

Hitachi IT Operations Director 構築ガイド

解説・手引・操作書

3021-3-292-10

前書き

■ 対象製品

P-2642-8554 Hitachi IT Operations Director 04-50 (適用 OS : Windows 8.1 Enterprise、Windows 8.1 Pro、Windows 8 Enterprise、Windows 8 Pro、Windows Server 2012、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows 7 Enterprise、Windows 7 Professional、Windows 7 Ultimate)

P-2642-8654 Hitachi IT Operations Director Agent 04-50 (適用 OS : Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、Windows Vista、Windows Server 2003、Windows XP)

■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

■ 商標類

HITACHI、HiRDB は、(株) 日立製作所の商標または登録商標です。

Active Directory は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Microsoft および Forefront は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft および Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft および MS-DOS は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Office および Outlook は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Pentium は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。

RSA および BSAFE は、米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows Live は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Media は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows NT は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

インテル、Intel、および Intel Core は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

本製品には、一般社団法人 ソフトウェア資産管理評価認定協会が著作権を有している部分が含まれています。

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by IAIK of Graz University of Technology.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).



本製品は、米国 EMC コーポレーションの RSA BSAFE(R)ソフトウェアを搭載しています。

HITACHI
Inspire the Next

◎ 株式会社 日立製作所



■ マイクロソフト製品のスクリーンショットの使用について

マイクロソフトの許可を得て使用しています。

■ 発行

2015 年 8 月 3021-3-292-10

■ 著作権

All Rights Reserved. Copyright (C) 2013, 2015, Hitachi, Ltd.

Copyright, patent, trademark, and other intellectual property rights related to the "TMEng.dll" file are owned exclusively by Trend Micro Incorporated.

変更内容

変更内容 (3021-3-292-10) Hitachi IT Operations Director 04-50

追加・変更内容	変更箇所
ユーザーアカウントをロックする連続入力失敗の回数、およびパスワードの有効期限を設定できるようにした。	1.2.3、1.4.1、1.4.2、1.4.4、3.7
機器情報の変更履歴を取得できるようにした。	1.2.3、2.7.3、3.3、4.1.4
Windows 2000 を次の製品の適用 OS 外とした。 Hitachi IT Operations Director Agent	1.6.1
設定画面の【エージェント設定】画面の画面名を【エージェント設定とインストールセットの作成】画面に変更した。	1.6.1、4.1.3、7.5
サポートするクラスタソフトウェアから、Microsoft Cluster Service を削除した。	2.7.1、2.7.2
コンフィグレーションファイルで次の内容を設定できるようにした。 エージェントのアンインストール時に機器の廃棄とするか、アンインストールとしないかどうかの設定	4.1.4
Hitachi IT Operations Director Agent のインストール先のフォルダパスを 130 文字以内から 104 バイト以内に変更した。	5.2、5.3
Hitachi IT Operations Director のバージョンアップ時の注意事項を追加した。	5.4

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは、Hitachi IT Operations Director の構築方法を説明したものです。

■ 対象読者

このマニュアルは、次の方にお読みいただくことを前提に説明しています。

- Hitachi IT Operations Director のシステムの構築をしている方
- Hitachi IT Operations Director の構築方法、上書きインストール方法、アンインストール方法、または環境の移行方法について知りたい方

■ マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

第 1 章 最小構成システム（管理用サーバとエージェント）の構築

最小構成システム（管理用サーバとエージェント）の構築方法について説明しています。

第 2 章 各システム構成の構築

システム構成ごとの構築方法について説明しています。

第 3 章 セットアップ内容の変更

管理用サーバでセットアップ時に設定した内容の変更について説明しています。

第 4 章 構築時の設定のカスタマイズ

構築時の設定で、カスタマイズできる項目について説明しています。

第 5 章 製品の上書きインストールおよびコンポーネントのアップデート

Hitachi IT Operations Director の上書きインストール、およびコンポーネント（エージェントおよびネットワークモニタエージェント）のアップデートについて説明しています。

第 6 章 製品のアンインストール

Hitachi IT Operations Director の各種プログラムをアンインストールする方法について説明しています。

第 7 章 環境の移行

Hitachi IT Operations Director で環境を移行する方法について説明しています。

第 8 章 構築関連で使用するコマンド

システムの構築、設定変更、リプレイスなどで使用する、Hitachi IT Operations Director のコマンドについて説明しています。

第 9 章 トラブルシューティング

Hitachi IT Operations Director の構築時にトラブルが発生した場合の対処方法について説明しています。

付録 A 参考情報

Hitachi IT Operations Director を使用する上での参考情報について説明しています。

このマニュアルをお読みになる場合の参考情報は、マニュアル「Hitachi IT Operations Director 導入・設計ガイド」を参照してください。

目次

前書き	2
変更内容	5
はじめに	6

1	最小構成システム（管理用サーバとエージェント）の構築	13
1.1	最小構成システムを構築する流れ	14
1.2	管理用サーバの環境構築	15
1.2.1	Hitachi IT Operations Director のインストールタイプ	15
1.2.2	Hitachi IT Operations Director をインストールする手順	15
1.2.3	管理用サーバをセットアップする手順	17
1.3	製品ライセンスを認証する	19
1.3.1	ライセンス認証をする手順	19
1.3.2	製品ライセンスを追加する手順	20
1.4	操作画面にログインする	22
1.4.1	ログインする手順	22
1.4.2	デフォルトパスワードを変更する手順	23
1.4.3	ユーザーアカウントの情報を設定する手順	24
1.4.4	ユーザーアカウントのロックを解除する手順	24
1.5	組織内の機器を把握する	26
1.5.1	ネットワークに接続されている機器を探索する手順	26
1.5.2	エージェントの導入計画を立案する	28
1.6	エージェントを手動でインストールする	30
1.6.1	インストールセットを作成する手順	30
1.6.2	エージェントをコンピュータに導入する方法	32
1.6.3	Web サーバでエージェントを公開する	33
1.6.4	ファイルサーバでエージェントを公開する	34
1.6.5	エージェントインストール用の媒体（CD-R や USB メモリ）を配布する	35
1.6.6	メールの添付ファイルでエージェントを配布する	36
1.6.7	ログオンスクリプトを利用してエージェントをインストールする	37
1.6.8	ディスクコピーでエージェントをインストールする	39
1.6.9	エージェントを提供媒体からインストールする手順	40
1.6.10	エージェントをセットアップする手順	42
1.7	エージェントを自動でインストールする	44
1.7.1	エージェントのインストール状況を確認する流れ	44
1.7.2	探索と同時にエージェントを自動配信する手順（ネットワークの探索）	45

1.7.3	機器の探索状況の確認	46
1.7.4	最新の探索状況を確認する手順	46
1.7.5	発見した機器を確認する手順	47
1.7.6	管理対象の機器を確認する手順	48
1.7.7	除外対象の機器を確認する手順	48
1.7.8	エージェント未導入のコンピュータに個別配信する手順	49
2	各システム構成の構築	50
2.1	オフライン管理構成システムの構築	51
2.1.1	オフライン管理構成システムを構築する流れ	51
2.2	エージェントレス構成システムの構築	52
2.2.1	エージェントレス構成システムを構築する流れ	52
2.3	サポートサービス連携構成システムの構築	53
2.3.1	サポートサービス連携構成システムを構築する流れ	53
2.4	Active Directory 連携構成システムの構築	54
2.4.1	Active Directory 連携構成システムを構築する流れ	54
2.5	MDM 連携構成システムの構築	55
2.5.1	MDM 連携構成システムを構築する流れ	55
2.6	ネットワーク監視構成システムの構築	56
2.6.1	ネットワーク監視構成システムを構築する流れ	56
2.6.2	ネットワークモニタを有効にする手順	57
2.7	クラスタシステムの構築	59
2.7.1	クラスタシステムを構築する流れ	59
2.7.2	現用系サーバでグループリソースを作成する手順	60
2.7.3	現用系サーバで Hitachi IT Operations Director をセットアップする	64
2.7.4	待機系サーバで Hitachi IT Operations Director をセットアップする	67
3	セットアップ内容の変更	68
3.1	使用するフォルダを変更する手順	69
3.2	操作ログの取得を設定する手順	70
3.3	保存用の変更履歴の出力を設定する手順	74
3.4	ポート番号を変更する手順	76
3.5	通貨単位を変更する手順	78
3.6	配布時に使用されるネットワーク帯域を制御する手順	80
3.7	ログイン制限情報を変更する手順	82
3.8	データベースをアップグレードする手順	84
3.9	データベースを初期化する手順	85
4	構築時の設定のカスタマイズ	86
4.1	最小構成システムの構築時の設定	87

4.1.1	探索条件を設定する手順（ネットワークの探索）	87
4.1.2	ネットワークの探索時に使用する認証情報	88
4.1.3	エージェント設定を追加する手順	89
4.1.4	コンフィグレーションファイルで処理の設定を変更する手順	89
4.1.5	エージェントの監視項目を変更する手順	90
4.2	エージェントレス構成システムの構築時の設定	92
4.2.1	エージェントレスの機器の情報を定期的に更新する手順	92
4.3	サポートサービス連携構成システムの構築時の設定	93
4.3.1	サポートサービスと接続するための情報を設定する手順	93
4.4	Active Directory 連携構成システムの構築時の設定	95
4.4.1	Active Directory と接続するための情報を設定する手順	95
4.4.2	追加管理項目として Active Directory から取得する情報を設定する手順	95
4.4.3	Active Directory に登録されている機器を探索する手順	96
4.4.4	探索条件を設定する手順（Active Directory の探索）	97
4.4.5	機器を管理対象にする手順	98
4.5	MDM 連携構成システムの構築時の設定	99
4.5.1	MDM システムと連携するための情報を設定する手順	99
4.6	ネットワーク監視構成システムの構築時の設定	101
4.6.1	ネットワーク制御リストの機器を編集する手順	101
4.6.2	ネットワーク制御リストの自動更新の設定を編集する手順	101
4.6.3	ネットワークモニタ設定を追加する手順	102
4.6.4	ネットワークモニタ設定の割り当てを変更する手順	102
5	製品の上書きインストールおよびコンポーネントのアップデート	104
5.1	Hitachi IT Operations Director を上書きインストールする手順	105
5.2	エージェントを提供媒体から上書きインストールする手順	107
5.3	Hitachi IT Operations Director のシステム全体をバージョンアップする流れ	108
5.4	Hitachi IT Operations Director をバージョンアップする手順	109
5.5	コンポーネントのアップデート方法	112
5.6	コンポーネントを登録する手順	114
5.7	クラスタシステムで上書きインストールする流れ	115
6	製品のアンインストール	116
6.1	システム全体でのアンインストールの流れ	117
6.2	Hitachi IT Operations Director をアンインストールする手順	118
6.3	エージェントをアンインストールする手順	119
6.4	ネットワークモニタを無効にする手順	121
6.5	コントローラをアンインストールする手順	123
6.6	クラスタシステムで Hitachi IT Operations Director をアンインストールする手順	124

7	環境の移行 125
7.1	管理用サーバをリプレースする手順 126
7.2	エージェント導入済みのコンピュータをリプレースする手順 132
7.3	ネットワークモニタを有効にしたコンピュータをリプレースする手順 133
7.4	システム構成要素のホスト名および IP アドレスを変更する 134
7.4.1	管理用サーバのホスト名を変更する手順 134
7.4.2	管理用サーバの IP アドレスを変更する手順 134
7.4.3	クラスタシステムの論理ホスト名を変更する手順 134
7.4.4	クラスタシステムの論理 IP アドレスを変更する手順 135
7.5	エージェントが接続する管理用サーバを切り替える手順 137
8	構築関連で使用するコマンド 138
8.1	コマンドを実行する手順 139
8.2	コマンドの説明形式 141
8.3	updatesupportinfo (サポートサービスからの情報の登録) 142
8.4	exportdb (バックアップの取得) 145
8.5	importdb (バックアップデータのリストア) 149
8.6	stopservice (サービス停止) 153
8.7	getlogs (トラブルシュート用情報の取得) 155
8.8	getinstlogs (インストール時のトラブルシュート用情報の取得) 157
8.9	resetnid.vbs (ホスト識別子のリセット) 159
9	トラブルシューティング 162
9.1	構築時のトラブルシューティングの流れ 163
9.2	最小構成システムの構築時のトラブルシューティング 165
9.2.1	管理用サーバ構築時のトラブルシューティング 165
9.2.2	エージェントインストール時のトラブルシューティング 166
9.2.3	1 台のコンピュータに対して 2 つの機器情報が表示される場合のトラブルシューティング 168
9.3	オフライン管理構成システムの構築時のトラブルシューティング 169
9.3.1	オフライン管理からオンライン管理に切り替える手順 169
9.3.2	オンライン管理からオフライン管理に切り替える手順 170
9.4	エージェントレス構成システムの構築時のトラブルシューティング 171
9.5	サポートサービス連携構成システムの構築時のトラブルシューティング 172
9.6	Active Directory 連携構成システムの構築時のトラブルシューティング 173
9.7	MDM 連携構成システムの構築時のトラブルシューティング 174
9.8	ネットワーク監視構成システムの構築時のトラブルシューティング 175
9.9	クラスタシステムの構築時のトラブルシューティング 176
付録 177	
付録 A	参考情報 178

付録 A.1	ポート番号一覧	178
付録 A.2	エージェントの環境を変更した場合の認識方法	180
付録 A.3	各バージョンの変更内容	181

索引 183

1

最小構成システム（管理用サーバとエージェント） の構築

ここでは、最小構成システム（管理用サーバとエージェント）の構築方法について説明します。

最小構成システムを構築したあとは、設定を変更したり、ほかのシステム構成要素を導入したりして、管理の目的に応じたシステム構成を構築してください。最小構成システム以外のシステムを構築する場合は、先に「[2. 各システム構成の構築](#)」を参照してください。

1.1 最小構成システムを構築する流れ

最小構成システムを構築するには、管理用サーバを構築したあとで、管理対象とするコンピュータにエージェントを導入します。

1. 管理用サーバを構築します。
2. Hitachi IT Operations Director の製品ライセンスを認証します。
3. 操作画面にログインしてユーザーアカウントの情報を設定します。
4. 事前に組織内の機器を把握して、どのコンピュータにどの方法でエージェントを導入するかを計画します。
5. Hitachi IT Operations Director の管理対象とするコンピュータに、エージェントを導入します。

最小構成システムの構築が完了します。

関連リンク

- [1.2 管理用サーバの環境構築](#)
- [1.3 製品ライセンスを認証する](#)
- [1.4 操作画面にログインする](#)
- [1.5 組織内の機器を把握する](#)
- [1.6 エージェントを手動でインストールする](#)
- [1.7 エージェントを自動でインストールする](#)

1.2 管理用サーバの環境構築

管理用サーバは、Hitachi IT Operations Director をインストールおよびセットアップして構築します。

1.2.1 Hitachi IT Operations Director のインストールタイプ

Hitachi IT Operations Director のインストールタイプには、次の 2 種類があります。インストール時に、目的に応じて選択してください。

簡単インストール

最小限の操作でインストールとセットアップを完了できます。インストールおよびセットアップには、デフォルトの値が設定されます。特別な設定をする必要がない場合は、この方法をお勧めします。

カスタムインストール

各種設定をしながらインストールを進めます。インストール終了後にセットアップを実行してデータベースを作成する必要があります。インストールおよびセットアップで任意の値を設定したい場合は、この方法をお勧めします。

1.2.2 Hitachi IT Operations Director をインストールする手順

Hitachi IT Operations Director のインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

注意事項

ユーザーアカウント制御 (UAC) がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

注意事項

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- システムドライブ:¥program files¥WindowsApps 配下のフォルダ

- 仮想プロビジョニングによって作成した記憶域のフォルダ

注意事項

インストール前は、すべての Windows アプリケーションを終了させてください。誤って Hitachi IT Operations Director のプログラムを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、Hitachi IT Operations Director のプログラムが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. サービス (IT Operations Director Service) を停止してください。
3. 上書きインストールを再実行してください。サービスが開始されます。

Hitachi IT Operations Director をインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される [日立総合インストーラ] ダイアログで、[Hitachi IT Operations Director] を選択して、[インストール実行] ボタンをクリックします。
3. インストール開始のダイアログで [次へ] ボタンをクリックします。
4. [使用許諾契約] ダイアログで、内容を確認してから [使用許諾契約の条項に同意します] を選択し、[次へ] ボタンをクリックします。
5. [インストールタイプ] ダイアログで、インストールタイプを選択して [次へ] ボタンをクリックします。
簡単インストールを選択した場合は、手順 7.へ進んでください。
6. [ユーザー登録] ダイアログで、ユーザー名と会社名を入力して [次へ] ボタンをクリックします。
7. [インストール先のフォルダ] ダイアログで、インストール先のフォルダを指定して [次へ] ボタンをクリックします。
簡単インストールの場合は、ここでデータベースの作成先フォルダも指定してください。
8. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、[インストール] ボタンをクリックします。
インストールが実行されます。インストール内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。
9. インストールが完了したら、[完了] ボタンをクリックします。

Hitachi IT Operations Director のインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

簡単インストールの場合は、インストール時にセットアップも自動で実行されるので、インストール完了後すぐに Hitachi IT Operations Director にログインして操作を開始できます。

カスタムインストールの場合は、データベースを作成するために、インストール完了後にセットアップを実行する必要があります。インストール完了時に、[セットアップ] をチェックした場合、インストールが完了するとセットアップが自動で起動します。

ポイント

インストールが完了すると、デスクトップに操作画面へログインするためのショートカットが作成されます。ただし、カスタムインストールの場合、ショートカットはセットアップが完了するまで使用できません。

1.2.3 管理用サーバをセットアップする手順

Hitachi IT Operations Director をカスタムインストールでインストールした場合、データベースの作成や各種環境設定のために、インストール直後にセットアップを実行する必要があります。

管理用サーバをセットアップするには：

1. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
2. セットアップ画面で、[次へ] ボタンをクリックします。
3. [セットアップの選択] 画面で、セットアップの種類を選択して [次へ] ボタンをクリックします。
インストール後の初回セットアップ時には、この画面は表示されません。
4. [クラスタ環境] 画面で、クラスタシステムを運用するための設定をして、[次へ] ボタンをクリックします。
5. [フォルダの設定] 画面で、Hitachi IT Operations Director が使用する各種フォルダを指定して [次へ] ボタンをクリックします。
手順 4. でクラスタ環境を使用する場合に [待機系] を選択したときは、手順 5. ～手順 12. は不要です。
6. [操作ログの設定] 画面で、操作ログを取得するかどうかを設定して [次へ] ボタンをクリックします。
操作ログを取得しない場合は、手順 9. へ進んでください。
7. 表示された画面で、操作ログを保管するかどうかを設定して、[次へ] ボタンをクリックします。
8. 表示された画面で、管理対象の機器の台数、操作ログのデータベース格納最大日数、および操作ログのデータベースフォルダを設定して、[次へ] ボタンをクリックします。

9. [保存用の変更履歴の出力設定] 画面で、保存用の変更履歴を定期的に出力するかどうかを設定して [次へ] ボタンをクリックします。
10. [ポート番号の設定] 画面で、Hitachi IT Operations Director が使用するポート番号を設定して [次へ] ボタンをクリックします。
11. [その他の設定] 画面で、操作画面に表示される通貨記号、および配布の機能を使用するときに流量制御するかどうかを設定して [次へ] ボタンをクリックします。
12. 表示された画面で、アカウントをロックする連続入力失敗の回数、およびユーザパスワードの有効日数を設定して [次へ] ボタンをクリックします。
13. [セットアップの確認] 画面で、セットアップ内容に問題がないことを確認し、[次へ] ボタンをクリックします。
セットアップが実行されます。セットアップ内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。
14. セットアップの完了を示す画面で、[OK] ボタンをクリックします。
[コンポーネントを登録する] が表示された場合は、セットアップに続いてコンポーネントを登録するかどうかを設定してから [OK] ボタンをクリックしてください。
コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムを管理用サーバに登録しておくことで、エージェントを配信したり、ネットワークモニタエージェントを操作画面からインストールしたりできるようになります。
コンポーネントを登録する場合は、[コンポーネントの登録] ダイアログが表示されるので、コンポーネントの登録とアップデートについて設定します。

