。入力したユーザ名とパスワードがコア サーバの認証時のものと異なる場合は、この操作によってコア サーバのアカウントが新しいものに切り替えられます。
4. [**ライセンス認証**] をクリックします。

## 手動によるコア サーバのライセンス認証とノード カウント データの確認

コア サーバがインターネットに接続していない場合は、コア サーバの使用開始 ユーティリティはノード カウント データを送信できません。ライセンス認証とノード カウント検証データの送信を電子メールを使って実行するよう求めるメッセージが表示されます。電子メールによるライセンス認証は、簡単で時間のかからない処理です。コア サーバ上で手動によるライセンス認証の実行を求めるメッセージが表示されたり、または コア サーバの使用開始 ユーティリティを使用していて手動によるライセンス認証を求めるメッセージが表示されたりする場合は、次の手順に従います。

**手動によりコア サーバのライセンス認証とノード カウント データの確認を行うには**

1. コア サーバがノード カウント データを手動で検証するように求める場合は、「¥Program Files¥LANDesk¥Authorization Files」フォルダに ACTIVATE.TXT というデータ ファイルが作成されます。このファイルを電子メール メッセージに添付し、licensing@landesk.com へ電子メールで送信してください。メッセージの件名や本文は空白のままで問題ありません。
2. LANDesk Software がメッセージの添付ファイルを処理し、メッセージが送信されたメール アドレスに返信されます。LANDesk Software メッセージに新しいライセンス認証ファイルが添付され、その処理手順が本文に記されます。
3. 添付されているライセンス認証ファイルを「¥Program Files¥LANDesk¥Authorization Files」フォルダに保存します。コア サーバがすぐにこのファイルを処理し、ライセンス認証ステータスを更新します。

手動によるライセンス認証に失敗したり、コア サーバが添付されたライセンス認証ファイルを処理できない場合は、ライセンス認証ファイルは .rejected という拡張子が追加され、Windows のイベント ビューアにあるアプリケーション ログによりユーティリティが詳細な情報を記録します。

# 付録 C :サービスの設定

Configure Services アプレットを使用して、コア
サーバおよびデータベースについて、次のサービスを設定できます。

- コア サーバおよびデータベースの選択
  インベントリ サービスの設定
  重複デバイス名の処理方法の設定
  重複デバイス ID の処理方法の設定
  スケジューラ サービスの設定
  カスタム ジョブ サービスの設定
  マルチキャスト サービスの設定
  BMC パスワードの設定
  Intel AMT パスワードの設定

Configure Services アプレットを起動するには、コア サーバ上で **[スタート]**、**[プログラム ファイル]**、**LANDeskLANDesk[Configure Services]**の順にクリックします。

タブの外側に 2 つのボタンが表示されます。

- **認証資格情報** : 優先サーバとして動作可能なデバイスを追加するための
  [サーバ認証資格情報] ダイアログを開きます。デバイスを追加するには、**[追加]**
  をクリックします。すると、**[ユーザ名とパスワード]** ダイアログが開きます (下記を参照)。
2. **OSD 検証** : Windows PE または DOS ベースの起動前環境を作成するためには、Windows PE 2005 または Windows NT 4 のインストール CD
   へのアクセスを提供する必要があります。双方のイメージング環境で
   **[今すぐ確認]**をクリックして、適切な CD へのパスを入力し、**[OK]** をクリックします。

## [ユーザ名とパスワード] ダイアログ

**[ユーザ名とパスワード]** ダイアログを使って、追加する優先サーバに関する情報を入力します。

**優先サーバ情報を入力するには**

1. [サービスの設定] アプレットで、**[認証資格情報]**をクリックします。
- [サーバ認証資格情報] ダイアログの **[追加]**をクリックします。
- 説明、認証情報、および IP アドレスの範囲を入力します。
- **[認証資格情報のテスト]** をクリックして、情報の有効性を検証します。
- **[OK]** をクリックして、優先サーバを [サーバ認証資格情報] ダイアログに追加します。
- **サーバ名** : 優先サーバ名。
  **ユーザ名**
:サーバに認証するのに使用されるユーザ名。完全修飾ドメイン名である必要があります
(例、Mydomainr name)。
  **説明** : 優先サーバの説明。
  **パスワード** : 優先サーバのパスワード。

**開始 IP アドレス** : 優先サーバの使用を制限するアドレス範囲の開始 IP アドレスを入力します。開始 IP アドレスは、終了 IP アドレス未満である必要があります。開始 IP アドレスと終了 IP アドレスの最初の 3 組の数字は、10.100.10.1 と 10.100.10.255 のように一致していなければなりません。

**終了 IP アドレス** :スキャンするアドレス範囲の終了 IP アドレスを入力します。

**追加** :ダイアログの下部の作業キューに IP アドレスの範囲を追加します。

**削除** :作業キューに対して選択した IP アドレスの範囲を削除します。

# [サービスの設定] タブ

サービスを構成する前に、**[全般]** タブを使用して、サービスを設定するコア サーバとデータベースを指定してください。

---

**注意** :コア サーバおよびデータベースに対して行った設定の変更は、そのコア サーバ上でサービスを再起動するまで有効になりません。

---

## コア サーバおよびデータベースの選択

**[全般]**タブでは、コア サーバとデータベースを選択し、そのコア サーバのサービスを設定するための認証資格情報を付与できます。

## [サービスの設定] ダイアログについて : [全般] タブについて

このダイアログでは、特定のサービスを設定するコア サーバとデータベースを選択します。次に、[サービス] タブを選択し、そのサービスの設定を指定します。

- **サーバ名** :現在接続されているコア サーバの名前を表示します。
2. **サーバ** :別のコア サーバとそのデータベース ディレクトリの名前を入力できます。
3. **データベース** :コア データベースの名前を入力できます。
4. **ユーザ名** :コア サーバへの認証資格情報を持つユーザを識別します。
5. **パスワード** :コア データベースへのアクセスに必要なユーザ パスワード (セットアップ時に指定) を識別します。
6. **これは Oracle データベースです** :上記で指定されているコア データベースが Oracle データベースであることを示します。(System Manager には当てはまりません。)
7. **変更の取り消し** :[サービスの設定] ダイアログを開いたときの設定を復元します。