ポイント

インストールの続きでセットアップを起動した場合は、セットアップの完了を示す画面上でコンポーネントのアップデートについて設定できます。

コンポーネントのアップデートについては、「[5.5 コンポーネントのアップデート方法](#)」を参照してください。

セットアップが完了し、設定した内容で管理用サーバが動作するようになります。

ポイント

カスタムインストール後に初めてセットアップする場合、セットアップ時にデータベースが新規作成されます。

1.3 製品ライセンスを認証する

ここでは、製品ライセンスを認証する方法について説明します。

1.3.1 ライセンス認証をする手順

Hitachi IT Operations Director にログインするためには、あらかじめライセンス認証をしておく必要があります。ライセンス認証をするには、[ライセンス認証をしましょう] ウィザードを実行します。

[ライセンス認証をしましょう] ウィザードを実行するには：

1. ログイン画面を表示します。
2. [ライセンス] ボタンをクリックします。
3. 表示されたダイアログで [認証を開始] ボタンをクリックします。

[ライセンス認証をしましょう] ウィザードが実行されます。

ポイント

[ライセンス認証をしましょう] ウィザードは、設定画面の [製品ライセンス] - [製品ライセンスの設定] 画面からも実行できます。

ポイント

試用版を使用する場合も、[ライセンス認証をしましょう] ウィザードで試用版をライセンス認証する必要があります。

[ライセンス認証をしましょう] ウィザードでは、次の 2 種類の方法でライセンス認証ができます。ご利用の環境に応じて、適切な方法を選択してください。

- オンラインでの認証

購入すると取得できるライセンス認証キーを入力すると、自動的にライセンス認証サーバに接続してライセンス認証をします。管理者が操作するコンピュータがインターネットに接続できる環境の場合は、この方法をお勧めします。オンラインでの認証の流れを次に示します。

1. [ライセンス認証をしましょう] ウィザードを表示します。
2. 使用許諾書の内容を確認します。
3. ライセンス認証キーを入力します。

ライセンス認証が完了します。

- オフラインでの認証

Web サイトを利用してライセンス登録用ファイルを取得します。そのあと、ライセンス登録用ファイルを使ってオフラインでライセンス認証をします。管理者が操作するコンピュータがインターネットに接続できない場合は、この方法を使用してください。オフラインでの認証の流れを次に示します。

1. [ライセンス認証をしましょう] ウィザードを表示します。
2. 使用許諾書の内容を確認します。
3. ライセンス認証キーを基に、送信用キーファイルを生成します。
4. Web サイト経由で、送信用キーファイルを基にライセンス登録用ファイルを発行してもらいます。
この手順は、インターネットに接続できるコンピュータで操作します。
5. 発行されたライセンス登録用ファイルを入力します。

ライセンス認証が完了します。

ポイント

オフライン認証の場合、手順 3.の終了後にいったんウィザードを終了してもかまいません。ライセンス登録用ファイルが発行されてから、再度 [ライセンス認証をしましょう] ウィザードを実行してライセンス登録用ファイルを入力すれば、製品ライセンスを認証できます。

関連リンク

- [1.3.2 製品ライセンスを追加する手順](#)

1.3.2 製品ライセンスを追加する手順

組織内の機器を Hitachi IT Operations Director で管理するためには、製品ライセンスが必要です。

製品ライセンスを追加するには：

1. 製品ライセンスを追加購入します。
2. 設定画面を表示します。
3. メニューエリアで [製品ライセンス] - [製品ライセンスの設定] を選択します。
4. [認証を開始] ボタンをクリックします。

[ライセンス認証をしましょう] ウィザードが実行されます。ウィザードに沿って、製品ライセンスを認証してください。新しい製品ライセンスが追加されます。

ポイント

「ライセンス認証をしましょう」ウィザードは、ログイン画面の「ライセンス」ボタンをクリックして表示されるダイアログからも実行できます。

1.4 操作画面にログインする

ここでは、Hitachi IT Operations Director の操作画面にログインする方法について説明します。

1.4.1 ログインする手順

ログイン画面ではユーザーの認証をします。認証に成功すると Hitachi IT Operations Director にログインできます。

初めてログインする場合は、Hitachi IT Operations Director のライセンスを認証する必要があります。ライセンスを認証するには、[ライセンス] ボタンをクリックしてください。

ログインするには：

1. Web ブラウザのアドレスバーに次の URL を入力します。

http://管理用サーバの IP アドレスまたはホスト名:管理者のコンピュータからの接続受付ポート番号
※/Director/Director.jsp

注※ セットアップの [ポート番号の設定] 画面で設定したポート番号です。簡単インストール時にはデフォルトの「31080」が設定されています。

2. ユーザー ID とパスワードを入力します。

3. [ログイン] ボタンをクリックします。

ユーザーアカウントの認証に成功するとホーム画面が表示されます。

デフォルトのユーザー ID は「system」、パスワードは「manager」です。デフォルトのユーザー ID とパスワードでログインすると [パスワードの変更] ダイアログが表示されるので、パスワードを変更してください。なお、新しく追加したユーザーアカウントで初めてログインする場合も、[パスワードの変更] ダイアログが表示されます。

ポイント

パスワードの有効期限は、セットアップ時に [その他の設定] 画面で、ユーザーパスワードの有効日数として指定した日数です。有効期限の 7 日前からログイン時にパスワードの変更が要求されるので、新しいパスワードに変更してください。パスワードの有効期限を過ぎると、ログイン時に [パスワードの変更] ダイアログが表示されます。

注意事項

セットアップ時に [その他の設定] 画面で、アカウントをロックする連続入力失敗の回数が指定されている場合に、指定された回数続けてログインに失敗するとユーザーアカウントがロックされま

す。ユーザーアカウントがロックされると、ロックが解除されるまでそのユーザーアカウントではログインできません。

関連リンク

- [1.4.4 ユーザーアカウントのロックを解除する手順](#)

1.4.2 デフォルトパスワードを変更する手順

Hitachi IT Operations Director にビルトインアカウントで初めてログインするとき、または新規に作成したユーザーアカウントで初めてログインするときは、パスワードの変更が要求されます。また、ユーザーアカウント管理権限を持つ管理者によって、ユーザーアカウントのパスワードが変更された場合、次回ログイン時にパスワードの変更が要求されます。セキュリティ確保のため、デフォルトパスワードは必ず変更してください。パスワードを変更すると、次のログイン時から変更後のパスワードを使う必要があります。

ポイント

パスワードの有効期限は、セットアップ時に [その他の設定] 画面で、ユーザーパスワードの有効日数として指定した日数です。有効期限の 7 日前からログイン時にパスワードの変更が要求されるので、新しいパスワードに変更してください。パスワードの有効期限を過ぎると、ログイン時に [パスワードの変更] ダイアログが表示されます。

ポイント

脆弱なパスワードを設定すると、自分のユーザーアカウントが不正に使われるおそれがあります。例えば、次のような設定方針で強固なパスワードを利用することをお勧めします。

- 大文字、小文字、数字、記号の組み合わせである
- 連続した文字列（12345 など）ではない
- 自分や親しい人の名前または誕生日、辞書に掲載されている単語ではない

ログイン中のユーザーアカウントのパスワードを変更したい場合は、[ログアウト] ボタンの左側にあるユーザー ID のリンクをクリックして表示されるダイアログからパスワードを変更できます。

ユーザーアカウント管理権限を持つ管理者の場合は、設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面から、各ユーザーアカウントのパスワードを変更できます。

1.4.3 ユーザーアカウントの情報を設定する手順

Hitachi IT Operations Director にログインしたあとは、ユーザーアカウントの情報を設定してください。

[ログアウト] ボタンの左側にあるユーザー ID のリンクをクリックすると、表示されるダイアログでユーザーアカウントの情報を編集できます。

ユーザーアカウントには、次の情報を設定します。

- ユーザーアカウントを使用する利用者の名
- 利用者のメールアドレス

ユーザーアカウントにメールアドレスを設定しておくことで、そのメールアドレスに対してダイジェストレポートを送付したり、探索完了、イベントの発生を通知したりできます。操作画面を頻繁にチェックすることなく運用状況を把握できるようになるので、メールアドレスを設定しておくことをお勧めします。なお、これらの通知を受け取るには、メールアドレスの設定のほかに、ダイジェストレポートの送付先の設定、探索条件の設定、およびイベント通知の設定が必要です。

ポイント

ユーザーアカウントの情報は、設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面からも設定できます。[ユーザーアカウントの管理] 画面では、ユーザーアカウントを新規に追加することもできます。

1.4.4 ユーザーアカウントのロックを解除する手順

アカウントをロックする連続入力失敗の回数が指定されている場合に、指定された回数続けてログインに失敗するとユーザーアカウントがロックされます。ロックされたユーザーアカウントを使用するためには、ロックを解除する必要があります。

ユーザーアカウントのロックを解除するには：

1. ユーザーアカウント管理権限を持つユーザーでログインします。
2. 設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面を表示します。
3. ロックされたユーザーアカウントの [編集] ボタンをクリックします。
4. 表示されたダイアログで、[アカウントロック状態] の [解除] を選択します。

ユーザーアカウントのロックが解除されます。

ポイント

ユーザーアカウント管理権限を持つ別のユーザーアカウントがない場合は、管理用サーバを再起動してください。ユーザーアカウントのロックが解除されます。

1.5 組織内の機器を把握する

エージェントを導入するコンピュータを決定するために、組織内の機器の現状を把握する必要があります。

管理台帳がメンテナンスできていない、管理台帳が手もとにないなど、機器の現状を把握できていない場合は、Hitachi IT Operations Director を利用して機器を探索してください。探索によって組織内の機器の情報を収集できます。組織内の機器を把握したら、エージェントの導入計画を立案します。なお、探索と同時にエージェントを自動配信することもできます。

管理台帳などで組織内の機器の現状を把握できている場合は、機器を探索する必要はありません。エージェントの導入計画を立案します。

関連リンク

- [1.5.2 エージェントの導入計画を立案する](#)

1.5.1 ネットワークに接続されている機器を探索する手順

機器を探索する方法の一つです。ネットワークに接続されている機器を探索できます。

設定画面の [機器の探索] – [探索条件の設定] – [ネットワークの探索] 画面で、探索する IP アドレスの範囲や探索時に使用する認証情報などを設定します。[探索を開始] ボタンをクリックすると、設定したスケジュールに従って探索が開始されます。

ネットワークに接続されている機器を探索するには：

1. 設定画面の [機器の探索] – [探索条件の設定] – [ネットワークの探索] 画面を表示します。
2. [探索範囲の設定内容] で、探索したい IP アドレスの範囲を設定します。

デフォルトで、「管理用サーバセグメント」という名称の探索範囲が設定されています。管理用サーバセグメントとは、管理用サーバが含まれるネットワークセグメントのことです。

注意事項

期間を指定して集中的に探索する場合は、探索範囲に含まれる IP アドレスの数が 50,000 件以下になるように設定してください。IP アドレスの数が 50,000 件よりも多いと、ネットワーク探索が停止することがあります。

3. [認証情報] で、探索時に使用する認証情報を設定します。
4. [探索範囲の設定内容] で、各探索範囲に使用する認証情報を設定します。

注意事項

探索範囲の機器に、ログオンを一定回数失敗し、アカウントをロックするような設定がされている場合は、探索範囲ごとに特定の認証情報を割り当ててください。[すべて]を選択すると、機器に対してすべての認証情報を試します。そのため、利用者が知らないうちにアカウントがロックされてしまうおそれがあります。

注意事項

[すべて]を選択すると、認証情報を1つずつ使用して機器にアクセスを試みます。そのため、通信回数が増えネットワークの負荷が高くなります。ネットワークの負荷を考慮した上で選択してください。

5. [探索スケジュール] で探索スケジュールを設定します。
6. [発見した機器への操作] で、発見した機器を自動的に管理対象にするか、エージェントを自動配信するかを設定します。
7. 探索の完了を管理者にメールで通知したい場合は、[完了通知] で通知先を設定します。
8. 画面右上の [探索を開始] ボタンをクリックします。
9. 表示されるダイアログで探索の範囲を確認して、[OK] ボタンをクリックします。
[期間を指定して集中的に探索する] をチェックすると、指定した期間は探索が終了したらすぐに次の探索が開始され、絶え間なくネットワークが探索されるようになります。このため、運用の初期段階で、できるだけ多くの機器を発見したい場合にチェックすることをお勧めします。例えば、1回目の探索時に電源がOFFのため発見できなかった機器があっても、探索を繰り返すことで、2回目以降の探索で発見できる可能性が高くなります。

注意事項

[期間を指定して集中的に探索する] をチェックすると、探索が終了したらすぐに次の探索を繰り返します。そのため、設定した期間中はネットワークの負荷が高くなります。ネットワークの負荷を考慮した上で選択してください。

[機器の探索] - [探索履歴の確認] - [ネットワークの探索] 画面に移動し、設定したスケジュールに従って探索が実行されます。

関連リンク

- [4.1.1 探索条件を設定する手順（ネットワークの探索）](#)
- [1.7.3 機器の探索状況の確認](#)

1.5.2 エージェントの導入計画を立案する

組織内の機器を把握したら、どのコンピュータにエージェントを導入するか、どのような方法でエージェントを導入するかを検討します。

エージェントを導入するコンピュータ

組織内で利用されているコンピュータのうち、Hitachi IT Operations Director によるセキュリティ管理やソフトウェア配布の対象としたいコンピュータにエージェントを導入します。

エージェントを導入したコンピュータは、自動的に Hitachi IT Operations Director の管理対象になります。コンピュータを管理対象にすると Hitachi IT Operations Director のライセンスが消費されるため、ライセンス数を考慮して、エージェントを導入するコンピュータを決定してください。

ポイント

管理用サーバをセキュリティ管理の対象にする場合、利用者のコンピュータと同様にエージェントをインストールします。

エージェントの導入方法

エージェントの導入方法には、手動でインストールする方法と自動でインストールする方法があります。

どのインストール方法を選択するかは、インストールする際に重視するポイントによって異なります。各方法を確認して、ご使用の環境に合ったインストール方法を決定してください。

エージェントを手動でインストールする

まずインストールセットを作成します。その後、インストールセットを利用してコンピュータにエージェントをインストールします。手動でインストールするには、次の 7 種類の方法があります。

- Web サーバでエージェントを公開する
- ファイルサーバでエージェントを公開する
- エージェントインストール用の媒体（CD-R や USB メモリ）を配布する
- メールの添付ファイルでエージェントを配布する
- ログオンスクリプトを利用してエージェントをインストールする
- ディスクコピーでエージェントをインストールする
- エージェントを提供媒体からインストールする

エージェントを自動でインストールする

管理用サーバから各コンピュータに対して、エージェントを自動で配信します。自動でインストールするには、次の 2 種類の方法があります。

- 探索と同時にエージェントを自動配信する
- エージェント未導入のコンピュータに個別配信する

関連リンク

- [1.6 エージェントを手動でインストールする](#)
- [1.7 エージェントを自動でインストールする](#)

1.6 エージェントを手動でインストールする

エージェントを手動でインストールするためには、まずエージェントのインストールセットを作成します。その後、インストールセットを利用してコンピュータにエージェントをインストールします。

インストールセットの作成方法については、「[1.6.1 インストールセットを作成する手順](#)」を参照してください。

インストールセットを利用したエージェントのインストール方法は複数あります。インストール方法は、インストールする際に重視するポイントによって異なります。各方法を確認して、ご使用の環境に合ったインストール方法を決定してください。

利用者にインストールの作業だけをさせる場合

インストールセットを利用者が起動するように環境を準備しておくことで、利用者にセットアップの作業をさせることなく、エージェントをインストールします。利用者にインストールの作業だけをさせる方法を次に示します。

- [1.6.3 Web サーバでエージェントを公開する](#)
- [1.6.4 ファイルサーバでエージェントを公開する](#)
- [1.6.5 エージェントインストール用の媒体（CD-R や USB メモリ）を配布する](#)
- [1.6.6 メール添付ファイルでエージェントを配布する](#)

利用者にインストールの作業自体をさせたくない場合

インストールセットをファイルサーバに格納します。その後、ドメインコントローラにログオンスクリプトを登録しておくことで、利用者が Windows にログオンしたときに、自動的にエージェントがインストールされます。利用者にインストールの作業自体をさせない方法を次に示します。

- [1.6.7 ログオンスクリプトを利用してエージェントをインストールする](#)

利用者にコンピュータを配布する前にインストールしたい場合

利用者にコンピュータを配布する前に、配布するコンピュータのモデルとなるコンピュータに、インストールセットを使ってエージェントをインストールします。次に、モデルとなるコンピュータのディスク全体を、専用のツールやソフトウェアを使用して配布前のコンピュータにディスクコピーします。利用者にコンピュータを配布する前にインストールする方法を次に示します。

- [1.6.8 ディスクコピーでエージェントをインストールする](#)

これらのほかに、提供媒体を使用してエージェントを手動でインストールする方法もあります。この場合、セットアップの作業も必要です。

1.6.1 インストールセットを作成する手順

組織内のコンピュータにエージェントをインストールして管理する場合、インストールセットを作成します。インストールセットは Web ポータルに公開して利用者にダウンロードしてもらったり、CD/DVD

に記録して配布したりします。利用者はインストールセットを自分のコンピュータで実行することで、簡単にエージェントをインストールできます。

インストールセットを作成する手順を次に示します。

インストールセットを作成するには：

1. 画面上部の [実行] メニュー－ [機器の管理を始めましょう] を選択します。
2. 表示されたダイアログで [次へ] ボタンをクリックします。
3. コンピュータに適用したいエージェント設定を選択して、[作成] ボタンをクリックします。

エージェント設定とは、各エージェントの動作を設定したものです。エージェント設定は、設定画面の [エージェント]－ [エージェント設定とインストールセットの作成] 画面で追加できます。

ウィザードに沿って次に示す項目の情報を入力し、[次へ] ボタンをクリックしてください。

インストールフォルダの設定

エージェントのインストール先を変更できます。

インストール先を変更したい場合は、[インストールフォルダ] にエージェントのインストール先を入力してください。

アカウントの設定

エージェントをインストールするために、Administrator 権限を持つアカウント情報を設定するかどうかを選択できます。この設定は、OS が Windows XP、および Windows Server 2003 のコンピュータにエージェントをインストールする場合に限り有効になります。

エージェントをインストールするためには、対象コンピュータの Administrator 権限が必要です。ここで、Administrator 権限を持つアカウントを設定すると、Administrator 権限を持たない利用者がエージェントをインストールするとき、設定したアカウントでインストールが実行されます。Administrator 権限は、エージェントをインストールするときだけ使用されるため、権限を制限したい利用者のコンピュータにエージェントをインストールする場合に便利です。

4. インストールセットをダウンロードするダイアログで [保存] ボタンをクリックします。

デフォルトで表示されるファイル名は「ITODAg.exe」です。

インストールセットが作成され、ダウンロードが開始されます。

ポイント

設定画面の [エージェント]－ [エージェント設定とインストールセットの作成] 画面でも、インストールセットを作成できます。コンピュータに適用したいエージェント設定の [インストールセットを作成] ボタンをクリックしてください。表示されるダイアログで情報を入力して [OK] ボタンをクリックすると、インストールセットが作成され、ダウンロードが開始されます。

関連リンク

- [4.1.3 エージェント設定を追加する手順](#)
- [1.6.2 エージェントをコンピュータに導入する方法](#)

1.6.2 エージェントをコンピュータに導入する方法

インストールセットを作成したら、インストールセットを利用してエージェントをコンピュータに導入します。インストールセットの利用例を次に示します。

Web サーバでエージェントを公開する

Web サーバにインストールセットを格納して、組織内のサイトからダウンロードできるようにします。コンピュータの利用者は、組織内のサイトからインストールセットをダウンロードしてエージェントをインストールします。

ファイルサーバでエージェントを公開する

ファイルサーバにインストールセットを格納して、ファイルサーバにアクセスしてダウンロードできるようにします。コンピュータの利用者は、ファイルサーバからインストールセットをダウンロードしてエージェントをインストールします。

エージェントインストール用の媒体を配布する

インストールセットを格納した媒体（CD-R や USB メモリ）を作成して、この媒体をコンピュータの利用者に配布します。コンピュータの利用者は、受け取った媒体からエージェントをインストールします。

メールの添付ファイルでエージェントを配布する

インストールセットをメールに添付して、コンピュータの利用者に送信します。メールを受け取ったコンピュータの利用者は、添付されたファイルを実行してエージェントをインストールします。

ログオンスクリプトを利用してエージェントをインストールする

インストールセットを作成して、ドメインコントローラにインストールセットを実行するログオンスクリプト用のバッチファイルを格納します。コンピュータの利用者が OS にログオンしたときに、自動的にエージェントがインストールされます。