## インベントリ サービスの設定

[全般] タブで選択したコア サーバとデータベースに対し、**[インベントリ]** タブを使用して、インベントリ サービスを設定します。

# [サービスの設定] ダイアログについて : [インベントリ] タブ

このタブでは、次のインベントリ オプションを指定します。

- **サーバ名** :現在接続されているコア サーバの名前を表示します。
- **統計情報の記録** :コア データベースのアクションや統計のログを保存します。
- **転送データの暗号化** :インベントリ スキャナによりスキャンされたデバイスから返されるデバイス インベントリ データが、SSL を通して暗号化データとしてコア サーバに送信されます。
- **サーバ スキャンの時刻** : コア サーバをスキャンする時刻を指定します。
- **メンテナンスの時刻** : 標準コア データベース メンテナンスを実行する時刻を指定します。
- **インベントリ スキャン保存日数** :インベントリ レコードを削除するまでの日数を設定します。
- **プライマリ オーナー ログイン** :インベントリ スキャナがログインを追跡する回数を設定して、デバイスのプライマリ オーナーを特定します。プライマリ オーナーは、この指定されたログイン回数内で最も多くログインしたユーザです。既定値は 5 で、最小値と最大値はそれぞれ 1 と 16 です。すべてのログインが 1 回限りの場合は、前回のユーザがプライマリ オーナーと見なされます。デバイスは一度に 1 人のプライマリ オーナーにのみ関連付けられます。プライマリ ユーザ ログイン データは、ADS、NDS、ドメイン名、またはローカル名フォーマット (その順で) のいずれかのユーザの完全修飾名だけでなく前回のログインの日付も含みます。
- **詳細設定** : インベントリ スキャナに関連した様々な詳細設定を設定できる**[詳細設定]**ダイアログを開きます。設定を変更するには、その設定をクリックし **[値]** テキストボックスの設定を変更してから **[設定]** をクリックします。ある設定の説明を表示するには、その設定をクリックして **[説明]** ボックスにある詳細を表示します。
- **ソフトウェア** :**[ソフトウェア スキャン設定]**ダイアログが開き、サーバ ソフトウェア スキャンの時刻と履歴の設定が構成できるようになります。
- **属性** : データベースに保存されるインベントリ スキャン属性を選択できる [保存する属性の選択] ダイアログを開きます。
- **重複の管理 :デバイス**:[重複デバイス名の処理方法の設定] ダイアログを開き、重複デバイス名、MAC アドレス、またはその両方を持つデバイスを削除するオプションを選択できます (以下の**「重複デバイス」**を参照)。
- **重複の管理 :デバイス ID : [重複デバイス ID]**ダイアログが開き、一意に識別するデバイスの属性を選択できます。このオプションを使用すると、コア データベースに重複デバイス ID をスキャンする必要がありません (次の「重複デバイス ID 処理の設定」を参照)。
- **インベントリ サービス ステータス** :コア サーバ上で、サービスが開始または停止したかどうかを示します。
- **開始** :コア サーバでサービスを開始します。
- **停止** :コア サーバでサービスを停止します。

## [ソフトウェア スキャンの設定] ダイアログについて

このダイアログでは、ソフトウェア
スキャンの頻度を設定します。デバイスのハードウェアは、デバイスでインベントリ
スキャナが実行されるごとにスキャンされますが、デバイスのソフトウェアは、ここで指定した間隔でのみスキャンされます。

- **ログインごと**
  :ユーザがログオンするごとに、デバイスにインストールされたすべてのソフトウェアをスキャンします。
- **指定日数 に 1 回**
  :指定した日数単位の間隔で、デバイスのソフトウェアのみを自動スキャンします。
- **履歴保存日数** :デバイスのインベントリ履歴を保存する日数を指定します。

## 重複デバイス名の処理方法の設定

[重複デバイス] ダイアログを使用して、データベースから重複デバイスを削除します。

1. [インベントリ] タブで、**[デバイス]** をクリックします。
- [重複デバイス]
  ダイアログで、重複デバイスを削除するときに使用するオプションをクリックして、**[OK]**をクリックします。

  **重複しているデバイスの削除** :
  - **デバイス名一致** :データベース内で 2
    つ以上のデバイス名が一致するときに、古い方のレコードを削除します。

  **MAC アドレス一致** :データベース内で 2 つ以上の MAC
アドレスが一致するときに、古い方のレコードを削除します。

  **デバイス名と MAC アドレスが一致** :同じレコードに対して 2 つ以上のデバイス名と MAC
アドレスが一致するときには、古い方のレコードのみを削除します。

## 重複デバイス ID の処理方法の設定

ネットワークのデバイスの設定にはイメージングが頻繁に使用されるので、デバイス間でデバイス ID
が重複する可能性が高くなります。この問題を回避するために、他の固有のデバイス属性を指定し、それをデバイス ID
と組み合わせて、デバイス固有の識別子を作成できます。これらの他の属性の例には、デバイス名、ドメイン名、BIOS、バス、コプロセッサなどがあります。

重複 ID
チェック機能を使用すると、サーバを一意に識別するためのデバイス属性を選択できます。この機能では、これらの属性の内容を指定し、そのうちのいくつが欠けていたときにデバイスが他のデバイスと重複していると判断するかを指定できます。インベントリ
スキャナは、重複するデバイスを検出すると、アプリケーション イベント

ログにイベントを書き込んで、重複デバイスのデバイス ID を示します。[重複デバイス ID] ダイアログには次のオプションがあります。

- **属性リスト** :デバイスを一意に識別するために選択できる属性をすべて一覧表示します。
2. **ID 属性** :デバイスを一意に識別するために選択した属性が表示されます。
3. **重複デバイス ID トリガ** :
    - **ID 属性**
      :一致していないデバイスの属性がいくつあれば、他のデバイスと重複していると判断するかを識別します。

**ハードウェア属性**
:一致していないデバイスのハードウェアの属性がいくつあれば、他のデバイスと重複していると判断するかを識別します。

4. **重複した ID を拒否** :インベントリ スキャナによって重複したデバイスのデバイス ID を記録し、そのデバイス ID を再びスキャンすることを拒否します。このとき、インベントリ スキャナは新しいデバイス ID を生成します。

**重複した ID の処理方法を設定するには**

1. [サービスの設定] ダイアログで、**[インベントリ]**タブをクリックし、**[デバイス ID]**をクリックします。
- デバイスを一意に識別するために使用する **[属性リスト]**から属性を選択し、右矢印ボタンをクリックして、属性を **[ID 属性]** リストに追加します。追加する属性の数に制限はありません。
- 一致していないデバイスの ID 属性 (およびハードウェア属性) がいくつあれば他のデバイスと重複していると判断するかを選択します。
- インベントリ スキャナによって重複デバイス ID を拒否するには、**[重複した ID を拒否]**オプションをオンにします。

## スケジューラ サービスの設定

**[全般]** タブで選択したコア サーバとデータベースに対し、**[スケジューラ]** タブを使用して、スケジューラ サービスを設定します。これらのタスクを実行するには、管理デバイスに対する完全な管理者権限など、System Managerからパッケージ配布の受け取りが許可された適切な権限が必要です。**[ログインの変更]**をクリックしてデバイスで使用する複数のログイン資格情報を指定できます。

## [サービスの設定] ダイアログについて : [スケジューラ] タブ

このタブでは、それまでに選択したコア サーバとデータベースの名前を表示し、次の [スケジュールされているタスク] オプションを指定します。

- **ユーザ名** :[スケジュールされているタスク] のサービスを実行するユーザ名。この名前は、**[ログインの変更]**ボタンをクリックして変更できます。

**再試行間の秒数**:この設定は、スケジュールされているタスクに複数の再試行を設定した場合に、スケジュールされているタスクがタスクを再試行するまでの待機秒数を制御します。

**ウェイクアップ実行秒数** : この設定は、Wake On LAN を使用してスケジュールされているタスクを設定した場合、スケジュールされているタスクがデバイスをウェイクアップするまでの待機秒数を制御します。

**クエリ評価の間隔** : クエリ評価間の時間を示す数値とその数値の単位 (分、時、日、週)。

**Wake on LAN の設定** : クライアントをウェイクアップするためにスケジュールされているタスクが設定する Wake On LAN パケットで使用される **IP ポート**。

**サービス ステータスのスケジュール** :コア サーバ上で、サービスが開始または停止したかどうかを示します。

**開始** :コア サーバでサービスを開始します。

**停止** :コア サーバでサービスを停止します。

**再起動** :コア サーバでサービスを再起動します。

**詳細** : スケジューラの動作方法をコントロールする設定を変更できる **[スケジューラの詳細設定]** ダイアログを開きます。設定を変更するには、その設定をクリックして **[編集]**をクリックし、設定を変更してから **[OK]**をクリックします。

## [サービスの設定] ダイアログについて :[ログインの変更] ダイアログ

**[ログインの変更]** ダイアログ (**[スケジューラ]** タブの **[ログインの変更]** をクリック) を使用して、既定のスケジューラ ログインを変更できます。非管理デバイスでタスクを実行するのに必要な場合に、スケジューラ サービスが使用する代替の資格情報を指定することもできます。

非管理デバイスに System Manager エージェントをインストールするには、スケジューラ サービスが管理者アカウントでデバイスに接続できる必要があります。スケジューラ サービスが使用する既定のアカウントは、LocalSystem です。LocalSystem の資格情報は、通常ドメイン内にないデバイスについて有効です。デバイスがドメイン内にある場合は、ドメインの管理者アカウントを指定する必要があります。

スケジューラ サービスのログイン資格情報を変更する場合は、異なるドメインレベルの管理アカウントを指定してデバイスで使用できます。複数のドメインにわたってデバイスを管理している場合は、スケジューラ サービスが使用する資格情報を追加することができます。スケジューラ サービスで LocalSystem 以外のアカウントを使用する場合、または代替の資格情報を提供する場合は、コア サーバの管理者権限を持つプライマリのスケジューラ サービス ログインを指定する必要があります。代替の資格情報にはコア サーバの管理者権限は必要ありませんが、デバイスでは管理者権限が必要となります。

スケジューラ サービスは、既定の資格情報を使用してから、ログインが可能になるか代替の資格情報がなくなるまで、[代替の資格情報] リストで指定したそれぞれの資格情報を使用します。指定する資格情報は、セキュリティが保護された状態で暗号化され、コア サーバのレジストリに保存されます。

既定のスケジューラ情報では、次のオプションを設定できます。

- **ユーザ名** :スケジューラが使用する既定のドメイン¥ユーザ名、またはユーザ名を入力します。
2. **パスワード** :指定した資格情報のパスワードを入力します。
3. **パスワードの確認入力** :パスワードを再度入力して、確認を行います。

追加のスケジューラ情報では、次のオプションを設定できます。

- **追加** :クリックして、[代替の資格情報] リストで指定したユーザ名とパスワードを追加します。
- **削除**:クリックして、リストから選択した資格情報を削除します。
- **変更** :クリックして、選択した資格情報に変更を加えます。