ディスクコピーでエージェントをインストールする

モデルとなるコンピュータにエージェントをインストールします。このコンピュータのディスク全体をバックアップします。エージェントを導入するコンピュータにバックアップデータをリストアすることでエージェントがインストールされます。

関連リンク

- [1.6.3 Web サーバでエージェントを公開する](#)
- [1.6.4 ファイルサーバでエージェントを公開する](#)
- [1.6.5 エージェントインストール用の媒体（CD-R や USB メモリ）を配布する](#)

- 1.6.6 メール添付ファイルでエージェントを配布する
- 1.6.7 ログオンスクリプトを利用してエージェントをインストールする
- 1.6.8 ディスクコピーでエージェントをインストールする

1.6.3 Web サーバでエージェントを公開する

管理者は、作成したインストールセットを組織内の Web サーバに格納したあと、組織内のサイトからダウンロードできるようにして、利用者に公開します。

利用者はそのページにアクセスしてエージェントをインストールします。

ポイント

Web サーバに格納したファイルを直接ダウンロードできる URL を公開する方法もあります。

メリット

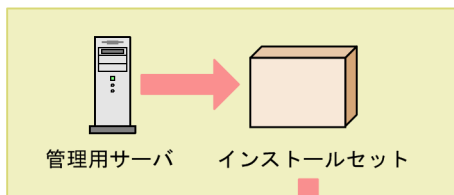
利用者にサイトの URL を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。また、Web システムを利用するので、アクセス制御しなくてもサーバ側にセキュリティ上の問題が発生しません。

デメリット

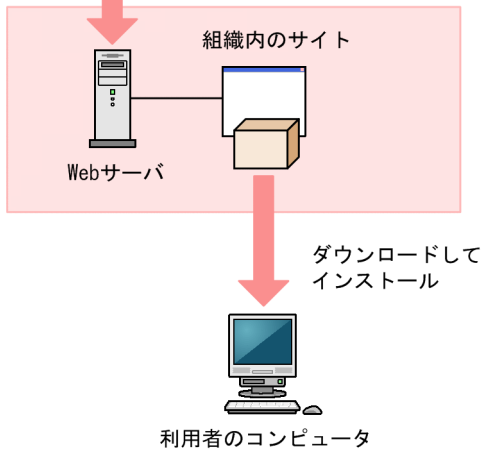
組織内に Web サーバを構築できる環境、および Web サーバにアクセスできる環境が必要です。

Web サーバからエージェントをインストールするイメージを、次の図に示します。

インストールセットの作成



インストールセットの格納



関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)

1.6.4 ファイルサーバでエージェントを公開する

管理者は、ファイル共有できるファイルサーバにインストールセットを格納します。利用者は、ファイルサーバにアクセスしてエージェントをインストールします。

メリット

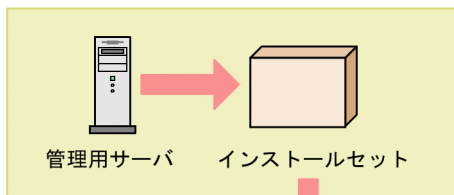
利用者にインストールセットの格納先を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

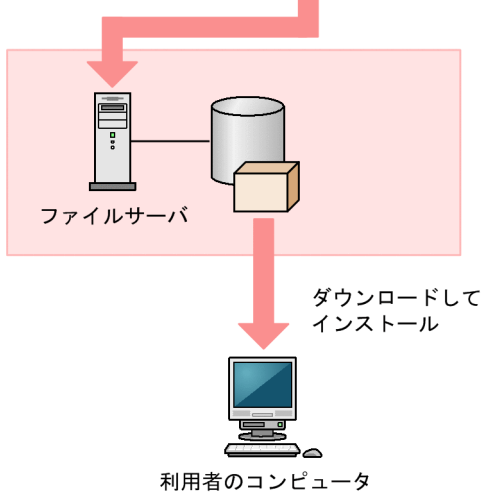
ファイル共有できる環境が必要です。また、ファイル共有の参照先を公開するため、公開の範囲や権限などサーバ側で確実にアクセス制御をしておく必要があります。

ファイル共有でエージェントをインストールするイメージを、次の図に示します。

インストールセットの作成



インストールセットの格納



関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)

1.6.5 エージェントインストール用の媒体（CD-R や USB メモリ）を配布する

管理者は、インストールセットのデータを媒体（CD-R や USB メモリ）に書き込みます。そして、その媒体を利用者に配布します。利用者は、配布された媒体を使用してエージェントをインストールします。

メリット

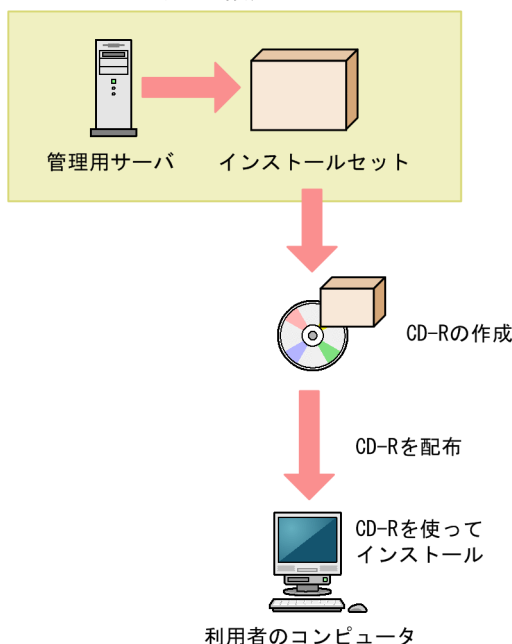
Web ページにセキュリティ管理用のページを作成したり、共有フォルダの環境を作成したりする必要がありません。この方法は、エージェントをインストールするコンピュータの台数が少ない場合に有効です。また、ネットワークの通信速度が遅い場合に、ネットワークに負荷をかけないでエージェントをインストールできます。利用者のコンピュータを構築するユーザー専用、エージェントのプログラムを保持できることにもなります。

デメリット

必要な枚数分だけデータを媒体に書き込んで利用者に配布する必要があるため、展開に時間が掛かります。

CD-R の場合を例に、媒体を配布してエージェントをインストールするイメージを、次の図に示します。

インストールセットの作成



ポイント

Autorun.inf を作成してインストールセットと一緒に CD-R に格納しておくと、媒体をコンピュータに接続した際に、自動でインストールが開始されます。インストールセットのファイル名が「ITODAg.exe」の場合の Autorun.inf の作成例は次のとおりです。

```
[Autorun]
```

```
open=ITODAg.exe
```

関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)

1.6.6 メールの添付ファイルでエージェントを配布する

管理者は、インストールセットをメールに添付して利用者に送信します。利用者は、添付ファイルをダブルクリックしてエージェントをインストールします。

メリット

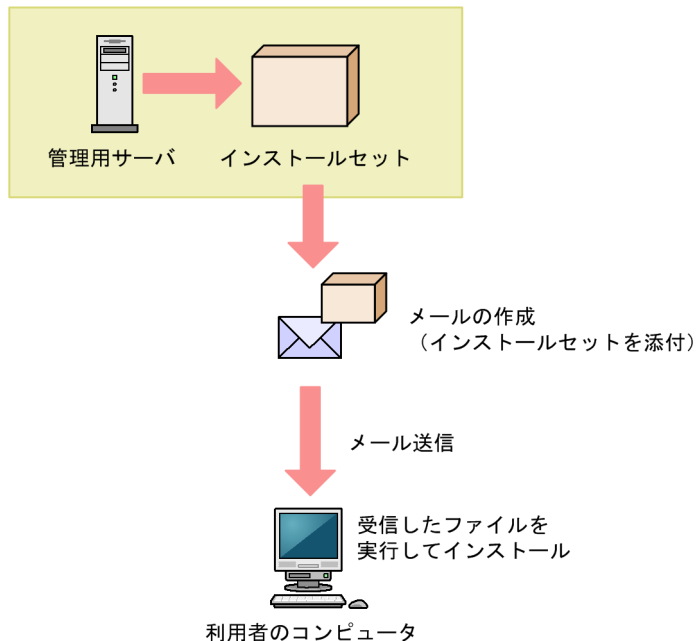
利用者にメールを一斉送信することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

インストールセットの容量は、約 35 メガバイトです。そのため、インストールセットを添付して一斉に多数の宛先にメールを送信すると、メールサーバに負担が掛かったり、添付ファイルの容量に制限があるとメールを送信できなくなったりします。

メールの添付ファイルでエージェントをインストールするイメージを、次の図に示します。

インストールセットの作成



関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)

1.6.7 ログオンスクリプトを利用してエージェントをインストールする

管理者は、インストールセットをファイルサーバに格納します。そのあと、インストールセットを実行するログオンスクリプト用のバッチファイルを作成し、Active Directory サーバに格納しておきます。利用者が Windows にログオンしたときに、自動的にエージェントがインストールされます。なお、すでにエージェントがインストールされている場合はインストールされません。

ログオンスクリプト用のバッチファイルの作成例を次に示します。

```
if %PROCESSOR_ARCHITECTURE%==AMD64 (  
if not exist "%ProgramFiles(x86)%¥Hitachi¥Director Agent¥bin¥jdnnglogon.exe" (  
start /w ¥¥サーバ名¥共有フォルダ名¥ITODAg.exe  
)  
) else (  

```

```
if not exist "%ProgramFiles%\Hitachi\Director Agent\bin\jdnnglogon.exe" (  
start /w %¥¥サーバ名¥共有フォルダ名¥ITODAg.exe  
)  
)
```

メリット

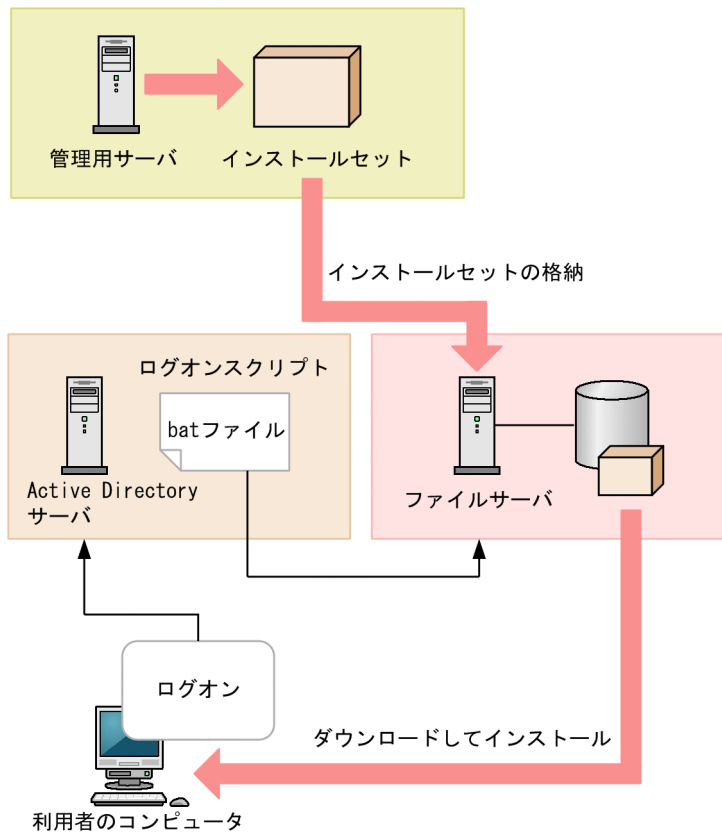
ログオンスクリプトを利用することで、利用者に作業してもらうことなくエージェントを自動的にインストールできます。そのため、利用者の操作ミスによるトラブルを避けられます。

デメリット

ファイルサーバおよびファイルサーバにアクセスできる環境が必要です。また、利用者のコンピュータはドメインで管理されていて、ログオンスクリプトを実行できる環境が必要です。

ログオンスクリプトを利用してエージェントを自動インストールするイメージを、次の図に示します。

インストールセットの作成



関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)

1.6.8 ディスクコピーでエージェントをインストールする

利用者にコンピュータを配布する前に、配布するコンピュータのモデルとなるコンピュータに、インストールセットを使ってエージェントをインストールします。また、インストールが完了したら、モデルとなるコンピュータで`resetnid.vbs` コマンドを実行し、機器を識別するための ID（ホスト識別子）をリセットしておきます。次に、モデルとなるコンピュータのディスク全体を、専用のツールやソフトウェアを使用して配布前のコンピュータにディスクコピーします。そのあと、利用者にコンピュータを配布します。

注意事項

ディスクコピーを開始する前に、必ずモデルとなるコンピュータ（ディスクコピー元のコンピュータ）で`resetnid.vbs` コマンドを実行してください。このコマンドを実行しない場合、ディスクコピー先のコンピュータが、ディスクコピー元のコンピュータと同一の機器として識別されてしまいます。

メリット

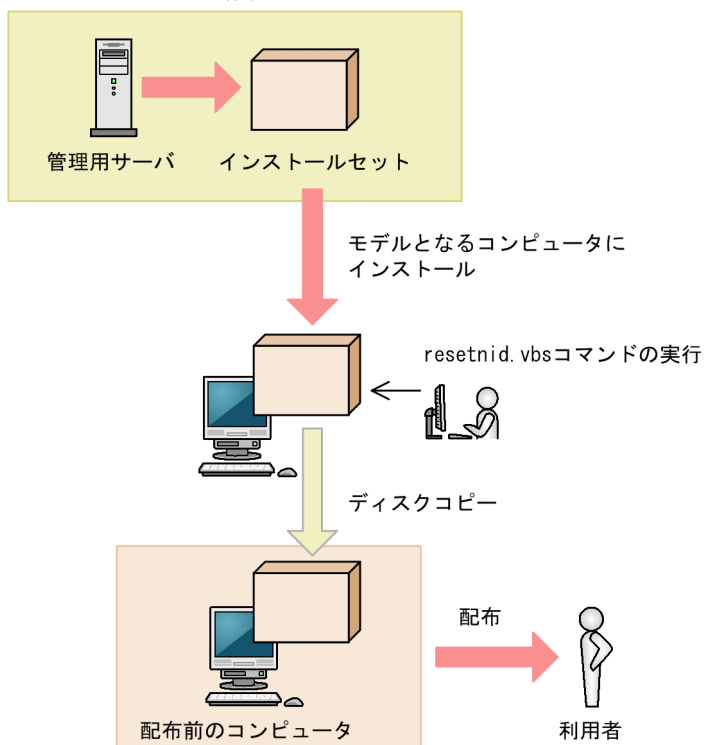
配布する時点でエージェントのインストールおよびセットアップがすでに完了しているため、利用者がエージェントをインストールする必要がありません。そのため、利用者の操作ミスによるトラブルを避けられます。

デメリット

配布前のコンピュータだけが対象です。すでに配布されているコンピュータには、この方法でエージェントをインストールできません。

ディスクコピーでエージェントをインストールするイメージを、次の図に示します。

インストールセットの作成



関連リンク

- [1.6.1 インストールセットを作成する手順](#)
- [1.7.1 エージェントのインストール状況を確認する流れ](#)
- [8.9 resetnid.vbs \(ホスト識別子のリセット\)](#)

1.6.9 エージェントを提供媒体からインストールする手順

エージェントのインストールを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

注意事項

ユーザーアカウント制御 (UAC) がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

注意事項

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

注意事項

エージェント環境を作成する場合、ユーザ環境変数およびシステム環境変数の TEMP および TMP で定義するディレクトリが存在することを確認してください。

エージェントをインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される [日立総合インストーラ] ダイアログで、[Hitachi IT Operations Director Agent] を選択して、[インストール実行] ボタンをクリックします。
3. インストール開始のダイアログで [次へ] ボタンをクリックします。
4. [インストールタイプ] ダイアログで、インストールタイプを選択して [次へ] ボタンをクリックします。
インストール先フォルダを指定したい場合はカスタムインストールを選択してください。簡単インストールの場合、インストール先フォルダにはデフォルト値が設定されます。
簡単インストールを選択した場合は、手順 9.へ進んでください。

ポイント

エージェントのインストール先フォルダのデフォルト値は、「C:¥Program Files¥HITACHI ¥Director Agent」です。ただし、OS が 64 ビット版の Windows の場合は、環境変数 %ProgramFiles(x86)% で定義されたフォルダ配下（OS が C ドライブにインストールされているときは、「C:¥Program Files (x86)¥Hitachi¥Director Agent¥」）になります。

注意事項

OS が 64 ビット版の Windows の場合、環境変数 %windir%¥system32 以下のフォルダにインストールしないでください。

注意事項

インストール先フォルダには、SYSTEM および Administrators グループのフルコントロール権限が必要です。また、適用先として「このフォルダ、サブフォルダおよびファイル」が設定されている必要があります。

5. [インストール先のフォルダ] ダイアログで、インストール先のフォルダを指定して [次へ] ボタンをクリックします。
6. インストールの開始準備の完了を示すダイアログで、[インストール] ボタンをクリックします。
インストールが実行されます。
7. インストールが完了したら、[完了] ボタンをクリックします。

エージェントのインストールが完了し、セットアップのダイアログが表示されます。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

ポイント

Hitachi IT Operations Director Agent をインストールすると、同時にリモコンエージェントもインストールされます。リモコンエージェントとは、リモートコントロール時に、接続される側のコンピュータに必要なプログラムです。

1.6.10 エージェントをセットアップする手順

提供媒体からエージェントをインストールした場合、管理用サーバと接続するためにセットアップを実行する必要があります。

なお、エージェントのセットアップを実行するには、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

エージェントをセットアップするには：

1. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations Director Agent] – [管理者ツール] – [セットアップ] を選択します。
エージェントにパスワード保護が設定されている場合、パスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。
2. [セットアップ] ダイアログの [接続先設定] タブで、接続先の管理用サーバのホスト名または IP アドレスと、ポート番号を指定して [OK] ボタンをクリックします。
3. 表示される確認ダイアログで [はい] ボタンをクリックします。

セットアップが完了し、設定した内容でエージェントが動作するようになります。

ポイント

エージェントが管理用サーバと接続できている場合、操作画面からエージェントのセットアップを実行できます。操作画面からエージェントをセットアップするには、エージェント設定を利用します。

1.7 エージェントを自動でインストールする

管理用サーバから各コンピュータに対して、エージェントを自動で配信できます。エージェントを配信するには、次の2つの方法があります。

探索と同時にエージェントを自動配信する

探索で発見した OS が Windows のコンピュータに対して、エージェントを自動的に配信できます。発見したコンピュータに順次エージェントが配信されるので、組織内のすべてのコンピュータにエージェントを自動配信したい場合は、この方法を選択してください。

エージェント未導入のコンピュータに個別配信する

管理対象のコンピュータ、および発見したコンピュータに対して、エージェントを個別に配信できます。エージェントを配信するコンピュータを選択できるので、組織内にエージェントをインストールしたくないコンピュータがある場合は、この方法を選択してください。

1.7.1 エージェントのインストール状況を確認する流れ

組織内のコンピュータにエージェントがインストールされているかどうかは、機器画面の [機器情報] 画面で確認します。

[機器情報] 画面には、管理対象の機器が表示されます。管理対象のコンピュータにエージェントがインストールされているかどうかは、一覧の項目の [管理種別] のアイコンで確認できます。

エージェントをインストールする前後で、[管理種別] 欄に表示されるアイコンを次に示します。

- ・  : コンピュータにエージェントがインストールされています。
- ・  : コンピュータにエージェントはインストールされていません。ただし、エージェントレスのコンピュータとして管理されています。
- ・  : コンピュータにエージェントはインストールされていません。

すべてのコンピュータにエージェントがインストールされたかどうかは、手持ちの機器の管理台帳と機器画面の [機器情報] 画面に表示されているコンピュータを比較して確認します。

ポイント

手持ちの管理台帳がない場合は、探索機能を利用して組織内の機器を発見してください。発見した機器を管理対象にすることで、管理台帳を作成できます。

1. エージェント導入済みのコンピュータだけを表示する

フィルタを利用して、[管理種別] が [エージェント管理] のコンピュータだけを表示します。

2. 機器情報をエクスポートする

【操作メニュー】 から【機器一覧をエクスポートする】または【機器一覧（詳細）をエクスポートする】を選択します。表示されるダイアログでエクスポートする項目を選択して、【OK】 ボタンをクリックしてください。エクスポートする項目には、手持ちの管理台帳と突き合わせて確認できる項目を選択します。