代替の資格情報を追加する場合は、次の項目を指定します。

- **ユーザ名** :スケジューラが使用するユーザ名を入力します。
- **ドメイン** :指定したユーザ名のドメインを入力します。
- **パスワード** :指定した資格情報のパスワードを入力します。
- **パスワードの確認入力** :パスワードを再度入力して、確認を行います。

## カスタム ジョブ サービスの設定

[全般] タブで選択したコア サーバとデータベースに対し、**[カスタム ジョブ]** タブを使用して、カスタム ジョブ サービスを設定します。カスタム ジョブの例には、インベントリ スキャンやソフトウェア配布などが含まれます。

リモート実行プロトコルとしての TCP リモート実行を無効にすると、カスタム ジョブは、無効に設定されているかどうかにかかわらず、既定で標準の管理エージェント プロトコルを使用します。また、TCP リモート実行と標準の管理エージェントの両方が有効な場合、カスタム ジョブは、TCP リモート実行の使用をまず試行し、存在しない場合は、標準の製品リモート実行を使用します。

**[カスタム ジョブ]** タブでも、サーバ検出のオプションを選択できます。カスタム ジョブ サービスがジョブを処理する前に、各サーバの現在の IP アドレスを検出する必要があります。このタブでは、サービスがサーバと接続する方法を設定できます。

## [サービスの設定] ダイアログについて : [カスタム ジョブ] タブ

このタブでは、次のカスタム ジョブ オプションを設定します。

**リモート実行オプション**:

- **TCP 実行を無効にする** : リモート実行プロトコルとしての TCP を無効にし、CBA プロトコルを既定で使用します。

- **[CBA 実行 / ファイル転送を無効にする]** :
  リモート実行プロトコルとして標準の管理エージェントを無効にします。標準の管理エージェントを無効にした場合、TCP
  リモート実行プロトコルがデバイスで検索できなければ、リモート実行ができません。
- **リモート実行タイムアウトを有効にする** :
  リモート実行タイムアウトを有効にし、タイムアウトとなるまでの秒数を指定します。リモート実行タイムアウトは、デバイスがハートビートを送信しても、デバイス上のジョブがハングまたはループしている場合に実行されます。この設定は、両方のプロトコル (TCP
  または標準の管理エージェント) に適用されます。この値の有効範囲は、300 秒 (5 分) ～ 86400 秒 (1 日) です。
- **クライアント タイムアウトを有効にする** : デバイス
  タイムアウトを有効にし、タイムアウトとなるまでの秒数を指定します。既定では、リモート実行が完了するかタイムアウトとなるまで、TCP リモート実行が、デバイスからデバイスに 45
  秒間隔でハートビートを送信します。クライアント
  タイムアウトは、デバイスがデバイスにハートビートを送信しない場合に実行されます。
- **リモート実行ポート (既定値は 12174)** :TCP
  リモート実行が行われるポート。このポートを変更する場合は、クライアント構成も変更する必要があります。

**配布オプション**:

- **同時に <nn> 台のサーバに配布** :同時にカスタム ジョブが配布されるデバイスの最大数。

**検索オプション**:

- **UDP** :UDP を選択すると、UDP を介して標準の管理エージェント Ping を使用します。多くの System Manager
  コンポーネントは、標準の管理エージェントに依存するため、管理デバイスに標準の管理エージェントがインストールされている必要があります。これは、最速の検索方法であり、既定となっています。UDP を使うと、UDP ping の **[再試行]** と **[タイムアウト]** を選択することもできます。
- **TCP** :TCP を選択すると、ポート 9595 でサーバへの HTTP
  接続を使用します。この検出方法は、ポート 9595
  を開いている場合にファイアウォールを介した作業が可能になるという利点があります。ただし、デバイスがない場合は、HTTP
  接続のタイムアウトが発生することがあります。これらのタイムアウトには、20
  秒以上かかる場合があります。数多くのターゲット デバイスが TCP
  接続に応答しない場合は、ジョブの開始までに時間がかかることがあります。
- **両方**:両方を選択すると、サービスはまず UDP、次に TCP、最後に DNS/WINS
  (選択されている場合) を使用して検出を試みます。
- **サブネット ブロードキャストを無効にする** :選択すると、サブネット
  ブロードキャストを介した検出を無効にします。
- **DNS / WINS 検索を無効にする** :選択すると、選択した TCP/UDP
  検出方法が失敗した場合に、各デバイスのネーム サービス ルックアップを無効にします。

## マルチキャスト サービスの設定

**[全般]** タブで選択したコア サーバとデータベースに対し、**[マルチキャスト]** タブを使用して、マルチキャスト ドメイン代表検索オプションを設定します。

## [サービスの設定] ダイアログについて : [マルチキャスト] タブ

このタブでは、次のマルチキャスト オプションを設定します。

- **マルチキャスト ドメイン代表を使用する** :ネットワーク表示の **[構成] > [マルチキャスト ドメイン代表]** グループに保存されているマルチキャスト ドメイン代表のリストを使用します。
- **キャッシュ ファイルを使用する** :ファイルが既にキャッシュされているかどうかを確認するために、各マルチキャスト ドメインにクエリします。ファイルをダウンロードする代わりにキャッシュされているファイルが使用されます。
- **優先ドメイン代表の前にキャッシュ ファイルを使用する:** 検索する順番を変更して、試行する最初のオプションが**キャッシュ ファイルとなる**ように設定します。
- **ブロードキャストを使用する** :サブネット指定のブロードキャストを送信して、マルチキャスト ドメイン代表とするサブネットのデバイスを見つけます。
- **ログ破棄期限 (日)** :ログのエントリが削除されずに保持される日数を**指定します**。