3. エージェントのインストール状況を確認する

手持ちの管理台帳とエクスポートしたコンピュータの一覧を比較します。このとき、エクスポートした一覧にないコンピュータが、エージェントをインストールしていないコンピュータになります。

エージェントが未導入のコンピュータがあった場合は、早急にインストールするよう指示してください。なお、エージェントを自動配信している場合は、配信に失敗しているおそれがあります。設定画面の【エージェントの配信】画面で配信状況を確認して再度配信するか、配信に失敗したコンピュータに対してエージェントを手動でインストールしてください。

1.7.2 探索と同時にエージェントを自動配信する手順（ネットワークの探索）

発見したコンピュータに対して自動的にエージェントを配信する方法の一つです。ネットワークの探索と同時にエージェントを配信します。

ポイント

エージェントを配信する際は、各コンピュータに約 35 メガバイトのデータ（インストールセット）が送信されます。

探索と同時にエージェントを自動配信するには（ネットワークの探索）：

1. 設定画面の【機器の探索】－【探索条件の設定】－【ネットワークの探索】画面を表示します。
2. 【発見した機器への操作】の【編集】ボタンをクリックします。
3. 表示されるダイアログで【エージェントを自動配信する】をチェックします。
4. 【OK】ボタンをクリックしてダイアログを閉じます。
5. 【探索を開始】ボタンをクリックします。
6. 表示されるダイアログで【OK】ボタンをクリックします。

探索が開始され、発見したコンピュータにエージェントが配信されます。エージェントの配信状況は、設定画面の【エージェント】－【エージェントの配信】画面に表示されます。

1.7.3 機器の探索状況の確認

Hitachi IT Operations Director では、組織内の機器を探索したあと、設定画面の「機器の探索」画面で、探索履歴や発見した機器の状況などを確認できます。探索状況を確認して、組織内の機器の現状を把握します。

機器の探索履歴には、次の 2 つがあります。探索で利用した方法に応じた探索履歴を確認してください。

- Active Directory の探索履歴
- ネットワークの探索履歴

また、機器の管理状態には、次の 3 つがあります。必要に応じて、発見した機器を管理対象にしたり、除外対象にしたりしてください。

発見

探索によって発見された機器は、この管理状態になり、設定画面の「機器の探索」－「発見した機器」画面に表示されます。発見した機器は管理対象にしたり、除外対象にしたりできます。

管理対象

Hitachi IT Operations Director で管理したい機器は、この管理状態にします。管理対象の機器は、設定画面の「機器の探索」－「管理対象機器」画面に表示されます。管理対象の機器は除外対象にできません。なお、機器を管理対象にすると、製品ライセンスを消費します。

除外対象

Hitachi IT Operations Director で管理する必要がない機器は、この管理状態に設定します。除外対象の機器は、設定画面の「機器の探索」－「除外対象機器」画面に表示されます。除外対象の機器は管理対象にしたり、削除したりできます。除外対象に設定すると、もう一度機器の探索を行っても、「発見した機器」画面には表示されません。

関連リンク

- [1.7.4 最新の探索状況を確認する手順](#)
- [1.7.5 発見した機器を確認する手順](#)
- [1.7.6 管理対象の機器を確認する手順](#)
- [1.7.7 除外対象の機器を確認する手順](#)

1.7.4 最新の探索状況を確認する手順

最新の探索の実行状況および実行結果を一覧で確認できます。

最新の探索状況を確認するには：

1. 設定画面を表示します。

2. メニューエリアで [機器の探索] – [探索履歴の確認] を選択します。

3. インフォメーションエリアで [Active Directory の探索] または [ネットワークの探索] を選択します。

[Active Directory の探索] 画面または [ネットワークの探索] 画面が表示されます。探索の進捗に伴って、探索履歴が更新されます。

ポイント

[Active Directory の探索] 画面または [ネットワークの探索] 画面では、探索を中止したり、実行したりすることもできます。探索エラーが多い場合は、探索を中止して探索条件の設定を見直すことをお勧めします。設定を見直したら、もう一度探索を実行してください。

1.7.5 発見した機器を確認する手順

Active Directory またはネットワークの探索で発見した機器を一覧で確認できます。また、発見した機器は管理対象や除外対象に変更したり、削除したりできます。

発見した機器を確認するには：

1. 設定画面を表示します。

2. メニューエリアで [機器の探索] – [発見した機器] を選択します。

[発見した機器] 画面が表示されます。発見した機器の台数や管理できる機器の台数、および管理対象とした機器の台数を確認できます。

インフォメーションエリアで機器を選択して [管理対象にする] ボタンをクリックすると、機器を管理対象にできます。[除外対象にする] ボタンをクリックすると、機器を除外対象にできます。また、[操作メニュー] の [削除する] を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で管理対象や除外対象に変更したり、削除したりすることもできます。

なお、除外対象に設定した機器は、この画面に表示されません。再び機器を管理したい場合は、[除外対象機器] 画面で機器の状態を管理対象に変更してください。また、削除した機器を管理したい場合は、再度探索を実行してください。

関連リンク

- [1.7.6 管理対象の機器を確認する手順](#)
- [1.7.7 除外対象の機器を確認する手順](#)

1.7.6 管理対象の機器を確認する手順

Hitachi IT Operations Director で管理している機器を一覧で確認できます。また、管理対象の機器は除外対象に変更したり、削除したりできます。

管理対象の機器を確認するには：

1. 設定画面を表示します。
2. メニューエリアで [機器の探索] – [管理対象機器] を選択します。

[管理対象機器] 画面が表示されます。管理対象の機器の台数および管理対象に変更できる機器の台数を確認できます。

インフォメーションエリアで機器を選択して [除外対象にする] ボタンをクリックすると、機器を除外対象にできます。また、[操作メニュー] の [削除する] を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で除外対象に変更したり、削除したりすることもできます。

なお、除外対象に設定した機器は、この画面に表示されません。再び機器を管理したい場合は、[除外対象機器] 画面で機器の状態を管理対象に変更してください。

ポイント

機器を削除すると、もう一度探索したとき、設定画面の [機器の探索] – [発見した機器] 画面に表示されるようになります。

関連リンク

- [1.7.7 除外対象の機器を確認する手順](#)

1.7.7 除外対象の機器を確認する手順

Hitachi IT Operations Director で管理しないと設定した機器を一覧で確認できます。また、除外対象の機器は管理対象に変更できます。

除外対象の機器を確認するには：

1. 設定画面を表示します。
2. メニューエリアで [機器の探索] – [除外対象機器] を選択します。

[除外対象機器] 画面が表示されます。除外対象の機器の台数および管理対象にできる機器の台数を確認できます。

インフォメーションエリアで機器を選択して「管理対象にする」ボタンをクリックすると、機器を管理対象にできます。また、「操作メニュー」の「削除する」を選択すると、一覧から機器を削除できます。複数の機器を選択して一括で管理対象にしたり、削除したりすることもできます。

ポイント

機器を削除すると、もう一度探索したとき、設定画面の「機器の探索」－「発見した機器」画面に表示されるようになります。

関連リンク

- 1.7.6 管理対象の機器を確認する手順

1.7.8 エージェント未導入のコンピュータに個別配信する手順

管理対象のコンピュータに対して、エージェントを個別に配信できます。

ポイント

エージェントを配信する際は、各コンピュータに約 35 メガバイトのデータが送信されます。

エージェントを個別配信するには：

1. 設定画面の「エージェント」－「エージェントの配信」画面を表示します。
2. エージェントを配信したいコンピュータを選択します。
3. 「配信を実行」ボタンをクリックします。
4. 表示されるダイアログで適用するエージェント設定を選択します。
5. 「OK」ボタンをクリックします。

選択したコンピュータにエージェントが配信されます。エージェントの配信状況は、設定画面の「エージェント」－「エージェントの配信」画面に表示されます。

ポイント

エージェントのインストールフォルダは、デフォルトエージェント設定で指定しているフォルダです。インストールフォルダを変更している場合は、ドライブおよび書き込みできるフォルダが指定されている必要があります。なお、指定したエージェント設定はインストール完了後に適用されます。

2

各システム構成の構築

ここでは、システム構成ごとの構築方法について説明します。

2.1 オフライン管理構成システムの構築

2.1.1 オフライン管理構成システムを構築する流れ

オフライン管理構成システムを構築するには、まず最小構成システムを構築します。そのあとで、コンピュータにオフライン管理用のエージェントをインストールします。

1. 最小構成システムを構築します。
2. オフライン管理用のエージェントを作成します。
3. オフライン管理したいコンピュータに、オフライン管理用のエージェントを導入します。

オフライン管理構成システムの構築が完了します。

関連リンク

- [1. 最小構成システム（管理用サーバとエージェント）の構築](#)

2.2 エージェントレス構成システムの構築

2.2.1 エージェントレス構成システムを構築する流れ

エージェントレス構成システムを構築するには、まず管理用サーバを構築します。そのあとで、探索を実行して、発見した機器を管理対象にします。

1. 管理用サーバを構築します。
2. 操作画面から、ネットワークの探索を実行して機器を発見します。
すべての機器を管理対象にする場合は、探索の設定で、発見した機器を自動的に管理対象にすることもできます。この場合、手順 4.に進んでください。
3. 発見された機器を管理対象にします。
4. 機器の情報を定期的に更新するための設定をします。

エージェントレス構成システムの構築が完了します。

ポイント

エージェント導入済みのコンピュータと、エージェントレスのコンピュータが混在するシステムを構築する場合、最小構成システムを構築したあとで、上記の手順 2.から始めてください。

関連リンク

- [4.1.1 探索条件を設定する手順（ネットワークの探索）](#)
- [1.7.5 発見した機器を確認する手順](#)
- [4.2.1 エージェントレスの機器の情報を定期的に更新する手順](#)

2.3 サポートサービス連携構成システムの構築

2.3.1 サポートサービス連携構成システムを構築する流れ

サポートサービス連携構成システムを構築するには、まず最小構成システムを構築し、そのあとでサポートサービスサイトに接続するための情報を設定します。

1. 最小構成システムを構築します。
2. 操作画面で、サポートサービスサイトに接続するための情報を設定します。

ポイント

管理対象のコンピュータの更新プログラムの状況を判定したり、判定結果に応じて自動対策したりするには、セキュリティポリシーの設定が必要です。セキュリティポリシーで更新プログラムを管理する方法については、マニュアル「Hitachi IT Operations Director 運用ガイド」を参照してください。

サポートサービス連携構成システムの構築が完了します。

関連リンク

- [4.3.1 サポートサービスと接続するための情報を設定する手順](#)

2.4 Active Directory 連携構成システムの構築

2.4.1 Active Directory 連携構成システムを構築する流れ

Active Directory 連携構成システムを構築するには、Active Directory と接続して、Active Directory に登録されているコンピュータを管理対象にします。

1. Active Directory が導入されているシステム内に、管理用サーバを構築します。
2. Hitachi IT Operations Director が Active Directory と接続するための情報を設定します。
3. 必要に応じて、Active Directory で管理されている情報を追加管理項目として取得するように設定します。
4. Active Directory に登録されているコンピュータを探索します。
すべての機器を管理対象にする場合は、探索の設定で、発見した機器を自動的に管理対象にすることもできます。同様に、探索と同時にエージェントを自動配信することもできます。手順 5.および手順 6.は必要に応じて実施してください。
5. 発見されたコンピュータを管理対象にします。
6. 管理対象のコンピュータに、エージェントを導入します。

Active Directory 連携構成システムの構築が完了します。

関連リンク

- [1.2 管理用サーバの環境構築](#)
- [4.4.1 Active Directory と接続するための情報を設定する手順](#)
- [4.4.2 追加管理項目として Active Directory から取得する情報を設定する手順](#)
- [4.4.3 Active Directory に登録されている機器を探索する手順](#)

2.5 MDM 連携構成システムの構築

2.5.1 MDM 連携構成システムを構築する流れ

MDM 連携構成システムを構築するには、まず最小構成システムを構築し、そのあとで MDM システムからスマートデバイスの情報を取得します。

1. 最小構成システムを構築します。
2. Hitachi IT Operations Director が MDM システムと連携するための情報を設定します。
3. MDM システム に登録されているスマートデバイスの情報を取得します。
すべてのスマートデバイスを管理対象にする場合は、MDM 連携の設定で、発見したスマートデバイスを自動的に管理対象にすることもできます。手順 4. は必要に応じて実施してください。
4. 発見されたスマートデバイスを管理対象にします。

MDM 連携構成システムの構築が完了します。

関連リンク

- [4.5.1 MDM システムと連携するための情報を設定する手順](#)

2.6 ネットワーク監視構成システムの構築

2.6.1 ネットワーク監視構成システムを構築する流れ

ネットワーク監視構成システムを構築するには、まず最小構成システムを構築し、そのあとでネットワークセグメントごとにネットワークモニタを有効にします。

1. 最小構成システムを構築します。
2. 操作画面からネットワークの探索を実行し、組織内のすべての機器を発見します。
3. ネットワーク制御リストで、ネットワーク接続を許可するかどうかの設定が正しいかを確認します。

ポイント

ネットワーク接続を許可しない機器があった場合は、その機器のネットワーク接続を許可しない設定にしてください。

4. 操作画面から、各ネットワークセグメントのネットワークモニタ機能を有効にします。

表示されるダイアログで、ネットワークへの接続を許可するネットワークモニタ設定を選択してください。

ネットワーク監視構成システムの構築が完了します。

なお、この手順で構築したシステムでは、新規にネットワーク接続した機器を検知することはできますが、自動的に遮断することはできません。新規にネットワーク接続した機器を自動的に遮断したい場合は、システム構築完了後に、次の設定をしてください。

新規にネットワーク接続した機器を自動的に遮断する

発見した機器のネットワークへの接続を許可しないように指定したネットワークモニタ設定を、その設定を反映したいネットワークセグメントに割り当ててください。

ポイント

セキュリティに問題がある機器のネットワーク接続を自動的に遮断することもできます。この場合は、セキュリティポリシーのアクション項目にあるネットワーク接続制御の設定で、セキュリティ状況の判定結果に応じたネットワーク接続の制御を設定してください。

関連リンク

- 4.1.1 探索条件を設定する手順（ネットワークの探索）
- 4.6.1 ネットワーク制御リストの機器を編集する手順
- 2.6.2 ネットワークモニタを有効にする手順

- 4.6.3 ネットワークモニタ設定を追加する手順
- 4.6.4 ネットワークモニタ設定の割り当てを変更する手順

2.6.2 ネットワークモニタを有効にする手順

オンライン管理のコンピュータのネットワークモニタを有効にすると、そのコンピュータが所属するネットワークセグメントに対して、ネットワークに接続された機器を自動的に発見したり、機器のネットワーク接続を制御したりできるようになります。

ネットワークモニタを有効にするには：

1. 機器画面を表示します。
2. メニューエリアの [機器情報] で、[機器一覧 (ネットワーク)] から該当するネットワークセグメントを選択します。
3. インフォメーションエリアでエージェント導入済みのコンピュータを選択します。
4. [操作メニュー] の [ネットワークモニタを有効にする] を選択します。

選択したコンピュータのネットワークモニタが有効になり、ネットワークセグメントのネットワークが監視されます。

ネットワークモニタが有効になっているコンピュータには、管理種別に  が表示されます。また、メニューエリアのグループに  が表示されます。

注意事項

メニューエリアに表示されるネットワークモニタの動作状態が「ネットワークモニタが有効です」または「ネットワークモニタを有効化しています」の場合、次の操作が制限されます。

- 該当するネットワークのグループを削除できません。
- ネットワークモニタが有効になっているコンピュータは除外対象にできません。また、削除もできません。

注意事項

ネットワークモニタを有効化するコンピュータの OS が Windows Server 2003 の場合、あらかじめ WinPcap がインストールされていないことを確認してください。WinPcap がインストール済みのときは、WinPcap をアンインストールしてからネットワークモニタを有効化してください。

注意事項

ネットワークモニタを有効にする場合、あらかじめ管理用サーバにコンポーネント（ネットワークモニタエージェント）が登録されている必要があります。

ポイント

設定画面の［ネットワーク制御］－［ネットワークモニタ設定の割り当て］画面でもネットワークモニタを有効にできます。

ポイント

ネットワークモニタを有効にしたコンピュータが複数のネットワークセグメントに所属している場合、所属しているすべてのネットワークセグメントでネットワークモニタが有効になります。

2.7 クラスタシステムの構築

2.7.1 クラスタシステムを構築する流れ

クラスタシステムを構築する場合、管理用サーバの構築から開始します。

クラスタシステムを構築するには：

1. 現用系サーバと待機系サーバに Hitachi IT Operations Director をインストールします。
インストールタイプは、カスタムインストールを選択してください。また、インストール完了後は、続けてセットアップを実行しないでください。
2. 現用系サーバでグループリソースを作成します。
3. 現用系サーバをセットアップします。
4. 現用系サーバのセットアップ完了時に出力されるファイルを待機系サーバにコピーします。
5. 待機系サーバでセットアップを実行するために、手順 2. で作成したグループリソースの所有者を待機系サーバに移動します。
6. 待機系サーバをセットアップします。
7. クラスタシステムの運用を開始するために、手順 2. で作成したグループリソースの所有者を現用系サーバに移動します。
8. Hitachi IT Operations Director の一部のサービスリソースをオンラインにします。
Windows Server Failover Cluster で管理用サーバのグループに登録したサービスリソース（汎用サービス）のリソースのうち、「IT Operations Director Service」と「IT Operations Director Agent Control」以外をオンライン状態にします。
9. 操作画面からライセンス認証をします。
10. Hitachi IT Operations Director のサービスリソースをオンラインにします。
「IT Operations Director Service」と「IT Operations Director Agent Control」をオンライン状態にします。

クラスタシステムの構築が完了します。

関連リンク

- [1.2.2 Hitachi IT Operations Director をインストールする手順](#)
- [2.7.2 現用系サーバでグループリソースを作成する手順](#)
- [2.7.3 現用系サーバで Hitachi IT Operations Director をセットアップする](#)

- 2.7.4 待機系サーバで Hitachi IT Operations Director をセットアップする

2.7.2 現用系サーバでグループリソースを作成する手順

Hitachi IT Operations Director のインストール後は、Windows Server Failover Cluster で Hitachi IT Operations Director のグループを作成し、リソースを登録します。リソースを登録する手順を次に示します。

1. 管理用サーバのグループを作成します。

Windows Server Failover Cluster にあらかじめ登録されている「Cluster Group」とは別に管理用サーバのグループを作成してください。

2. 作成したグループに必要なリソースを登録します。

グループに登録が必要なリソースを次の表に示します。

リソースの種類	リソース名
Hitachi IT Operations Director のサービスリソース以外のリソース	IP アドレスリソース
	ネットワーク名リソース
	共有ディスク（物理ディスク）リソース
Hitachi IT Operations Director のサービスリソース（汎用サービス）	IT Operations Director DB Service
	IT Operations Director DB Cluster Service
	IT Operations Director Web Container※
	IT Operations Director Web Server
	IT Operations Director Service
	IT Operations Director Agent Control

注※ Windows Server 2012 および Windows Server 2008 の場合はコマンドを実行して、リソースを作成します。

Windows Server 2012 の場合は、Administrator 権限を持つユーザーで、コマンドプロンプトから PowerShell を起動し、次に示すコマンドを実行してください。

```
Get-ClusterResource△"IT Operations Director Web Server サービスリソースの名前"△|△Set-ClusterParameter△-Name△StartupParameters△-value△""
```

Windows Server 2008 の場合は、Administrator 権限を持つユーザーで、コマンドプロンプトから、次に示すコマンドを実行してください。

```
cluster△res△"IT Operations Director Web Server サービスリソースの名前"△/priv△StartupParameters=""
```

（凡例）△：半角スペース

3. 現用系サーバを優先サーバに設定します。

4. Hitachi IT Operations Director のサービスリソース以外のリソースをオンライン状態にします。

Hitachi IT Operations Director のサービスリソース（汎用サービス）はオフライン状態のままです。

グループリソースが作成されます。

グループリソースの作成方法の詳細については、または Windows Server Failover Cluster のマニュアルを参照してください。

以降で、各リソースの設定項目および設定内容を説明します。

Hitachi IT Operations Director のサービスリソース以外のリソースの設定内容

リソース名	設定項目	設定内容
• IP アドレスリソース • ネットワーク名リソース • 共有ディスク（物理ディスク）リソース	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director DB Service の設定内容

リソース名	設定項目	設定内容
IT Operations Director DB Service	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。
	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「ネットワーク名リソース」および「共有ディスク（物理ディスク）リソース」を設定する。
	サービス名	「HiRDBEmbeddedEdition_JE1」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	0（固定）
	フェールオーバーの期間（秒）	0（固定）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director DB Cluster Service の設定内容