## BMC パスワードの設定

**[BMC パスワード]** タブを使用して IPMI Baseboard Management Controller (BMC) のパスワードを作成します。

- **[BMC パスワード]** タブで、**[パスワード]** テキスト ボックスにパスワードを入力し、**[パスワードの確認入力]**テキスト ボックスにパスワードを再入力して、**[OK]**をクリックします。

  パスワードは英数字で 15 文字以内にします。使用できる文字は 0～9 の数字、または a～z の大文字または小文字のアルファベットです。

## Intel AMT オプションの設定

Intel Active Management Technology 対応デバイスのパスワードを作成または変更し、AMT デバイスの検出方法を表示するには、**[Intel AMT 構成]** タブを使用します。

### Intel AMT のパスワードを設定するには

1. 現在のユーザ名とパスワードを入力します。このユーザ名とパスワードは Intel AMT 構成画面で設定されているものに一致する必要があります (コンピュータの BIOS 設定からアクセスできます)。
- ユーザ名とパスワードを変更するには、**[新しい Intel AMT パスワード]** セクションで設定してください。
- **[OK]** をクリックします。この変更は、そのクライアント設定の実行中に行います。

**注意**
:新しいパスワードは堅牢なパスワード、つまり次の条件を満たしたパスワードである必要があります。

- 7 文字以上
  アルファベット文字、数字、および記号を含む
  2 番目から 6 番目の文字のうち、少なくとも 1 文字が記号である
  前のパスワードと大幅に異なる
  名前やユーザ名を含まない
  一般的な単語や名前ではない

### Intel AMT デバイスの検索とプロビジョニング

AMT デバイスを検索するには、AMT BIOS の [プロビジョニング サーバ] フィールドにコア サーバの IP アドレスを入力して、ポート 9982 を使用します。詳細については **[サービスの設定]** の **[ヘルプ]** を押してください。Intel AMT デバイスが検出され **[マイ デバイス]** リストに移動された場合、TLS モードを使って、自動的に提供されます。

# 付録 D
# :エージェントのセキュリティと信頼されている証明書

コア サーバをデバイスに初めてインストールするとき、セットアップ プログラムによって各コア サーバに固有の証明書と秘密キーが作成されます。デバイスは、信頼されている証明書ファイルが一致するコア サーバのみと通信します。

インストールされる秘密キーと証明書ファイルを次に示します。

- **<キー名>.key:**.KEY ファイルは、コア サーバの秘密キーであり、コア サーバだけに置かれます。このキーが漏洩すると、コア サーバとサーバの通信が安全ではなくなります。このキーを保護してください。たとえば、電子メールで転送しないでください。
2. **<キー名>.crt:**.CRT ファイルには、コア サーバの公開キーが含まれています。.CRT ファイルは、公開キーを閲覧者にわかりやすく表示したバージョンです。このファイルを表示して、キーに関する詳細を参照できます。
3. **<ハッシュ>.0:**.0 ファイルは、信頼されている証明書ファイルであり、.CRT ファイルと同じ内容が含まれています。ただし、さまざまな証明書が含まれているディレクトリでコンピュータが適切な証明書ファイルを速やかに検索できるように、名前が付けられます。その名前は、証明書のサブジェクト情報のハッシュ (チェックサム) です。特定の証明書のハッシュ ファイル名を調べるには、<キー名>.CRT ファイルを表示します。ファイルには .INI ファイル セクション [LDMS] があります。ハッシュと値のペアは、<ハッシュ> 値を示します。

すべてのキーは、コア サーバの ¥Program Files¥LANDesk¥Shared Files¥Keys に保存されています。<ハッシュ>.0 公開キーは LDLOGON ディレクトリにもあり、既定でこのディレクトリに存在する必要があります。<キー名>はコア サーバのセットアップで入力した証明書名です。セットアップ時に、コア サーバ名などのわかりやすいキー名 (またはその完全修飾名) を入力すると便利です (例 :ldcore や ldcore.org.com)。それによって、多数のコアが存在する環境で証明書/秘密キーを簡単に識別できるようになります。

## コア サーバ間での証明書/秘密キーのバックアップと復元

コア サーバをインストールすると、セットアップによって新しい証明書が作成されます。既存のコア サーバを再インストールする場合でも、新しい証明書が作成されます。新しいコア サーバの証明書と一致しない証明書をデバイスにインストールすると、コア サーバはこのデバイスと通信できません。コア サーバを再インストールする必要がある場合、次の 2 つのオプションがあります。

1. 新しいコア サーバの設定を指定してエージェントを手動で再インストールします。コア サーバとデバイスの証明書/キーは一致しないため、ソフトウェア配布を使用してエージェントをアップデートできません。

- コア
  サーバを再インストールする前に、既存の証明書/キーのバックアップを安全な場所に取ります。再インストールした後で、古いキーを新しいコア
  インストールにコピーします。新しいキーと古いキーは共存できます。コアは適切なキーを自動的に使い分けます。

コアは、複数の証明書/秘密キー
ファイルを保持できます。クライアントは、コアにあるいずれかのキーで認証できる限り、そのコアと通信できます。

上記第 2 のオプションを実行するユーティリティが本製品に含まれています。このコア
データ移行ユーティリティ (CoreDataMigration.exe) は ¥ProgramFiles¥LANDesk¥ManagementSuite
フォルダにインストールされています。.このユーティリティは、新しいコアをインストールする際にキーや証明書などのデータのバックアップとコピー処理を行います。

**証明書/秘密キー セットを保存するには**

1. コピー元のコア サーバで、¥Program Files¥LANDesk¥Shared Files¥Keys フォルダに移動します。
2. コピー元のサーバの <キー名> .key、<キー名> .ctr、および <ハッシュ> .0
   の各ファイルをフロッピー ディスクなどの安全な場所にコピーします。
3. コピー先のコア サーバで、コピー元のコア サーバから同じフォルダ (¥Program Files¥LANDesk¥Shared Files¥Keys) にファイルをコピーします。キーはすぐに有効になります。