リソース名	設定項目	設定内容
IT Operations Director DB Cluster Service	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。

リソース名	設定項目	設定内容
IT Operations Director DB Cluster Service	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「IT Operations Director DB Service」のリソースを設定する。
	サービス名	「HiRDBClusterService_JE1」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director Web Container の設定内容

リソース名	設定項目	設定内容
IT Operations Director Web Container	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。
	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「IT Operations Director DB Cluster Service」のリソースを設定する。
	サービス名	「JP1_DTNAVI_WEBCON」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director Web Server の設定内容

リソース名	設定項目	設定内容
IT Operations Director Web Server	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。

リソース名	設定項目	設定内容
IT Operations Director Web Server	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「ネットワーク名リソース」のリソースを設定する。
	サービス名	「JP1_DTNAVI_WEBSVR」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director Service の設定内容

リソース名	設定項目	設定内容
IT Operations Director Service	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。
	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「IT Operations Director DB Cluster Service」のリソースを設定する。
	サービス名	「JP1_DTNAVI_MGRSRV」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

IT Operations Director Agent Control の設定内容

リソース名	設定項目	設定内容
IT Operations Director Agent Control	名前	任意の名称を指定する。
	リソースの種類	「汎用サービス」を設定する。

リソース名	設定項目	設定内容
IT Operations Director Agent Control	グループ	管理用サーバのグループ名を設定する。
	実行可能所有者	現用系および待機系の 2 台のサーバを設定する。
	依存関係	「IT Operations Director DB Cluster Service」のリソースを設定する。
	サービス名	「JP1_DTNAVI_AGCTRL」を設定する。
	レジストリの複製	指定しない。
	フェールオーバーのしきい値	1（推奨値）
	フェールオーバーの期間（秒）	900（推奨値）
	待ちのタイムアウト（秒）	300（推奨値）

2.7.3 現用系サーバで Hitachi IT Operations Director をセットアップする

ここでは、セットアップ画面のうち、クラスタシステムを運用するための設定が必要なものについて説明します。

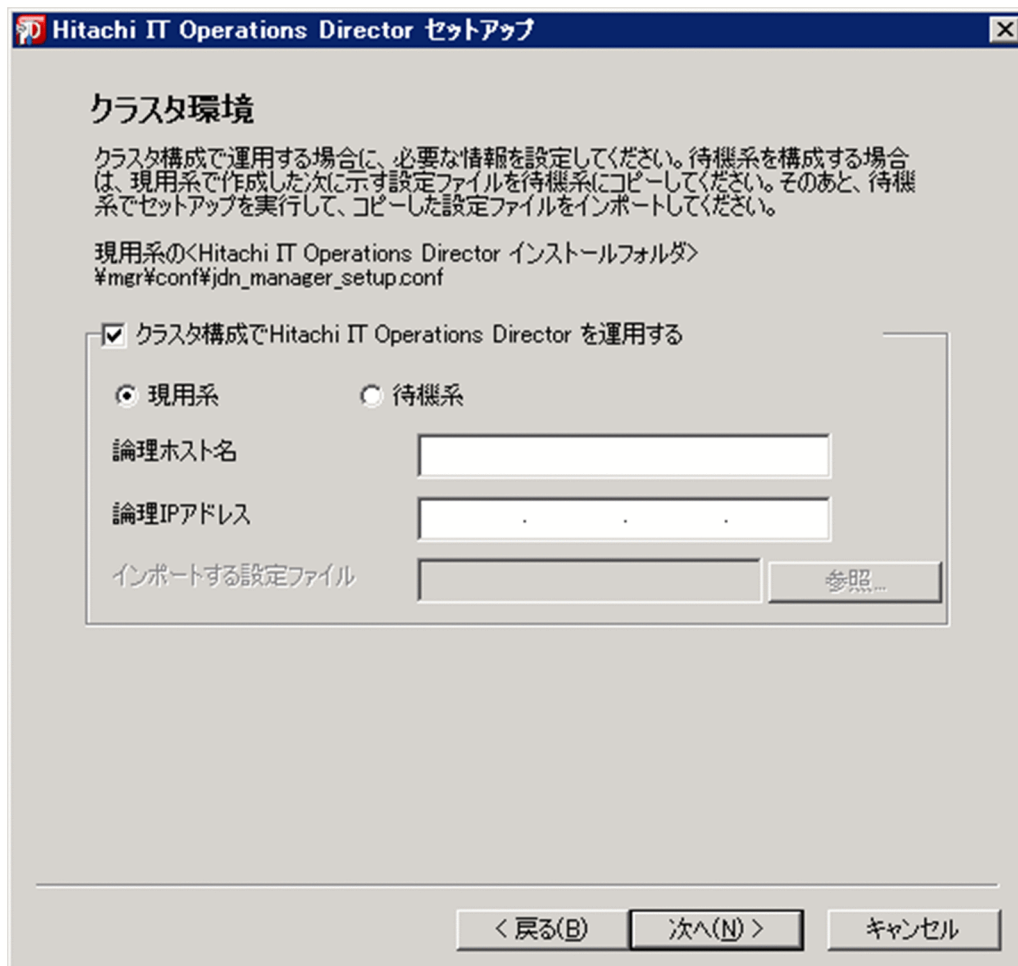
■ 注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

【クラスタ環境】画面の設定内容

セットアップの【クラスタ環境】画面で、クラスタシステムを運用するための設定をします。【クラスタ環境】画面を次の図に示します。



次のように設定してください。

- ・ [クラスタ構成で Hitachi IT Operations Director を運用する] をチェックする。
- ・ [現用系] を選択する。
- ・ [論理ホスト名] および [論理 IP アドレス] を設定する。

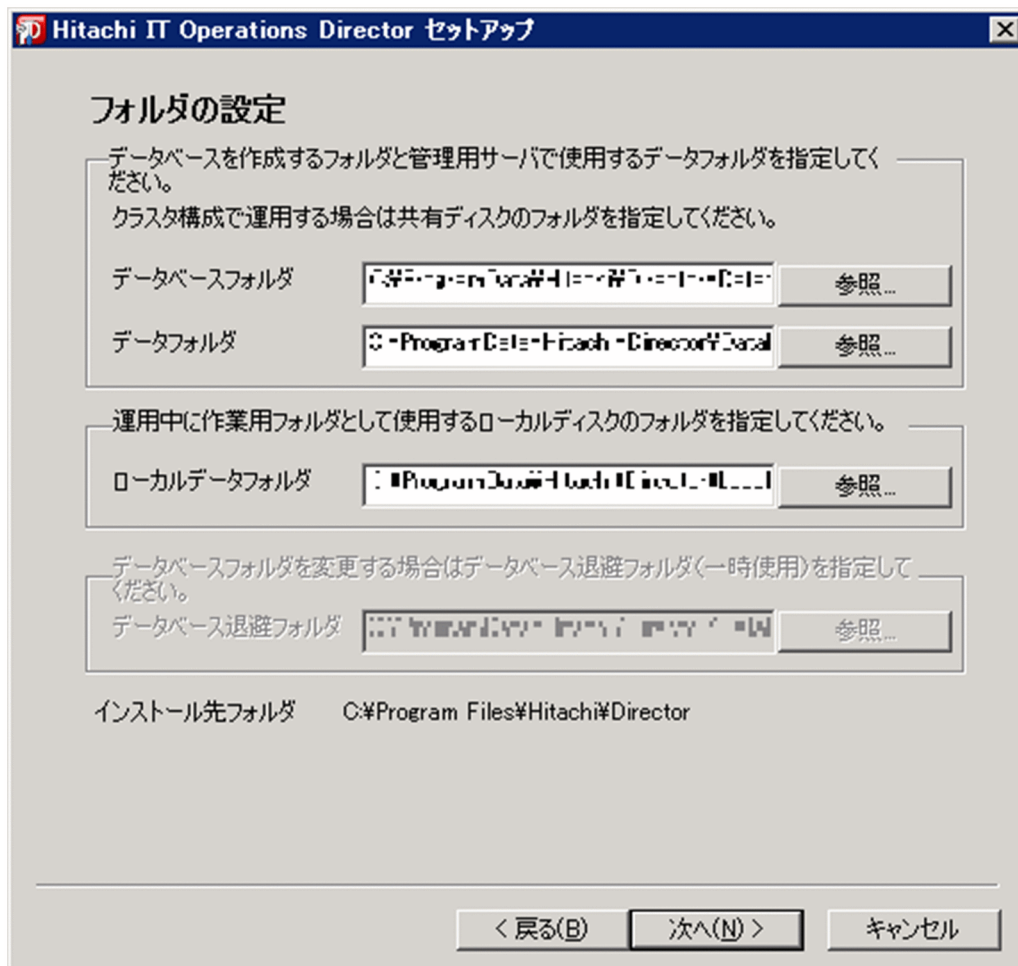
このとき、[インポートする設定ファイル] は設定不要です。

セットアップが完了すると、次に示すファイルが出力されます。このファイルを待機系サーバにコピーしてください。

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥conf¥jdn_manager_setup.conf

【フォルダの設定】 画面の設定内容

セットアップの [フォルダの設定] 画面で、クラスタシステムを運用するための設定をします。[フォルダの設定] 画面を次の図に示します。



次に示す項目に共有ディスクのパスを設定してください。

- [データベースフォルダ]
- [データフォルダ]

また、以降の画面で、次に示す項目に共有ディスクのパスを設定してください。

- [操作ログの設定] 画面の [操作ログのデータベースフォルダ] (操作ログを取得する場合)、および [操作ログの保管先フォルダ] (操作ログの保管先フォルダにローカルディスク上のフォルダを指定する場合)
- [保存用の変更履歴の出力設定] 画面の [変更履歴の出力先フォルダ] (変更履歴の出力先フォルダにローカルディスク上のフォルダを指定する場合)

このほかの項目については、通常のセットアップと同じです。

関連リンク

- [1.2.3 管理用サーバをセットアップする手順](#)

2.7.4 待機系サーバで Hitachi IT Operations Director をセットアップする

現用系サーバでの設定と同様に、待機系サーバでのセットアップを実行します。

ここでは、セットアップ画面のうち、クラスタシステムを運用するための設定が必要なものについて説明します。

セットアップの [クラスタ環境] 画面では、次のように設定してください。

- [クラスタ構成で Hitachi IT Operations Director を運用する] をチェックする。
- [待機系] を選択する。
- [インポートする設定ファイル] に現用系サーバでの設定でコピーしたファイルを指定する。

[フォルダの設定] 画面の設定内容は、通常のセットアップと同じです。ただし、待機系サーバをセットアップする場合は、次に示す項目は非活性表示され設定できません。

- [データベースフォルダ]
- [データフォルダ]
- [データベース退避フォルダ]

また、待機系サーバでエージェントを登録する必要はありません。

関連リンク

- [1.2.3 管理用サーバをセットアップする手順](#)

3

セットアップ内容の変更

ここでは、管理用サーバでセットアップ時に設定した内容の変更について説明します。

3.1 使用するフォルダを変更する手順

管理用サーバで使用するフォルダを変更できます。データベースに使用するディスク容量が不足した場合は、十分な空き容量があるディスクにデータベースのフォルダを変更してください。

注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- ・ システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- ・ 仮想プロビジョニングによって作成した記憶域のフォルダ

使用するフォルダを変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [フォルダの設定] 画面が表示されるまで、[次へ] ボタンをクリックします。
6. 必要に応じてフォルダを変更します。
7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。
8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

データベースフォルダについては、変更前のフォルダからデータベースが削除され、変更後のフォルダにデータベースが作成されます。データベース内のデータは、変更前の状態で引き継がれます。

データフォルダのデータは、変更後のフォルダに移動されます。

操作ログの保管先フォルダは、変更前のフォルダとそのフォルダに格納されているデータがそのまま残ります。変更後のフォルダには、フォルダの変更後に取得される操作ログのデータが格納されます。1つのフォルダに操作ログのデータをまとめておきたいときは、変更前のフォルダに格納されているデータを、変更後のフォルダに移動してください。

操作ログのデータベースフォルダを変更すると、変更前のデータは削除されます。必要に応じて操作ログの手動取り込みを実施してください。

3.2 操作ログの取得を設定する手順

管理用サーバのセットアップ項目です。

利用者の操作をログとして記録できます。操作ログを取得すると、ファイルの持ち込みまたは持ち出しを追跡したり、不審操作を行ったコンピュータを特定したりできます。

なお、操作ログを取得できるのは、オンライン管理のコンピュータだけです。

ポイント

操作ログの取得の有無は、セットアップとセキュリティポリシーの両方で設定が必要です。操作ログを取得する場合、ここでの設定とあわせて、セキュリティポリシーで操作ログの取得を有効に設定してください。また、取得する操作ログの種類はセキュリティポリシーで設定できます。

注意事項

管理用サーバのセットアップで操作ログを取得しない設定にしている場合、セキュリティポリシーで操作ログの取得を有効にしても、コンピュータから取得した操作ログは保存されません。

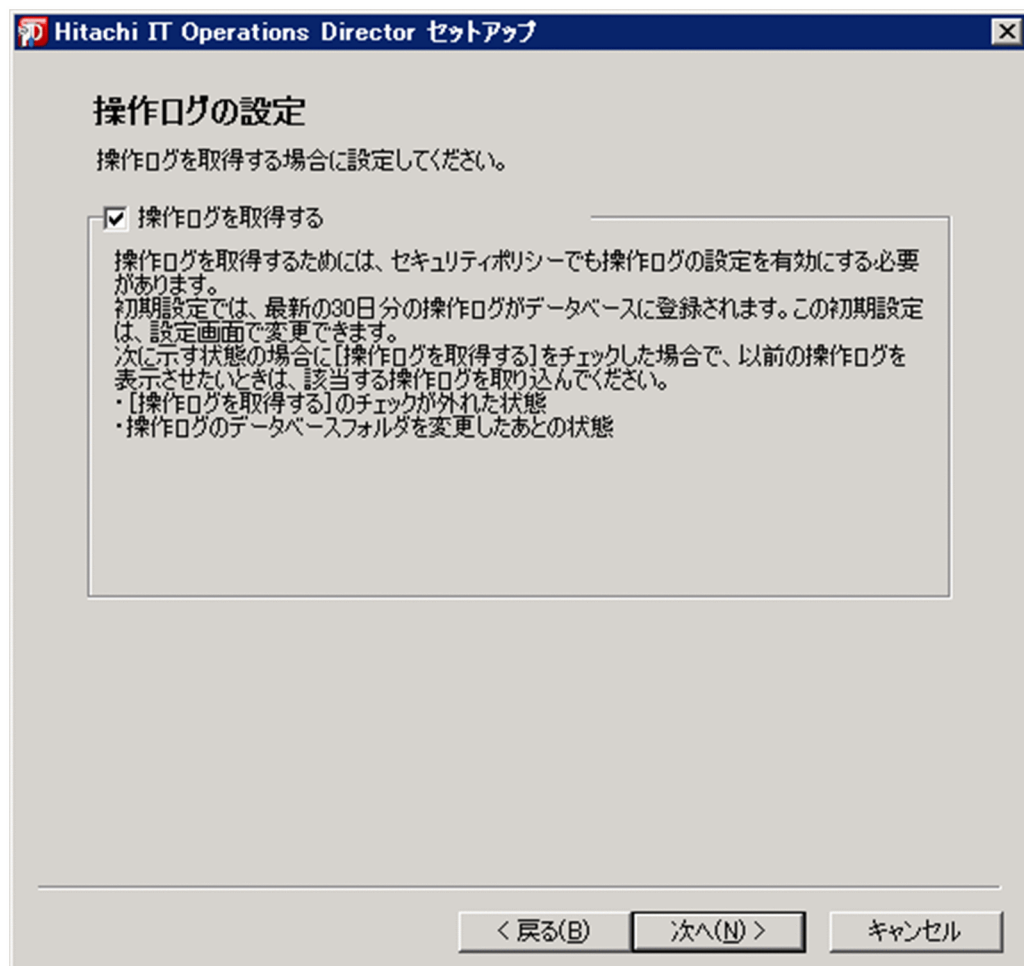
注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- ・ システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- ・ 仮想プロビジョニングによって作成した記憶域のフォルダ

操作ログの取得を設定するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [操作ログの設定] 画面が表示されるまで、[次へ] ボタンをクリックします。



6. [操作ログを取得する] をチェックして、[次へ] ボタンをクリックします。
7. 操作ログを保管する場合は、表示された画面で [操作ログを保管する] をチェックして、[操作ログの保管先フォルダ] を指定します。また、必要に応じて、保管先フォルダに接続するためのユーザー名とパスワードを指定します。

Hitachi IT Operations Director セットアップ

操作ログの設定

過去に取得した操作ログを取り込みたい場合に設定してください。

☒ 操作ログを保管する

操作ログの保管先フォルダを指定してください。
 ネットワーク上のフォルダを指定する場合は、UNC形式で指定してください。また、保管先フォルダに接続するためのユーザー名とパスワードを指定してください。
 クラスタ構成で運用する場合で、ローカルディスクのフォルダを指定するときは、共有ディスクのフォルダを指定してください。

操作ログの保管先フォルダ

ユーザー名

パスワード

※ 操作ログの保管先フォルダを変更しても、変更前のフォルダに保管されているファイルは移動されません。操作ログの保管先フォルダを変更する場合は、必要に応じて保管されているファイルも移動してください。

8. [次へ] ボタンをクリックします。

9. 表示された画面で、次の項目を設定します。

- [管理対象の機器の台数]
操作ログを取得するコンピュータの大よその台数を指定します。
- [操作ログのデータベース格納最大日数]
操作ログを操作ログのデータベースに何日分取り込むかを指定します。デフォルトは 60 日です。
なお、操作ログの自動取り込みを設定した場合、利用者の操作ログはデフォルトでは最新 30 日分が、[操作ログのデータベースフォルダ] で指定したフォルダに自動的に保存されます。自動取り込みされる操作ログの格納期間は、[操作ログの設定] で変更できます。
- [必要なディスク容量]
[管理対象の機器の台数] および [操作ログのデータベース格納最大日数] の指定に基づいて、自動で算出されます。
- [操作ログのデータベースフォルダ]
操作ログを保存するためのデータベースを作成するフォルダを指定します。[必要なディスク容量] に表示されている容量よりも、空き容量が大きいディスクのフォルダを指定してください。

ポイント

〔操作ログのデータベース格納最大日数〕 および 〔必要なディスク容量〕 は目安です。取り込める操作ログの期間や使用するディスク容量は、実際に管理している機器の台数や操作ログの情報量によって異なります。

10. [次へ] ボタンをクリックします。

11. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

12. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

13. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

操作ログを取得できるようになります。

注意事項

操作ログの取得に関する設定を変更する場合、すでに操作ログを取得しているときは、〔管理対象の機器の台数〕 および 〔操作ログのデータベース格納最大日数〕 を現在の設定値より小さくすることはできません。

3.3 保存用の変更履歴の出力を設定する手順

管理用サーバのセットアップ項目です。

保存用の変更履歴の出力を設定すると、CSV ファイルに保存用の変更履歴が定期的に出力されます。保存用の変更履歴を出力しておけば、変更履歴が 60,000 件を超える場合も変更の内容を保持できます。

保存用の変更履歴の出力を設定するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] - [Hitachi IT Operations] - [Director Tools] - [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [保存用の変更履歴の出力設定] 画面が表示されるまで、[次へ] ボタンをクリックします。

6. [保存用の変更履歴を定期的に出力する] をチェックして [変更履歴の出力先フォルダ] を指定します。

注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- ・ システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- ・ 仮想プロビジョニングによって作成した記憶域のフォルダ

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

保存用の変更履歴が定期的に出力されるようになります。保存用の変更履歴では、次の項目が CSV ファイルに出力されます。

変更履歴の項目	説明
変更された日時	機器情報に変更が発生した日時（機器情報の更新日時と同じ日時）が出力されます。 なお、外部記憶媒体を使用して機器情報を管理用サーバに通知した場合は、情報収集用ツールで機器情報を収集した日時を出力します。
変更された項目	変更された機器情報の項目が出力されます。
変更前	変更前の機器情報が出力されます。
変更後	変更後の機器情報が出力されます。
変更発生時のホスト名	機器情報が変更された時点の、機器のホスト名を出力します。変更された項目がホスト名の場合は、変更後のホスト名を出力します。変更が発生した機器を特定するための情報です。