---

**警告 :秘密キーは安全な場所に保存します。**
秘密キーの <キー名>.key
が破損しないようにしてください。秘密キーは、電子メールや公開ファイル共有など安全でない方法で転送しないでください。コア サーバはこのファイルを使用してデバイスを認証し、適切な <キー名>.key
ファイルを保持しているコアは、管理するデバイスに対してリモート実行やファイル転送を実行できます。

---

# トラブルシューティングのヒント

コンソールでの発生頻度がもっとも高い問題の、トラブルシューティングのヒントを次に示します。

**コア サーバのライセンスを認証できない。**
コア サーバをインストールし、デバイス時刻を変更すると、ライセンスを認証することができません。コア サーバのライセンスを認証するには、製品を再インストールする必要があります。

**コアをアクティブにしようとした時に、コア サーバ データベースが読み取れないというエラー メッセージを受けとった。**
コア
サーバが物理的にネットワークに接続されており、有効なインターネット接続が存在していることを確認します。ケーブルが外れているか、コア
サーバのインターネット接続が有効になっていない場合、アクティベーション
プロセスを完了できません。

**コンソール ページへの URL がわからない。**
コア サーバのインストール担当者 (通常はユーザ サイトのネットワーク管理者)
に問い合わせてください。通常 Server Manager と System Manager の URL は、http:// *コア サーバ マシン名*/ldsm です。Management Suite の URL は http://*コア サーバ マシン名*/remote です。

**誰の名前でログインするのか。**
**[接続ユーザ]** セクションで、LANDeskSystem Manager という名前の下のバーをご覧ください。

**どのコンピュータにログインするのか。**
**[接続先]**セクションで、LANDeskSystem Manager という名前の下のバーをご覧ください。

**System Manager を起動してすぐに、「Session Timed Out (セッションがタイムアウトになりました)」というメッセージを受け取った。**
[お気に入り] または [ブックマーク] メニューから「/frameset.aspx」という拡張子の付いた System Manager を開いても正しく起動しません。これを修正するには、[ブックマーク] または [お気に入り] リンクを編集して、この拡張子を削除するか、またはブラウザ ウィンドウに直接 URL (拡張子なし)
を貼り付けます。

**左側のナビゲーション ペイン リンクの一部が表示されない。**
これは多くの場合、ネットワーク管理者が LANDeskSystem Manager
の役割ベース管理や機能レベルのセキュリティ
オプションを使用して、ユーザが一定のタスクを実行するのを制限しているためです。

**スキャナがデバイスに接続できない。**
スキャナがデバイスに接続できない場合は、Web アプリケーション
ディレクトリが正しく設定されていることを確認してください。https
を使用している場合は、有効な証明書が必要です。有効な証明書を持っていることを確認してください。

**コンソールにアクセスしようとして「アクセス拒否」のエラーが発生した場合**
Windows 2000 および 2003

上で機能レベルのセキュリティを使用するには、匿名認証を無効にする必要があります。Web サイト上の認証設定と Web サイト下の「..¥LANDesk¥ldsm」フォルダを確認してください。

1. Web コンソールをホストするサーバで、**[スタート]**、**[管理ツール]**、**[Internet Information Services (IIS) Manager]**の順にクリックします。
2. **[既定の Web サイト]** ショートカット メニューから、**[プロパティ]**をクリックします。
3. **[ディレクトリ セキュリティ]**タブで、**[匿名アクセスおよび認証コントロール]**ボックスの**[編集]**をクリックします。**[匿名アクセスを有効化]**オプションをオフにして、**[統合 Windows 認証]**オプションをオンにします。
4. **[OK]**をクリックしてダイアログを終了します。
5. [既定の Web サイト] の .¥LANDesk¥ldsm サブフォルダから、**[プロパティ]**をクリックします。ステップ 3 ～ 4 を繰り返します。

**コンソールを表示すると無効なセッションを受け取る。**
ブラウザのセッションがタイムアウトした可能性があります。ブラウザの**[更新]**ボタンを使って、新しいセッションを開始してください。

**Web コンソールを開始したときに ASP.NET エラーが表示される。**
Web コンソールへのログインを試みたときに ASP.NET エラー メッセージが表示された場合、ASP と ASP
ディレクトリへのアクセス権が正しく設定されていない可能性があります。このような場合、次のコマンドを実行して ASP.NET 設定をリセットしてください。

```
ASPNET_REGIIS.EXE –i
```

**1 ページに表示される項目数が、指定した数と異なる。**
1 ページに表示する項目数を指定すると、この設定は Web ブラウザのクッキー ディレクトリに格納され、コンソール セッションがタイムアウトになると無効になります。

**コンソールが頻繁にタイムアウトする。**
コンソールの Web ページに対して既定のセッション タイムアウトを変更できます。IIS の既定では、20 分間操作が行われないと、ログインはタイムアウトとなります。IIS セッション タイムアウトを変更するには

1. Web サーバで、IIS Internet Service Manager を開きます。
2. 既定の Web サイトを展開します。
3. **[LDSM]**フォルダを右クリックし、**[プロパティ]**をクリックします。
4. **[仮想ディレクトリ]**タブで、**[構成]**をクリックします。
5. **[アプリケーション オプション]**タブをクリックし、セッション タイムアウトを適切な値に変更します。

**注意** :LANDeskSystem Manager8.70 は、セッション ベースの製品です。セッション状態を無効にしないでください。

**Web コンソールでリモート コントロール ページが表示できない。**
**リモート コントロール**ページを表示するには、ActiveX コントロールを有効にする必要があります。ブラウザによっては、ActiveX は既定で無効とされています。**リモート**