3.4 ポート番号を変更する手順

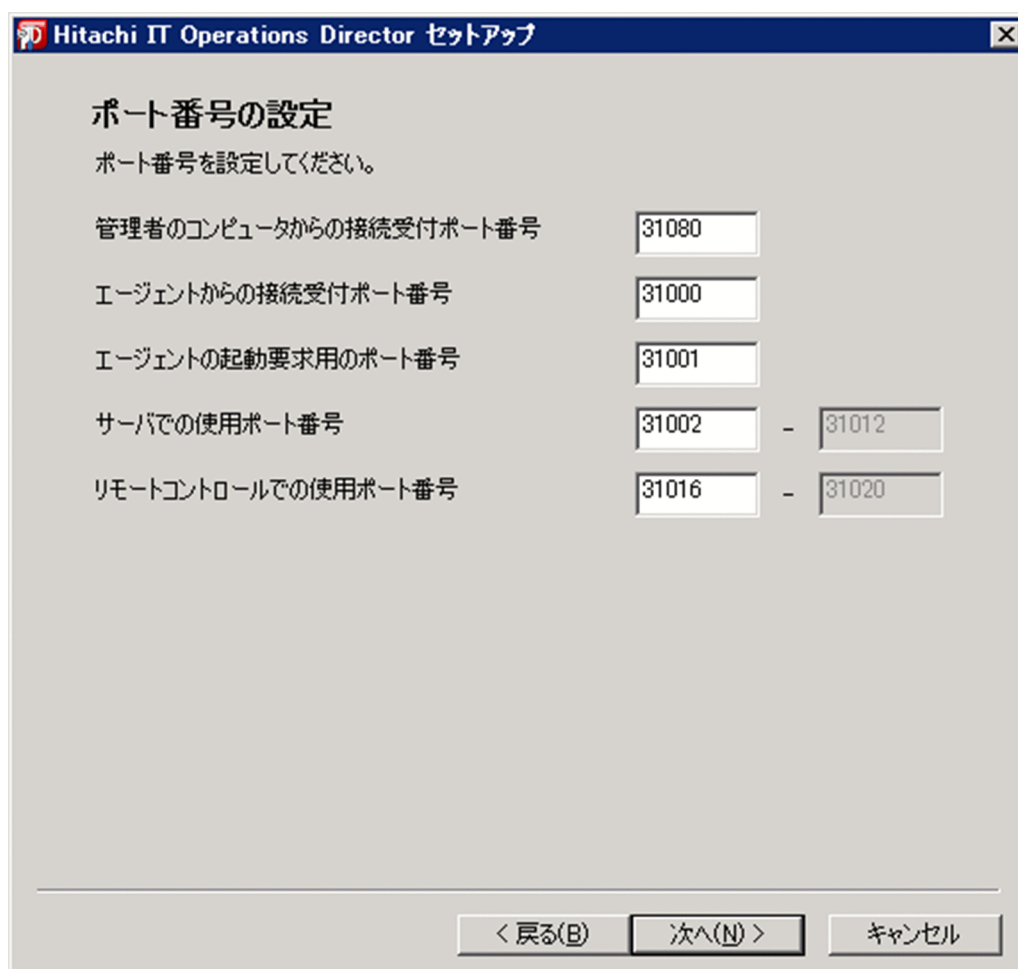
管理用サーバで使用するポート番号を変更できます。

注意事項

運用中にポート番号を変更すると、エージェントからの接続ができなくなります。ポート番号を変更する場合は、エージェントでもポート番号の設定を変更してください。

ポート番号を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] - [Hitachi IT Operations] - [Director Tools] - [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [ポート番号の設定] 画面が表示されるまで、[次へ] ボタンをクリックします。



Hitachi IT Operations Director セットアップ

ポート番号の設定
ポート番号を設定してください。

管理者のコンピュータからの接続受付ポート番号	31080
エージェントからの接続受付ポート番号	31000
エージェントの起動要求用のポート番号	31001
サーバでの使用ポート番号	31002 - 31012
リモートコントロールでの使用ポート番号	31016 - 31020

< 戻る(B) 次へ(N) > キャンセル

6. 必要に応じてポート番号を変更します。

変更できる内容を次に示します。

[管理者のコンピュータからの接続受付ポート番号]

Hitachi IT Operations Director を操作するコンピュータから管理用サーバの接続に使用するポート番号を入力します。

[エージェントからの接続受付ポート番号]

エージェントから管理用サーバの接続に使用するポート番号を入力します。

[エージェントの起動要求用のポート番号]

管理用サーバからエージェントへの通信に使用するポート番号を入力します。

[サーバでの使用ポート番号]

Hitachi IT Operations Director が使用するポート番号を入力します。

[リモートコントロールでの使用ポート番号]

リモートコントロール機能で使用するポート番号を入力します。

ポート番号の詳細については、「[付録 A.1 ポート番号一覧](#)」を参照してください。

7. [セットアップの確認] 画面が表示されるまで、[次へ] ボタンをクリックします。

8. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

9. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ポート番号が変更されます。

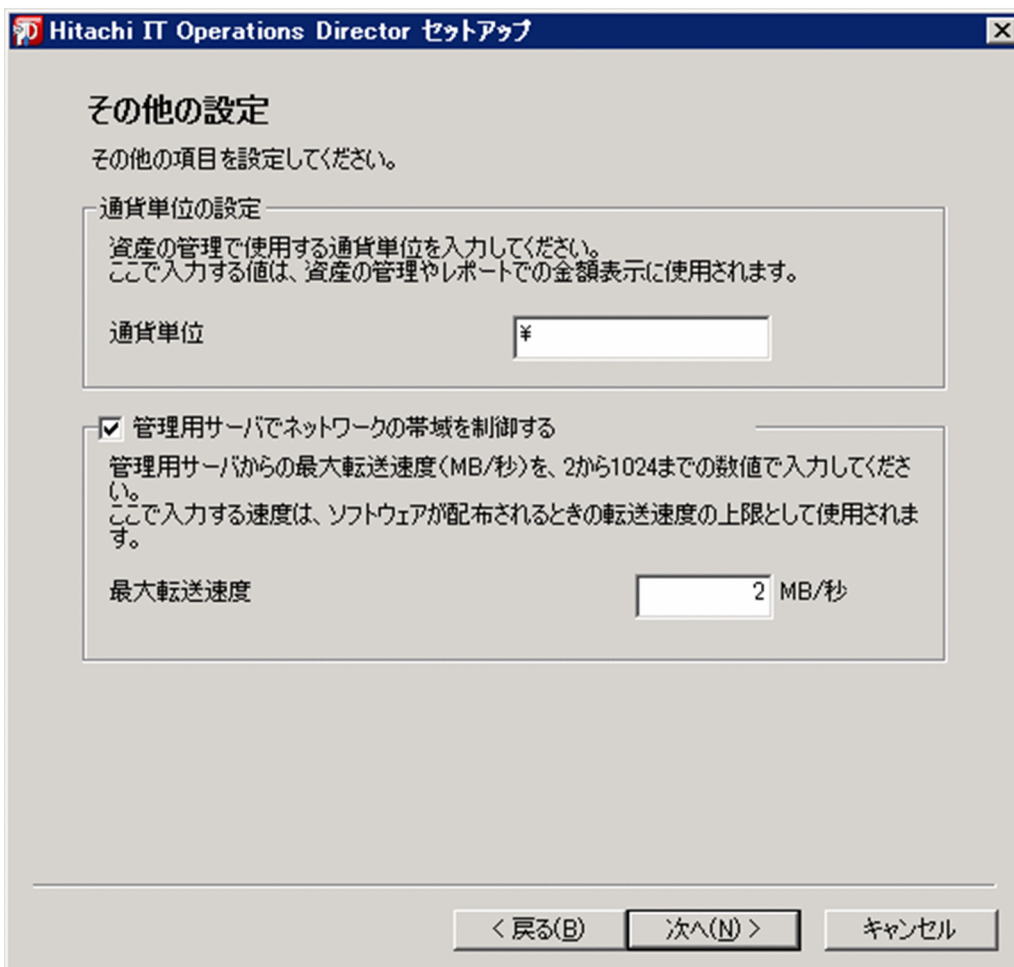
3.5 通貨単位を変更する手順

管理用サーバのセットアップ項目です。

資産管理で使用する通貨単位を変更できます。

通貨単位を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [その他の設定] 画面が表示されるまで、[次へ] ボタンをクリックします。



Hitachi IT Operations Director セットアップ

その他の設定
その他の項目を設定してください。

通貨単位の設定
資産の管理で使用する通貨単位を入力してください。
ここで入力する値は、資産の管理やレポートでの金額表示に使用されます。

通貨単位

☒ 管理用サーバでネットワークの帯域を制御する
管理用サーバからの最大転送速度(MB/秒)を、2から1024までの数値で入力してください。
ここで入力する速度は、ソフトウェアが配布されるときの転送速度の上限として使用されます。

最大転送速度 MB/秒

< 戻る(B) 次へ(N) > キャンセル

6. [通貨単位の設定] で [通貨単位] を入力し、[次へ] ボタンをクリックします。
7. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

8. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

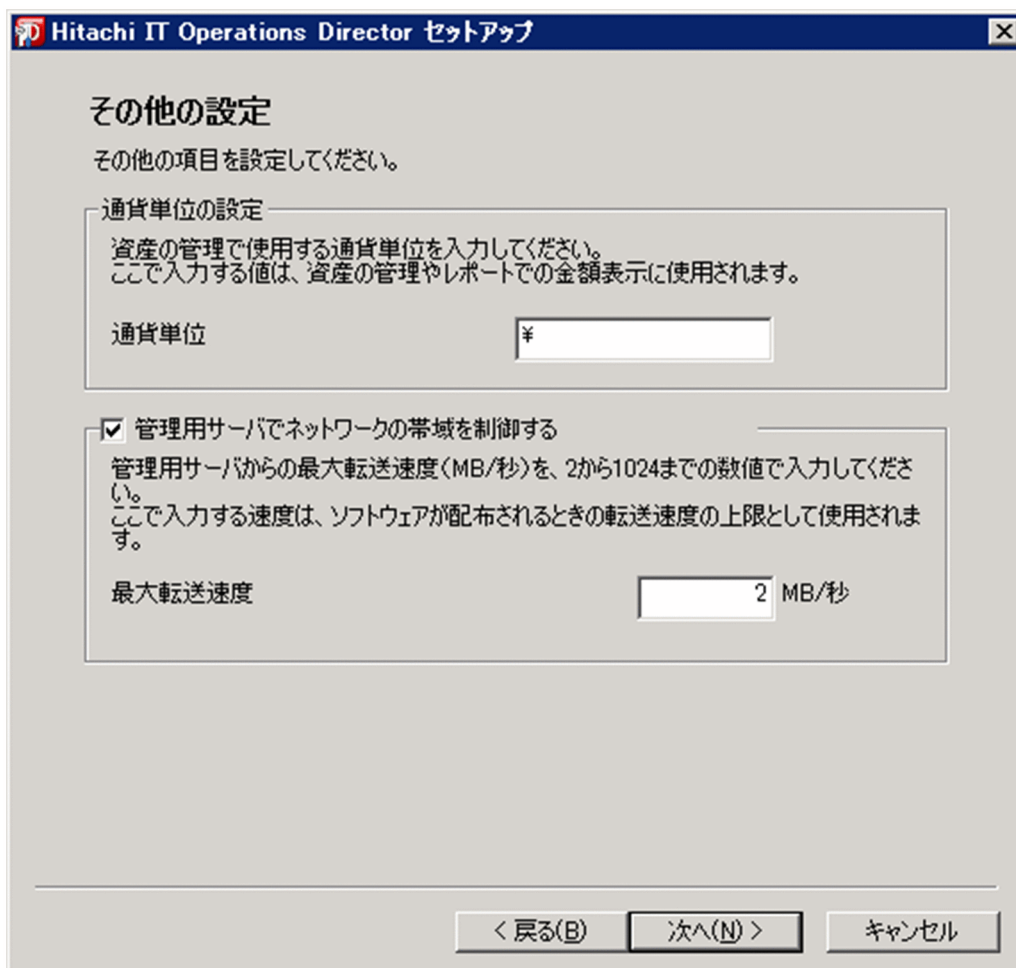
通貨単位が変更されます。

3.6 配布時に使用されるネットワーク帯域を制御する手順

管理用サーバから管理対象のコンピュータにソフトウェアやファイルを配布するときに、すべてのネットワーク帯域を使用しないように最大転送速度を設定して、ネットワーク帯域を制御できます。

ネットワーク帯域を制御するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [その他の設定] 画面が表示されるまで、[次へ] ボタンをクリックします。



Hitachi IT Operations Director セットアップ

その他の設定
その他の項目を設定してください。

通貨単位の設定
資産の管理で使用する通貨単位を入力してください。
ここで入力する値は、資産の管理やレポートでの金額表示に使用されます。

通貨単位

☒ 管理用サーバでネットワークの帯域を制御する
管理用サーバからの最大転送速度 (MB/秒) を、2 から 1024 までの数値で入力してください。
ここで入力する速度は、ソフトウェアが配布されときの転送速度の上限として使用されます。

最大転送速度 MB/秒

< 戻る(B) 次へ(N) > キャンセル

6. [管理用サーバでネットワークの帯域を制御する] をチェックして [最大転送速度] を入力し、[次へ] ボタンをクリックします。
7. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

8. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ネットワーク帯域が制御されるようになります。

3.7 ログイン制限情報を変更する手順

連続して何回ログインに失敗したらアカウントをロックするかやログインユーザーのパスワードの有効期限を変更できます。

アカウントをロックする連続入力失敗の回数やログインユーザーのパスワードの有効期限を変更するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[設定変更] を選択して [次へ] ボタンをクリックします。
5. [その他の設定] 画面が表示されるまで、[次へ] ボタンをクリックします。
[その他の設定] 画面の例を次に示します。

The screenshot shows a Windows-style dialog box titled "Hitachi IT Operations Director セットアップ". The main content area is titled "その他の設定" (Other Settings) with the instruction "その他の項目を設定してください。" (Please set other items). Below this is a section titled "ログイン情報の設定" (Login Information Settings) with the instruction "ログイン情報に関する上限値を変更する場合に設定してください。" (Please set values when changing limits related to login information). There are two settings: "アカウントをロックする連続入力失敗の回数 (0:ロックしない)" (Number of consecutive failed login attempts to lock account (0: no lock)) with a spinner box set to 0 and a range of (0~10); and "ユーザーパスワードの有効日数 (0:無期限)" (User password validity period (0: unlimited)) with a spinner box set to 180, followed by "日" (days) and a range of (0~999). At the bottom are three buttons: "< 戻る(B)" (Back), "次へ(N) >" (Next), and "キャンセル" (Cancel).

6. 必要に応じて次の項目を変更し、[次へ] ボタンをクリックします。

- アカウントをロックする連続入力失敗の回数

連続して何回ログインに失敗したら、アカウントをロックするかを指定します。

- ユーザーパスワードの有効日数

ログインユーザーのパスワードの有効期限として、パスワードが有効な日数を指定します。

7. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。

セットアップが開始され、処理中を示すダイアログが表示されます。セットアップが終了すると、[セットアップを終了します] 画面が表示されます。

サービスの停止が必要な場合は、サービスの停止を確認するダイアログが表示されます。[OK] ボタンをクリックしてサービスを停止してください。

8. [セットアップを終了します] 画面で、[OK] ボタンをクリックします。

ログイン制限情報が変更されます。

3.8 データベースをアップグレードする手順

管理用サーバのセットアップ項目です。

Hitachi IT Operations Director を上書きインストールした場合に、データベースのアップグレードが必要なときは、セットアップからデータベースをアップグレードしてください。

データベースをアップグレードするには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] - [Hitachi IT Operations] - [Director Tools] - [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で [データベースアップグレード] を選択して、[次へ] ボタンをクリックします。
5. [データベースアップグレードの設定] 画面でアップグレードの設定をして、[次へ] ボタンをクリックします。
6. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。
7. セットアップの完了を示すダイアログで、セットアップに続いてコンポーネントを登録するかどうかを設定して [OK] ボタンをクリックします。

コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムを管理用サーバに登録しておくことで、エージェントを配信したり、ネットワークモニタエージェントを操作画面からインストールしたりできるようになります。

コンポーネントを登録する場合は、[コンポーネントの登録] ダイアログが表示されるので、コンポーネントの登録とアップデートについて設定します。

ポイント

インストールの続きでセットアップを起動した場合は、セットアップの完了を示すダイアログ上でコンポーネントのアップデートについて設定できます。

コンポーネントのアップデートについては、「[5.5 コンポーネントのアップデート方法](#)」を参照してください。

データベースがアップグレードされます。

3.9 データベースを初期化する手順

Hitachi IT Operations Director が使用するデータベースを初期化できます。

データベースを初期化するには：

1. Administrator 権限を持つユーザーで OS にログオンします。
2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] を選択します。
3. セットアップ画面で [次へ] ボタンをクリックします。
4. [セットアップの選択] 画面で、[サーバの再構築] を選択します。
5. [次へ] ボタンをクリックして、各画面でデータベースの設定をします。
6. [セットアップの確認] 画面で設定内容を確認して、[次へ] ボタンをクリックします。
7. セットアップの完了を示すダイアログで、セットアップに続いてコンポーネントを登録するかどうかを設定して [OK] ボタンをクリックします。

コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムを管理用サーバに登録しておくことで、エージェントを配信したり、ネットワークモニタエージェントを操作画面からインストールしたりできるようになります。

コンポーネントを登録する場合は、[コンポーネントの登録] ダイアログが表示されるので、コンポーネントの登録とアップデートについて設定します。

コンポーネントのアップデートについては、「[5.5 コンポーネントのアップデート方法](#)」を参照してください。

データベースが初期化されます。

注意事項

データベースを初期化しても、フォルダに格納されているファイルは削除されません。作業用フォルダや操作ログのバックアップデータの保存フォルダのデータが不要な場合は、手動で削除してください。

4

構築時の設定のカスタマイズ

ここでは、構築時の設定で、カスタマイズできる項目について説明します。

4.1 最小構成システムの構築時の設定

4.1.1 探索条件を設定する手順（ネットワークの探索）

ネットワークの機器を探索する場合の探索条件を設定できます。

探索条件を設定するには：

1. 設定画面を表示します。
2. メニューエリアで **「機器の探索」** - **「探索条件の設定」** - **「ネットワークの探索」** を選択します。
3. **「探索範囲の設定内容」** で探索範囲を設定します。
探索範囲には、最初から「管理用サーバセグメント」という名称の探索範囲が設定されています。管理用サーバセグメントとは、管理用サーバが含まれるセグメントのことです。
4. **「認証情報」** で認証情報を設定します。
認証情報を利用して探索する場合に、認証情報を設定してください。認証情報を登録したら、**「探索範囲の設定内容」** で探索範囲ごとに認証情報を割り当ててください。
5. **「探索スケジュール」** を編集します。
スケジュールを決めて定期的に探索を実行する場合に、スケジュールを設定してください。
6. **「発見した機器への操作」** を編集します。
機器の探索時に新しい機器が発見された場合の操作を設定してください。
7. **「完了通知」** を編集します。
機器の探索が完了したら Hitachi IT Operations Director の管理者にメールで通知する場合に、通知先を設定してください。
利用するメールサーバ（SMTP サーバ）の情報を設定していない場合は、**「メールサーバの設定へ」** のリンクをクリックして表示される画面で、メールサーバの情報を設定してください。

探索条件の設定が完了します。

設定した探索条件で探索を即時実行する場合は、**「探索を開始」** ボタンをクリックしてください。即時実行しない場合は、**「探索スケジュール」** に従って実行されます。

探索の実行状況と実行結果は、設定画面の **「探索履歴の確認」** - **「ネットワークの探索」** 画面で確認できます。

関連リンク

- [1.7.3 機器の探索状況の確認](#)
- [4.1.2 ネットワークの探索時に使用する認証情報](#)

4.1.2 ネットワークの探索時に使用する認証情報

ネットワークの探索では、ARP と ICMP を利用して機器が発見されますが、それだけでは機器の詳細情報は収集されません。探索時に機器の詳細情報も収集するためには、発見された機器に対して SNMP または Windows の管理共有を利用して接続できるように認証情報を設定する必要があります。

SNMP の認証情報

コミュニティ名

Windows の管理共有の認証情報

- Administrator 権限のユーザー ID
- パスワード

SNMP を利用できる機器の場合、コミュニティの認証ができるときは、発見と同時に機器種別の判別、および一部の機器情報を収集できます。

Windows の管理共有が有効なコンピュータの場合、Administrator 権限でログオン認証できるときは、コンピュータを発見すると同時に機器種別の判別、および大部分の機器情報を収集できます。さらに、エージェントを配信してインストールすることもできます。

注意事項

OS が Windows Me、Windows 98、Windows 95、および Windows NT 4.0 のコンピュータは、発見されても機器種別が「不明な機器」として扱われることがあります。

注意事項

1 台の機器にネットワークカードが複数ある場合、ICMP が使用されて探索されたとき、複数台の機器として発見されます。

ポイント

Windows の管理共有の認証で使用するユーザー ID は、ドメインユーザーで認証する場合は、「ユーザー ID@FQDN (完全修飾ドメイン名)」または「ドメイン名¥ユーザー ID」の形式で指定してください。FQDN とは、ホスト名やドメイン名を省略しないで記述する形式です。例えば、「User001@PC001.hitachi.com」のように指定します。

ポイント

Windows の管理共有の認証を利用する場合、コンピュータ側で管理共有の設定を有効にしておく必要があります。

探索は、各探索範囲に対して認証情報を組み合わせて実行します。デフォルトでは、設定したすべての認証情報が使われますが、部署ごとに SNMP のコミュニティ名を分けている場合や、Windows の認証情報がコンピュータによって異なる場合などでは、探索範囲ごとに必要な認証情報だけを選択して実行することもできます。

なお、ネットワークの探索で使用する認証情報は、エージェントを配信するときにも利用されます。探索したあとでエージェントを配信する場合は、設定画面の [機器の探索] - [探索条件の設定] - [ネットワークの探索] 画面で、配信先のコンピュータが含まれる探索範囲に対して Windows の管理共有の認証情報を設定しておく必要があります。

4.1.3 エージェント設定を追加する手順

コンピュータによって監視間隔の設定を分けたい場合、エージェント設定を追加できます。

エージェント設定を追加するには：

1. 設定画面を表示します。
2. メニューエリアで [エージェント] - [エージェント設定とインストールセットの作成] を選択します。
3. インフォメーションエリアで [エージェント設定を追加] ボタンをクリックします。
4. 表示されるダイアログでエージェント設定の情報を入力して、[OK] ボタンをクリックします。

エージェント設定が追加され、エージェント設定の一覧に表示されます。

追加したエージェント設定は、[エージェント設定の割り当て] 画面でエージェント設定を割り当てることで、エージェント導入済みのコンピュータにも適用できます。

4.1.4 コンフィグレーションファイルで処理の設定を変更する手順

処理の開始時刻や Hitachi IT Operations Director Agent をアンインストールした時に、機器の廃棄として扱うか、Hitachi IT Operations Director Agent のアンインストールとして扱うかどうかの指定などは、コンフィグレーションファイルの設定を変更することで有効になります。

コンフィグレーションファイル (jdn_manager_config.conf) を設定するには：

1. コンフィグレーションファイルに設定を追加します。
コンフィグレーションファイル (jdn_manager_config.conf) の格納先は次のとおりです。
Hitachi IT Operations Director のインストール先フォルダ¥mgr¥conf

コンフィグレーションファイルで設定する定義を次の表に示します。

プロパティ	説明	設定値	デフォルト
State_AfterAgentUninstalling ※	Hitachi IT Operations Director Agent をアンインストールした時に、機器の廃棄として扱うか、Hitachi IT Operations Director Agent のアンインストールとして扱うかどうかの指定	0：アンインストールとして扱う 1：機器の廃棄として扱う	0

注※

エージェントからのアンインストール通知を受信できなかった場合は、これまでと同様に機器情報は変更されません。この場合は、必要に応じて機器情報を削除するなどして、対処してください。

コンフィグレーションファイルの設定例を次に示します。

```
#
# コンフィグレーションファイル
#
# Hitachi IT Operations Director Agentをアンインストールした時に、機器の廃棄として扱うか、
# Hitachi IT Operations Director Agentのアンインストールとして扱うかどうかの指定
State_AfterAgentUninstalling=0
```

4.1.5 エージェントの監視項目を変更する手順

エージェント導入済みのコンピュータを定期的に監視する項目を、インベントリ設定ファイル (jdng_inventory.conf) を使用することで変更できます。

エージェントの監視項目を変更するには：

1. 次の表に示す内容を入力したインベントリ設定ファイル (jdng_inventory.conf) をテキストエディタで作成し、%ALLUSERSPROFILE%\HITACHI\Director Agent\conf フォルダに格納します。

セクション	キー名	説明	設定値	デフォルト
SystemInventory	DHCPLeaseExpires	DHCP リース期限日時の変更を監視するかどうかを指定できます。 セクションやキー名が存在しない場合、または無効な値が設定されている場合は、デフォルト値0として動作します。	0：監視しない 1：監視する	0
	DHCPLeaseObtained	DHCP リース取得日時の変更を監視するかどうかを指定できます。 セクションやキー名が存在しない場合、または無効な値が設定されている場合は、デフォルト値0として動作します。	0：監視しない 1：監視する	0

エージェントの監視項目が変更されます。

DHCP リース期限日時と DHCP リース取得日時を監視対象項目とする場合の、インベントリ設定ファイルの設定例を次に示します。この場合の監視間隔は、エージェント設定の [エージェント基本動作] – [監視間隔 (セキュリティ項目以外) (分)] に指定した値になります。

```
[SystemInventory]
DHCPLeaseExpires=1
DHCPLeaseObtained=1
```

なお、インベントリ設定ファイルで設定した内容は、次に機器情報を取得するタイミングから自動的に適用されます。

4.2 エージェントレス構成システムの構築時の設定

4.2.1 エージェントレスの機器の情報を定期的に更新する手順

エージェントを導入していない（エージェントレスの）機器から定期的に情報を収集して更新するかどうか、また、更新する頻度を設定できます。

エージェントレスの機器の情報を定期的に更新するには：

1. 設定画面を表示します。
2. メニューエリアで [エージェント] - [エージェントレス管理の設定] を選択します。
3. インフォメーションエリアで、[定期的に更新する] にチェックします。
4. [更新間隔] に、何時間ごとに更新するかを設定します。
5. [適用] ボタンをクリックします。

設定した更新頻度で、エージェントレスの機器から情報が収集されて更新されます。

[定期的に更新する] のチェックを外すと、エージェントレスの機器から情報が収集されなくなります。

ポイント

Hitachi IT Operations Director では、より安全なセキュリティ管理をするため、管理対象のコンピュータにエージェントを導入することをお勧めしています。

4.3 サポートサービス連携構成システムの構築時の設定

4.3.1 サポートサービスと接続するための情報を設定する手順

Windows の更新プログラムが最新かどうかを判定する場合や、最新のウィルス対策製品をセキュリティポリシーの判定項目にする場合、最新の更新プログラムやウィルス対策製品の情報をサポートサービスサイトから定期的にダウンロードする必要があります。このために、サポートサービスサイトと接続するための情報を設定しておく必要があります。

サポートサービスサイトに接続すると、更新プログラムの情報とウィルス対策製品の情報が自動的に最新の情報に更新されるようになります。

サポートサービスサイトから最新の情報を取得すると、管理対象のコンピュータに最新の更新プログラムやウィルス対策製品が適用されているかどうかを、セキュリティポリシーで判定できるようになります。

注意事項

サポートサービスサイトと接続するためには、サポートサービス契約をしている必要があります。

サポートサービスと接続するための情報を設定するには：

1. 設定画面を表示します。
2. メニューエリアで「他システムとの接続」－「サポートサービスの設定」を選択します。
3. インフォメーションエリアで、接続するサポートサービスの情報を設定します。

接続するサポートサービスの情報については、リリースノートを確認してください。[接続テスト] ボタンをクリックすると、設定したサポートサービスに接続できるかどうかを確認できます。

[更新スケジュールの編集] で、サポートサービスサイトから最新の更新プログラム情報およびウィルス対策製品情報を取得するスケジュールを設定できます。

また、[更新プログラム一覧の更新通知先] で、セキュリティ画面の更新プログラム一覧が更新されたことをメール通知する宛先も設定できます。

4. [適用] ボタンをクリックします。

[更新スケジュールの編集] で設定したスケジュールに従って、サポートサービスサイトから最新のサポート情報がダウンロードされます。また、ダウンロードされた結果、更新プログラム一覧が更新された場合は、設定した宛先にメール通知されます。

ポイント

管理用サーバが外部のネットワークに接続できない場合は、外部に接続できるコンピュータを利用してサポートサービスサイトからサポート情報をダウンロードしてください。ダウンロードしたサポート情報は、[サポートサービスからの情報のオフライン更新] ダイアログ、または `updatesupportinfo` コマンドで管理用サーバに登録できます。

ポイント

サポートサービスサイトから情報を取得してセキュリティポリシーが更新されると、更新のタイミングで機器のセキュリティ状況が判定されます。

関連リンク

- [8.3 updatesupportinfo（サポートサービスからの情報の登録）](#)

4.4 Active Directory 連携構成システムの構築時の設定

4.4.1 Active Directory と接続するための情報を設定する手順

Active Directory に登録されている機器を Hitachi IT Operations Director の管理対象にしたり、組織階層の情報を取り込んだりするためには、探索対象の Active Directory のドメイン情報を設定する必要があります。

Active Directory と接続するための情報を設定するには：

1. 設定画面を表示します。
2. メニューエリアで [他システムとの接続] - [Active Directory の設定] を選択します。
3. Active Directory から組織階層の情報を取得したい場合は、インフォメーションエリアの [Active Directory の組織の情報を取得して、部署の情報に反映する] にチェックします。
4. 接続する Active Directory の情報を設定します。
Active Directory の情報を複数設定する場合は、[追加] ボタンをクリックして情報を追加します。
5. [接続テスト] ボタンをクリックして、設定した Active Directory に接続できるかどうかを確認します。
6. 接続に問題がないことを確認できたら、[適用] ボタンをクリックします。

Active Directory の探索を開始すると、ここで設定した Active Directory の情報が収集されます。

Active Directory の探索と同時にエージェントを配信する場合は、この画面で設定した認証情報が利用されます。

関連リンク

- [4.4.4 探索条件を設定する手順 \(Active Directory の探索\)](#)

4.4.2 追加管理項目として Active Directory から取得する情報を設定する手順

Active Directory で管理されている各機器の詳細情報を、追加管理項目として取得できます。Active Directory で管理されている情報を追加管理項目として取得するには、追加管理項目の入力方法に [Active Directory から取得] を指定します。取得対象となる Active Directory の管理項目も設定します。

追加管理項目として Active Directory から取得する情報を設定するには：

1. 設定画面を表示します。

2. [資産管理] – [資産管理項目の設定] を選択します。

3. Active Directory から情報を取得する項目を作成または編集します。

項目を新規作成する場合は [項目を追加] ボタンをクリックします。項目を編集する場合は、項目を選択して [編集] ボタンをクリックします。

4. 表示されるダイアログで [入力方法] を [Active Directory から取得] に設定します。

5. 取得対象となる Active Directory の管理項目を設定します。

このように設定することで、Active Directory で管理されている情報が、各機器の追加管理項目として取得されるようになります。

4.4.3 Active Directory に登録されている機器を探索する手順

機器を探索する方法の一つです。Active Directory に登録されている機器を探索できます。

設定画面の [他システムとの接続] – [Active Directory の設定] 画面で、探索する Active Directory のドメイン情報を設定したあと、設定画面の [機器の探索] – [探索条件の設定] – [Active Directory の探索] 画面で探索スケジュールなどを設定します。[探索を開始] ボタンをクリックすると、設定したスケジュールに従って探索が開始されます。

Active Directory に登録されている機器を探索するには：

1. 設定画面の [他システムとの接続] – [Active Directory の設定] 画面を表示します。

2. 接続する Active Directory のドメイン情報を設定します。

[接続テスト] ボタンをクリックすると、設定した Active Directory に接続できるかどうかを確認できます。

3. 設定画面の [機器の探索] – [探索条件の設定] – [Active Directory の探索] 画面を表示します。

4. [探索スケジュール] で探索スケジュールを設定します。

5. [発見した機器への操作] で、発見した機器を自動的に管理対象にするかどうか、エージェントを自動配信するかどうかを設定します。

6. 探索の完了を管理者にメールで通知したい場合は、[完了通知] で通知先を設定します。

7. 画面右上の [探索を開始] ボタンをクリックします。

設定画面の [機器の探索] – [探索履歴の確認] – [Active Directory の探索] 画面に移動し、設定した探索スケジュールに従って探索が実行されます。

関連リンク

- [4.4.4 探索条件を設定する手順 \(Active Directory の探索\)](#)

- 1.7.3 機器の探索状況の確認

4.4.4 探索条件を設定する手順（Active Directory の探索）

Active Directory に登録されている機器を探索する場合の探索条件を設定できます。

探索条件を設定するには：

1. 設定画面を表示します。
2. メニューエリアで [機器の探索] - [探索条件の設定] - [Active Directory の探索] を選択します。
3. [探索スケジュール] を編集します。
スケジュールを決めて定期的に探索を実行する場合に、スケジュールを設定してください。
4. [発見した機器への操作] を編集します。
機器の探索時に新しい機器が発見された場合の操作を設定してください。

5. [完了通知] を編集します。

機器の探索が完了したら Hitachi IT Operations Director の管理者にメールで通知する場合に、通知先を設定してください。

Hitachi IT Operations Director が利用するメールサーバ（SMTP サーバ）の情報を設定していない場合は、[メールサーバの設定へ] のリンクをクリックして表示される画面で、メールサーバの情報を設定してください。

注意事項

接続する Active Directory のドメインを設定していないと探索は実行できません。[Active Directory の設定] 画面で、Active Directory のドメインを設定してください。

探索条件の設定が完了します。

設定した探索条件で探索を即時実行する場合は、[探索を開始] ボタンをクリックしてください。即時実行しない場合は、[探索スケジュール] に従って実行されます。

探索の実行状況と実行結果は、設定画面の [探索履歴の確認] - [Active Directory の探索] 画面で確認できます。

関連リンク

- 1.7.3 機器の探索状況の確認

4.4.5 機器を管理対象にする手順

探索で発見された機器や除外対象の機器のうち、管理する機器は、管理対象にします。

機器を管理対象にすることで、機器情報を収集したり、セキュリティ状況を把握したりできるようになります。

機器を管理対象にするには：

1. 設定画面を表示します。
2. メニューエリアで [機器の探索] – [発見した機器] を選択します。
3. 管理対象にする機器を選択します。
4. [管理対象にする] ボタンをクリックします。

機器が管理対象になります。

管理対象の機器は、機器画面で収集された機器情報を確認できます。

ポイント

ネットワークモニタ機能が導入されている場合、機器が発見された時点では、ネットワークモニタ設定やネットワーク制御リストの設定に基づいて、機器のネットワーク接続が制御されます。機器を管理対象に設定すると、自動的にネットワーク接続が許可されます。

注意事項

機器を管理対象にすると、1 台につきライセンスを 1 つ使用します。ライセンスが不足している場合は、機器を管理対象にできません。この場合、ライセンスを購入して追加する必要があります。

4.5 MDM 連携構成システムの構築時の設定

4.5.1 MDM システムと連携するための情報を設定する手順

MDM システムからスマートデバイスの情報を取得して Hitachi IT Operations Director で管理するためには、MDM システムとの接続情報や情報の取得スケジュールなどを設定する必要があります。

注意事項

MDM 連携の設定は、1 台の MDM サーバにつき 1 つとしてください。1 台の MDM サーバに対して複数の設定があると、Hitachi IT Operations Director からスマートデバイスを制御できないことがあります。

MDM システムと連携するための情報を設定するには：

1. MDM 製品のサーバ証明書を入手します。

1. Web ブラウザで MDM 製品のポータル画面にアクセスします。
2. サーバ証明書をファイルにエクスポートします。

Internet Explorer の場合

- (i)画面上で右クリックして [プロパティ] - [証明書] - [詳細] - [ファイルにコピー] を選択します。
- (ii)証明書のエクスポートウィザードで、証明書を「DER encoded binary X.509」形式でエクスポートします。

Firefox の場合

- (i)画面上で右クリックして [ページの情報を表示] - [セキュリティ] - [証明書を表示] - [詳細] - [エクスポート] を選択します。
- (ii)証明書の保存ダイアログで、証明書を「X.509 証明書(DER)」形式で保存します。

2. 手順 1. で入手したサーバ証明書を管理用サーバにコピーします。

3. サーバ証明書を管理用サーバにインポートします。

管理用サーバのコマンドプロンプトで次のコマンドを実行してください。

```
Hitachi IT Operations Director のインストール先フォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe  
-import -keystore Hitachi IT Operations Director のインストール先フォルダ¥mgr¥uCPSB¥jdk  
¥jre¥lib¥security¥cacerts -file ¥サーバ証明書のパス¥ -alias ¥サーバ証明書の別名※
```

注※ サーバ証明書のパスとは、手順 2. でコピーしたサーバ証明書のパスです。サーバ証明書の別名とは、インポートするサーバ証明書の別名称のことで、任意の名前を設定できます。

コマンドを実行するとサーバ証明書をインポートするためのパスワードを要求されます。パスワードを入力してください。デフォルトのパスワードは「changeit」です。

4. Hitachi IT Operations Director の設定画面を表示します。
5. メニューエリアで [他システムとの接続] – [MDM 連携の設定] を選択します。
6. インフォメーションエリアの [MDM 連携の設定] で、[追加] ボタンをクリックします。
7. 表示されるダイアログで、接続する MDM システムの情報を設定します。
8. [接続テスト] ボタンをクリックして、設定した MDM システムに接続できるかどうかを確認します。
9. [取得スケジュール] を編集します。
スケジュールを決めて定期的にスマートデバイスの情報を更新する場合に、スケジュールを設定してください。
10. [OK] ボタンをクリックします。
11. インフォメーションエリアの [発見した機器への操作] で、[編集] ボタンをクリックします。
12. 表示されるダイアログで、発見されたスマートデバイスを自動的に管理対象にするかどうかを設定します。

[MDM 連携の設定] で設定したスケジュールに従って、MDM システムからスマートデバイスの情報が取得されます。

[MDM 連携の設定] で指定したユーザー ID に対して、MobileIron で「API」権限を割り当てる必要があります。

ポイント

発見されたスマートデバイスは、[発見した機器への操作] の設定に従って管理対象になります。発見された機器を自動的に管理対象にする設定にしていない場合、スマートデバイスを管理するためには、設定画面の [発見した機器] 画面で、スマートデバイスを管理対象にする必要があります。

ポイント

MDM システムから取得したサーバ証明書を、管理用サーバにインポートしたあとで変更する場合は、変更後のサーバ証明書を再取得し、管理用サーバに再インポートする必要があります。

関連リンク

- [1.7.5 発見した機器を確認する手順](#)
- [1.7.6 管理対象の機器を確認する手順](#)

4.6 ネットワーク監視構成システムの構築時の設定

4.6.1 ネットワーク制御リストの機器を編集する手順

設定画面の [ネットワーク制御リストの設定] 画面のネットワーク制御リストに登録されている機器の設定を編集できます。

ネットワーク制御リストの機器を編集するには：

1. 設定画面を表示します。
2. メニューエリアで [ネットワーク制御] – [ネットワーク制御リストの設定] を選択します。
3. インフォメーションエリアで、編集したい機器の [編集] ボタンをクリックします。
4. 表示されるダイアログで情報を編集して、[OK] ボタンをクリックします。

選択した機器のネットワーク制御の設定が更新されます。

4.6.2 ネットワーク制御リストの自動更新の設定を編集する手順

設定画面の [ネットワーク制御リストの設定] 画面で、ネットワーク制御リストの自動更新の設定を編集できます。

ネットワーク制御リストの自動更新の設定を編集するには：

1. 設定画面を表示します。
2. メニューエリアで [ネットワーク制御] – [ネットワーク制御リストの設定] を選択します。
3. インフォメーションエリアで、[ネットワーク制御リストの自動更新] の [編集] ボタンをクリックします。
4. 表示されるダイアログで、ネットワーク制御リストの自動更新について設定します。
5. [OK] ボタンをクリックします。

ネットワーク制御リストの自動更新の設定が更新されます。

4.6.3 ネットワークモニタ設定を追加する手順

設定画面の［ネットワーク制御の設定］画面の一覧に、ネットワークモニタ設定を追加できます。ネットワークモニタ設定を追加すると、ネットワークセグメントごとに新規に発見された機器のネットワーク接続を許可するかどうかを設定できるようになります。