**コントロール**ページが正しくロードされない場合は、セキュリティ設定を変更してブラウザの ActiveX コントロールを有効にしてください。

**ソフトウェア配布ウィザードを完了したが、コンソールでパッケージが作成されない。.**
コンソールでは、コンソール サーバの IUSR アカウントと IWAM アカウントを使用します。これらのアカウントは、コンピュータ名に基づいて作成されます。コンピュータ名を変更した場合、ソフトウェア配布パッケージを正常に作成するには次の手順を実行する必要があります。

1. .Net Framework がインストールされている場合は、アンインストールします。
2. IIS をアンインストールします。
3. IIS を再インストールします。
4. .Net Framework をアンインストールした場合は、再インストールします。

**スケジュールされているソフトウェア配布ジョブが実行されない。**
ソフトウェア配布ジョブをスケジュールしたにもかかわらず開始されなかった場合は、Intel Scheduler Service がデバイス上で実行していることを確認してください。

また、ジョブのスケジュールがコア サーバ時間に基づいていることを考慮してください。別のタイム ゾーンにあるコンソールでジョブをスケジュールした場合、そのジョブはコア サーバの時間に基づいて開始します。したがってコンソールで予定した時間とは異なる場合があります。

**レポートのグラフが正しく表示されない。**
インタラクティブ バー、および多数のレポートに表示される円グラフを表示するためには、Macromedia Flash Player* がインストールされている必要があります。Flash がインストールされていることを確認してから、レポートを再実行します。

**データベースに認証できないという Web コンソール エラーが表示された。**
Oracle 9.2.0.1 を使用している場合、(IIS が使用する) 認証されているユーザに適切な権限が設定されないという Oracle のインストール バグがあります。データベースに認証できないという Web コンソール エラーが表示された場合、次の手順で問題を解決してください。

1. 管理者権限を持つユーザとして Windows にログインします。
2. **[スタート]**メニューから Windows エクスプローラを起動し、ORACLE_HOME フォルダに移動します。これは通常、Oracle フォルダの下にある Ora92 フォルダ (D:¥Oracle¥Ora92) です。
3. ORACLE_HOME フォルダのショートカット メニューで、**[プロパティ]**をクリックします。
4. **[セキュリティ]**タブをクリックします。
5. **[名前]**リストで、**[認証済みユーザ]**をクリックします。Windows XP では、[名前] リストは**[グループ名またはユーザー名]**と呼ばれています。
6. **[許可]**列の **[アクセス権]**リストで、**[読み取りと実行]**オプションをオフにします。Windows XP では、**[許可]**リストは認証済み**ユーザーのアクセス許可**と呼ばれています。
7. 前の手順でオフにした **[許可]**列の**[読み取りと実行]**オプションを再度オンにします。

8. **[詳細]**をクリックし、**アクセス許可エントリ**リストにある**[認証済みユーザ]**のアクセス権が「読み取りと実行」、適用先が
「このフォルダ、サブフォルダ、およびファイル」になっていることを確認します。このようになっていない場合は、**[適用先]**ボックスが
**[このフォルダ、サブフォルダ、およびファイル]**に設定されるようにその行を編集してください。この設定は既に正しく設定されているはずですが、必ず確認してください。
9. **[OK]**をクリックして、[セキュリティ] の [プロパティ] ウィンドウをすべて閉じます。
10. サーバを再起動して、これらの変更を反映させます。

**インストール中の Oracle エラー。**
インストール中に次のようなメッセージが表示されることがあります:

OraOLEDB.Oracle.1 プロバイダはローカル マシンに登録されていない。

このメッセージが表示される場合は、権限に問題がある可能性があります。おそらく、9i クライアントを使用して Oracle データベースに接続したと考えられます。これは既知の Oracle 問題に関連しています。既に OraOLEDB
ドライバをインストールしていることを確認したら、以下を行ってください。

1. Windows エクスプローラで、OraHome92 ディレクトリ (既定では、C:¥oracle¥ora92)
に移動し、このフォルダを右クリックして、**[プロパティ]**、**[セキュリティ]**を選択し、**[Authenticated Users]**を選択して、**[許可]**ボックスの [読み取りと実行]
許可の選択を解除してから再度選択し、**[適用]**をクリックします。
2. **[詳細]**ボタンをクリックし、**[継承可能な権限を親からこのオブジェクトに反映させる]**および
**[すべての子オブジェクトの権限をリセットして継承可能な権限を反映させる]**チェックボックスをオンにします。**[適用]**をクリックして、プロンプトが表示されたら、**[はい]**を選択します。このプロセスが終了したら、**[継承可能な権限を親からこのオブジェクトに反映させる]**チェックボックスがオンになっていることを確認します。
3. コマンド プロンプト ウィンドウに、「iisreset」と入力します。

この時点で、データベースを認証し、コンソールを使用できます。
**自分のデータベースに同じデバイスの 2 つのインスタンスが表示されるのはなぜか。**
コア データベースからデバイスを削除し、UninstallWinClient.exe
を使用してデバイスを再インストールしましたか。

UninstallWinClient.exe は メインの ManagementSuite プログラム フォルダである、LDMain 共有フォルダ内にあります。この共有フォルダにアクセスできるのは、管理者のみです。このプログラムは、このプログラムを実行しているデバイスの LANDesk
エージェントをアンインストールします。このプログラムは、必要なフォルダに移動させたり、ログインスクリプトに追加できます。これは、インターフェイスを表示しないで、非表示で実行する Windows アプリケーションです。削除したデータベースでデバイスの 2
つのインスタンスを表示できます。これらのインスタンスの 1 つには、履歴データのみが含まれ、もう 1 つのインスタンスには、転送されるデータが含まれます。UninstallWinClient.exe
の詳細については、*『導入ガイド』*を参照してください。

**Server Manager8.70 または Management Suite 8.X から Management Suite/Server Manager8.70 の再インストールで前のバージョンのデータベースを使用している。**
同一コンピュータ上で MSDE データベースを使用する LDMS 8.X または LDSM 8.70 を使用していて、アンインストールした場合、MSDE データベースと作成されたインスタンスはアンインストールされていないので、同じコンピュータに LDSM/LDMS 8.70 を再度インストールする場合にもう一度そのデータベースを利用できます。再インストール時に、このデータベースへの接続に必要な接続情報をレジストリで探してください。

キー :HKEY_LOCAL_MACHINE¥SOFTWARE¥LANDesk¥ManagementSuite¥Core¥Connections¥Local

次の文字列値は、[ユーザ指定データベース構成] ページに入力する必要がある値に対応しています。

Server <hostname¥ldmsdata>
User <sa>
Database <lddb>
Password （エンコード可能。「PWD Encrypted」の値に依存）

**IPMI デバイスの検出を試みた際、[非管理デバイス] ページの IPMI フォルダに一覧表示されない。**
IPMI デバイスには、IPMI として検出されて IPMI の全機能が利用できるように設定されている BMC (Baseboard Management Controller) が必要です。BMC が設定されていないと、デバイスは通常のコンピュータとして検出されます。その場合、そのデバイスを管理デバイスのリストに追加して、サービス設定ユーティリティを実行して BMC パスワードを設定します。すると、デバイスの IPMI 機能が本製品によって認識されます。

**PXE 起動メニューを選択した際にコア サーバのアドレスを取得できない。**
ターゲット コンピュータで PXE 代表の導入を試行して、デバイスを再起動し、F8 を押して PXE 起動メニューを選択した場合に、次のようなメッセージを受け取ります。「HTGET:Cannot get address for <core server>.Error:Unable to resolve name :<core server> into an address .ParseCoreAddressInof failure」

これは、クライアントが HTTP を使ってコア サーバからファイルをダウンロードしているためです。クライアントは WINS を使って IP アドレスへのコア サーバ名を解決します。コア サーバからファイルをダウンロードできない場合に、HTGET エラーが返されます。

この問題を解決するには、「http://kb.landesk.com/al/12/4/article.asp?aid=2558&n=7&tab=search&bt=4&r=0.1898264&s=1」の文書を読んでください。

**S.M.A.R.T. ドライブをサーバに追加したのに、そのサーバのインベントリ リスト内に S.M.A.R.T. ドライブの監視が表示されない。**
ハードウェア監視は、デバイスにインストールされているハードウェアの機能とハードウェアの正しい構成に依存します。S.M.A.R.T. 監視機能を持つハード ドライブがデバイスにインストールされているが、S.M.A.R.T. 検出がデバイスの BIOS 設定で有効になっていない場合、またはデバイスの BIOS が S.M.A.R.T. ドライブをサポートしていない場合、監視データは利用できず、結果のアラートも生成されません。

**PXE ベースの OSD DOS スクリプトのコンマ以降の部分が切り捨てられる。**
スクリプトのどの行でも、コンマ以降はすべての文字が切り捨てられます。したがって、コンマ以降のコマンドは実行されません。これを防ぐには、次のようにコマンド全体を引用符で囲んでください。

REMEXEC1=%QUOTE%echo ″hi,good morning″%QUOTE%

.INI ファイルの読み取りではずされるので、通常の引用符は機能しません。

**異なるサブネットにある Web コンソールからリモート コントロールのインストールを試みると、RC ビューアはインストールできません。**
異なるドメイン上のコアによってホスティングされている Web コンソールへ接続し、**[マイ デバイス]**リストにあるコンピュータを右クリックして**[リモート コントロール]** を選択した場合、RC ビューアが正常にインストールされていないというエラー メッセージを受け取ります。

解決するために、web.config の「CabUrl」というタグを読み取って CAB の URL を取得します。この CabUrl
タグには、ただのコンピュータ名だけでなく、完全修飾ドメイン名が含まれている必要があります。web.config を開いて、完全修飾ドメイン名を CabUrl タグに挿入する必要があります。

**インベントリ スキャンを実行するまで、USB ディスク デバイスがインベントリ リストに表示されない。**
USB ケーブルでディスク
デバイスが管理デバイスに接続された場合、そのデバイスは、デバイスのインベントリのハード ドライブにすぐには一覧表示されません。このドライブは、デバイスに接続した後、論理ドライブのもとに一覧表示されます。インベントリ スキャンをデバイス上で実行するまで、ハード ドライブのもとには表示されません。

管理対象の Linux デバイス上では、USB ディスク
デバイスをインベントリに一覧表示するためにマウントしておく必要があります。マウントしてもインベントリ スキャンをまだ実行していない場合、そのデバイスは論理ドライブのもとに表示されます。インベントリ スキャンを実行すると、ハード
ドライブのもとに一覧表示されます。デバイスを切断する場合、システムからアンマウントする必要があります。古いカーネルを実行している一部の Linux
システムでは、デバイスを切断してアンマウントしても、インベントリ
リストに残ってしまうことがあります。この場合、管理デバイスを再起動してからそのデバイスをインベントリ リストから削除する必要があります。

**Web コンソール ヘルプの索引を表示すると、空白ページが表示される。**
Web コンソールの HTML オンライン ヘルプには、Windows のインデックス
サービスを利用したフルテキスト検索の可能な検索機能があります。通常、この機能は既定で有効です。Web サーバでインデックス作成を有効にする必要がある場合は、次の手順を実行します。

1. **[スタート]**、**[プログラム]**、**[管理ツール]**、**[サービス]**の順にクリックします。
2. **[Indexing Service]**をダブルクリックし、**[開始]**をクリックします。
3. **[OK]**をクリックして、ダイアログを終了します。

インデックス サービスがサーバのインデックスを作成する間、しばらく待つ必要があります (2 – 3 時間程度)。