ネットワークモニタ設定を追加するには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワーク制御の設定］を選択します。
3. インフォメーションエリアで［ネットワークモニタ設定］の［追加］ボタンをクリックします。
4. 表示されるダイアログでネットワークモニタ設定名と、発見した機器への動作を設定して、［OK］ボタンをクリックします。

ネットワークモニタ設定が追加され、［ネットワークモニタ設定］の一覧に表示されます。

なお、ネットワークモニタ設定を追加しただけでは、ネットワークを制御できません。このあと、ネットワークモニタ設定の割り当てを実施してください。

4.6.4 ネットワークモニタ設定の割り当てを変更する手順

設定画面の［ネットワークモニタ設定の割り当て］画面から、ネットワークセグメントに割り当てられているネットワークモニタ設定を変更できます。

ポイント

ネットワークモニタが無効になっている場合、ネットワークモニタ設定の割り当てを変更できません。ネットワークモニタ設定の割り当てを変更する場合、先にネットワークモニタを有効にしてください。

ネットワークモニタ設定の割り当てを変更するには：

1. 設定画面を表示します。
2. メニューエリアで［ネットワーク制御］－［ネットワークモニタ設定の割り当て］を選択します。
3. インフォメーションエリアの上部で、ネットワークモニタ設定の割り当てを変更するネットワークセグメントを選択して、［ネットワークモニタ設定を変更］ボタンをクリックします。
4. 表示されるダイアログで、割り当てるネットワークモニタ設定を選択して、［OK］ボタンをクリックします。

選択したネットワークセグメントに、ネットワークモニタ設定の割り当てが変更されます。

5

製品の上書きインストールおよびコンポーネントのアップデート

ここでは、Hitachi IT Operations Director の上書きインストール、およびコンポーネント（エージェントおよびネットワークモニタエージェント）のアップデートについて説明します。

5.1 Hitachi IT Operations Director を上書きインストールする手順

Hitachi IT Operations Director の上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、上書きインストール中は、ハードディスクに最低 2.4 ギガバイトの空き容量が必要です。

注意事項

上書きインストールする前に、Hitachi IT Operations Director からログアウトして、操作画面を閉じてください。操作画面を表示したまま上書きインストールすると、インストール完了後に操作画面が正しく表示されない場合があります。

注意事項

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

注意事項

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

注意事項

インストール前は、すべての Windows アプリケーションを終了させてください。誤って Hitachi IT Operations Director のプログラムを起動したままインストールを実行した場合は、インストールの実行結果に関係なく OS を再起動してください。OS を再起動しても、サービスが起動しない場合や、Hitachi IT Operations Director のプログラムが動作しない場合は、次に示す手順でインストールを再実行してください。

1. すべての Windows アプリケーションを終了させてください。
2. サービス（IT Operations Director Service）を停止してください。
3. 上書きインストールを再実行してください。サービスが開始されます。

Hitachi IT Operations Director を上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される【日立総合インストーラ】ダイアログで、【Hitachi IT Operations Director】を選択して、【インストール実行】ボタンをクリックします。

3. インストール開始のダイアログで [次へ] ボタンをクリックします。
4. [使用許諾契約] ダイアログで、内容を確認してから [使用許諾契約の条項に同意します] を選択し、[次へ] ボタンをクリックします。
5. インストールの開始準備の完了を示すダイアログで、内容を確認し、[インストール] ボタンをクリックします。
インストールが実行されます。なお、クラスタ構成の場合は、必要に応じてサービス停止を促すダイアログが表示されます。表示内容に従って操作してください。
6. インストールの完了を示すダイアログで、コンポーネントのアップデートに関する設定をして、[完了] ボタンをクリックします。
コンポーネントのアップデートについては、「[5.5 コンポーネントのアップデート方法](#)」を参照してください。

ポイント

データベースのアップグレードが必要な場合は、上書きインストールの完了を示すダイアログに、セットアップを起動するための [セットアップ] が表示されます。ここをチェックするか、またはスタートメニューからセットアップを起動して実行してください。この場合、コンポーネントに関する設定は、セットアップの完了を示すダイアログに表示されます。

Hitachi IT Operations Director の上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

関連リンク

- [1.2.3 管理用サーバをセットアップする手順](#)

5.2 エージェントを提供媒体から上書きインストールする手順

エージェントの上書きインストールを実行するには、インストール対象のバージョンが、すでにインストールされているバージョン以上である必要があります。また、Administrator 権限を持つユーザーで OS にログオンしている必要があります。

注意事項

ユーザーアカウント制御（UAC）がサポートされている Windows のコンピュータにインストールする場合は、権限の昇格を求めるダイアログが表示されることがあります。このダイアログが表示されたときは、権限を昇格してください。

注意事項

インストール中に OS をシャットダウンしないでください。途中で OS をシャットダウンした場合、あとで再インストールしても正常に実行されないおそれがあります。

エージェントを上書きインストールするには：

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される [日立総合インストーラ] ダイアログで、[Hitachi IT Operations Director Agent] を選択して、[インストール実行] ボタンをクリックします。
3. インストール開始のダイアログで [次へ] ボタンをクリックします。
4. インストールの開始準備の完了を示すダイアログで、[インストール] ボタンをクリックします。
インストールが実行されます。
5. インストールの完了を示すダイアログで、[完了] ボタンをクリックします。

エージェントの上書きインストールが完了します。再起動を要求するメッセージが表示された場合は、コンピュータを再起動してください。

5.3 Hitachi IT Operations Director のシステム全体をバージョンアップする流れ

Hitachi IT Operations Director のシステム全体のバージョンアップは、配布機能または提供媒体を使用する場合と、管理用サーバに登録されたプログラムでコンポーネントを自動的にアップデートする場合とで、流れが異なります。

配布機能または提供媒体を使用してバージョンアップするには：

管理者が任意のタイミングでバージョンアップする場合は、事前に、管理用サーバに登録されたプログラムの自動アップデートの機能を無効にしてください。

1. 管理用サーバに新しいバージョンのプログラムを上書きインストールすることで、Hitachi IT Operations Director をバージョンアップします。
2. 次のコンポーネントをアップデートします。
 - ・ ネットワークモニタエージェントがインストールされているコンピュータのエージェントおよびネットワークモニタエージェント
 - ・ 管理者のコンピュータにインストールされているリモートコントロール機能のコントローラ
3. ネットワークモニタエージェントがインストールされていないコンピュータのエージェントをアップデートします。

管理用サーバに登録されたプログラムでコンポーネントを自動的にアップデートすることでバージョンアップするには：

1. 管理用サーバに新しいバージョンのプログラムを上書きインストールすることで、Hitachi IT Operations Director をバージョンアップします。
2. 管理用サーバにエージェントおよびネットワークモニタのコンポーネントに登録し、自動的にアップデートするよう設定します。

注意事項

Hitachi IT Operations Director のバージョンアップ後に、リモートコントロールを実行する場合は、事前にコントローラをバージョンアップしてください。

関連リンク

- ・ [5.4 Hitachi IT Operations Director をバージョンアップする手順](#)
- ・ [5.5 コンポーネントのアップデート方法](#)

5.4 Hitachi IT Operations Director をバージョンアップする手順

管理用サーバで、新しいバージョンのプログラムを上書きインストールすることで、Hitachi IT Operations Director をバージョンアップします。

注意事項

- バージョンアップする前に、Hitachi IT Operations Director からログアウトして、操作画面を閉じてください。操作画面を表示したままバージョンアップすると、バージョンアップ後に操作画面が正しく表示されない場合があります。
- セキュリティポリシーとして禁止操作のポリシーを設定していた場合は、Hitachi IT Operations Director 04-00 から Hitachi IT Operations Director 04-50 に上書きインストールしたあと、セキュリティ設定項目の「禁止操作」－「機器の使用抑止」で設定し直すことを推奨します。禁止操作のポリシーを設定する方法については、マニュアル「Hitachi IT Operations Director 運用ガイド」のデバイスの使用を抑止する手順の説明を参照してください。
- Hitachi IT Operations Director を 04-00 から 04-50 にバージョンアップした場合、04-50 のセキュリティポリシーを適用するまでは、04-00 のセキュリティポリシーが適用されたままになります。
- Hitachi IT Operations Director 04-50 では、04-00 以前と比較して制御するデバイスの区分が変更されています。04-00 以前のリムーバブルディスクの「読み取りと書き込みを抑止する」を使用している場合には、04-50 で変更されたデバイス区分で設定してください。04-50 で抑止できるデバイスは、マニュアル「Hitachi IT Operations Director 導入・設計ガイド」の、使用を抑止できるデバイスの説明を参照してください。04-00 以前のリムーバブルディスクの範囲で抑止を設定したい場合には、リムーバブルディスクの書き込み抑止を使用することを検討してください。

Hitachi IT Operations Director をバージョンアップするには：

1. データベースのバックアップを取得します。

障害に備えて、バックアップを取得してください。

データベースのバックアップは、データベースマネージャを利用してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

2. 管理用サーバの Hitachi IT Operations Director を上書きインストールします。

上書きインストール中は、ハードディスクに最低 2.4 ギガバイトの空き容量が必要です。

注意事項

上書きインストールに失敗した場合は、上書きインストール前の環境に戻してから手順 2.以降の作業をしてください。上書きインストール前の環境に戻すには、旧バージョンのプログラムをインストールしてライセンスを認証したあと、手順 1.でバックアップしたデータベースをリ

ストアします。データベースのリストアは、データベースマネージャを利用してください。なお、旧バージョンのプログラムが手元にない場合は、サポートサービスへお問い合わせください。

ポイント

上書きインストール時にコンポーネントを自動的にアップデートする設定にしている場合、利用者のコンピュータにインストールされているエージェントおよびネットワークモニタエージェントが自動的に更新されます。

ポイント

エージェントおよびネットワークモニタエージェントが自動的に更新される際に、管理用サーバから各コンピュータにデータが送信されます。エージェント導入済みのコンピュータには、1台当たり約 35 メガバイトのデータが送信されます。これに追加して、ネットワークモニタエージェントがインストールされているエージェント導入済みのコンピュータには、1台当たり約 5 メガバイトのデータが送信されます。

3. データベースをアップグレードします。

セットアップで、データベースをアップグレードします。

ポイント

データベースのアップグレードが完了したら、手順 1. で取得したデータベースのバックアップを削除してかまいません。

Hitachi IT Operations Director のバージョンアップが完了します。

上書きインストール時の Hitachi IT Operations Director 04-00 の操作ログの自動取り込み：

Hitachi IT Operations Director 04-00 の操作ログのデータベースに格納されているオンライン領域の最大 30 日分の操作ログを、Hitachi IT Operations Director 04-50 への上書きインストール時に、Hitachi IT Operations Director 04-50 の操作ログのデータベースに自動的に取り込むことができます。セットアップの完了画面で [旧製品の操作ログの取り込み] にチェックしてください。なお、自動的に取り込んだ操作ログは、設定画面の [操作ログの設定] 画面－ [自動取り込みされる操作ログの格納期間] の設定値を過ぎると自動的に削除されます。

注意事項

- Hitachi IT Operations Director 04-00 の操作ログを自動的に取り込むには、上書きインストール前に Hitachi IT Operations Director 04-00 のセットアップで操作ログの保管先を設定しておく必要があります。

- Hitachi IT Operations Director 04-00 の操作ログの取り込みには、1 日以上かかる場合があります。
- Hitachi IT Operations Director 04-00 の操作ログの取り込みの進捗は、ホーム画面の [監視候補の処理]、またはセキュリティ画面の [保管した操作ログの手動取り込み] ダイアログで確認できます。
- Hitachi IT Operations Director 04-00 の操作ログの取り込みには、Hitachi IT Operations Director 04-50 の手動取り込みを使用するため、イベントやメッセージには「手動取り込み」と表示されます。

ポイント

Hitachi IT Operations Director 04-00 のセットアップで操作ログの保管先が設定されていない場合、Hitachi IT Operations Director 04-00 の操作ログのデータベースに格納されているオンライン領域の操作ログデータは、Hitachi IT Operations Director 04-50 への上書きインストールでデータベース退避フォルダに出力されます。出力先はセットアップの完了画面にも表示されます。Hitachi IT Operations Director 04-50 の操作ログのデータベースに取り込むには、Hitachi IT Operations Director 04-50 の管理用サーバのセットアップで操作ログの保管先を設定して、次のファイルをコピーして、手動取り込みを実施してください。

- OPR_CATALOG_YYYYMMDD.csv
- OPR_DATA_YYYYMMDD.zip
- OPR_OTHER.zip

5.5 コンポーネントのアップデート方法

コンポーネントとは、エージェントおよびネットワークモニタエージェントを指します。これらのプログラムには、次に示すアップデート方法があります。

管理用サーバに登録されたプログラムで自動的にアップデートする

管理用サーバに新しいバージョンのプログラムを登録し、自動配信してアップデートします。

システム全体のバージョンアップの際など、Hitachi IT Operations Director を含めて複数のプログラムをアップデートする場合は、Hitachi IT Operations Director の上書きインストール時にコンポーネントの自動アップデートを設定することで、新しいバージョンのエージェントおよびネットワークモニタエージェントが管理用サーバに自動で登録され、配信されます。

コンポーネントの自動アップデートの設定、および各プログラムの管理用サーバへの登録は、Hitachi IT Operations Director の上書きインストール完了を示すダイアログ、または管理用サーバの [スタート] メニューから表示する [コンポーネントの登録] ダイアログで実施できます。

配布機能を使用してアップデートする

管理用サーバにパッケージを登録し、タスクを作成して配布することでアップデートします。ネットワークに負荷が掛かるタイミングを制御したいなどの理由で、自動ではアップデートしたくない場合に便利です。自動アップデートしたくない場合は事前に管理用サーバに登録されたプログラムの自動アップデートの機能を無効にする必要があります。

システム全体のバージョンアップの際など、Hitachi IT Operations Director を含めて複数のプログラムをアップデートする場合は、Hitachi IT Operations Director の上書きインストール時にコンポーネントのパッケージ登録を設定することで、新しいバージョンのエージェントおよびネットワークモニタエージェントがパッケージとして管理用サーバに自動で登録されます。

コンポーネントのパッケージ登録の設定、および各プログラムの管理用サーバへの登録は、Hitachi IT Operations Director の上書きインストール完了を示すダイアログ、または管理用サーバの [スタート] メニューから表示する [コンポーネントの登録] ダイアログで実施できます。

自動的に登録されるパッケージの名称は [プログラム形名_バージョン番号_各コンポーネントのプログラム名] (例: [P-2642-8654_0450_Hitachi IT Operations Director Agent]) です。このパッケージを指定したタスクを追加して配布してください。タスクを追加する際は、コンポーネントが「[5.3 Hitachi IT Operations Director のシステム全体をバージョンアップする流れ](#)」に記載されている順番でアップデートされるようにしてください。

ポイント

すでに同じバージョンのパッケージが登録されている場合、上書き登録はされません。

提供媒体を使用してアップデートする

新しいバージョンの提供媒体から各プログラムを上書きインストールすることでアップデートします。上書きインストールは、「[5.3 Hitachi IT Operations Director のシステム全体をバージョンアップする流れ](#)」に記載されている順番でアップデートされるようにしてください。

コントローラをアップデートする

Hitachi IT Operations Director のバージョンアップに伴ってコントローラが更新された場合は、操作画面からリモートコントロールを実行したタイミングで自動的に上書きインストールされます。

なお、[スタート] メニューからリモートコントロールを実行しても、コントローラは上書きインストールされません。[スタート] メニューからリモートコントロールを実行する運用のときは、エージェントをアップデートする前に、操作画面からリモートコントロールを実行して、コントローラをバージョンアップしてください。

注意事項

次の場合、コントローラは自動的に上書きインストールされません。

- プロキシサーバを介して Hitachi IT Operations Director に接続している環境で、インターネットオプションのプロキシサーバが正しく設定されていない場合
- Internet Explorer がオフラインモードになっている場合

関連リンク

- [5.6 コンポーネントを登録する手順](#)

5.6 コンポーネントを登録する手順

コンポーネントとは、エージェントおよびネットワークモニタエージェントのことです。

アップデート版のコンポーネントまたは修正パッチがリリースされた場合、それらのプログラムを管理用サーバに登録して、自動アップデートするように設定すると便利です。

ネットワークに負荷が掛かるタイミングを制御したいなどの理由で、自動ではアップデートしたくない場合も、管理用サーバにアップデート版のプログラムを登録することで、パッケージの自動登録ができます。この場合は、自動登録されたパッケージを指定してタスクを作成し、配布します。

ポイント

Hitachi IT Operations Director をバージョンアップする場合は、Hitachi IT Operations Director の上書きインストールの際にコンポーネントの自動アップデートやパッケージ登録を設定できます。この場合、アップデート版のコンポーネントが自動的に管理用サーバに登録されて配信またはパッケージ登録されるので、ここで説明する操作は不要です。

ポイント

エージェントおよびネットワークモニタエージェントが自動的に更新される際に、管理用サーバから各コンピュータにデータが送信されます。エージェント導入済みのコンピュータには、1 台当たり約 35 メガバイトのデータが送信されます。これに追加して、ネットワークモニタエージェントがインストールされているエージェント導入済みのコンピュータには、1 台当たり約 5 メガバイトのデータが送信されます。

コンポーネントを登録するには：

1. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [コンポーネントの登録] を選択します。
2. 表示されるダイアログで [参照] ボタンをクリックして、ダウンロードしたフォルダにあるアップグレード版のコンポーネントまたは修正パッチを指定します。
3. 登録したコンポーネントについて、自動アップデートおよびパッケージ登録について設定します。
4. [OK] ボタンをクリックします。

アップグレード版のコンポーネントまたは修正パッチが管理用サーバに登録され、設定内容に応じて、配信またはパッケージ登録されます。

5.7 クラスタシステムで上書きインストールする流れ

クラスタシステムで Hitachi IT Operations Director を上書きインストールするには、現用系サーバで上書きインストールしたあと、待機系サーバで上書きインストールします。

クラスタシステムを上書きインストールするには：

1. 現用系サーバの Hitachi IT Operations Director のサービスリソースをオフラインにします。
オフラインにするサービスリソースについては、「[2.7.2 現用系サーバでグループリソースを作成する手順](#)」の、グループに登録が必要なリソースの表にある「Hitachi IT Operations Director のサービスリソース（汎用サービス）」を参照してください。IP アドレスリソース、ネットワーク名リソース、および共有ディスク（物理ディスク）リソースは、オンラインのままです。
2. 現用系サーバで Hitachi IT Operations Director を上書きインストールします。
3. 現用系サーバでセットアップを起動し、データベースアップグレードを実行します。
データベースのアップグレードが不要な場合は、この手順は実行不要です。
4. 現用系サーバのセットアップ完了時に出力されるファイルを待機系サーバにコピーします。
5. グループリソースの所有者を待機系サーバに移動します。
6. 待機系サーバで Hitachi IT Operations Director を上書きインストールします。
7. 待機系サーバでセットアップを起動し、データベースアップグレードを実行します。
データベースのアップグレードが不要な場合は、この手順は実行不要です。
8. グループリソースの所有者を現用系サーバに移動します。
9. 手順 1. でオフラインにしたサービスリソースをオンラインにします。

クラスタシステムの上書きインストールが完了します。

関連リンク

- [5.1 Hitachi IT Operations Director を上書きインストールする手順](#)

6

製品のアンインストール

ここでは、Hitachi IT Operations Director の各種プログラムをアンインストールする方法について説明します。

6.1 システム全体でのアンインストールの流れ

1. 機器のネットワーク接続を監視している場合は、各ネットワークセグメントのネットワークモニタを無効にします。
2. エージェント導入済みのコンピュータからエージェントをアンインストールします。
3. 管理用サーバから Hitachi IT Operations Director をアンインストールします。

このほか、リモートコントロール機能を使用している場合は、管理者のコンピュータからコントローラをアンインストールする必要があります。コントローラのアンインストールは、どのタイミングで実施しても問題ありません。

ポイント

リモコンエージェントは、エージェントをアンインストールすると自動的にアンインストールされます。

関連リンク

- [6.4 ネットワークモニタを無効にする手順](#)
- [6.3 エージェントをアンインストールする手順](#)
- [6.2 Hitachi IT Operations Director をアンインストールする手順](#)
- [6.5 コントローラをアンインストールする手順](#)

6.2 Hitachi IT Operations Director をアンインストールする手順

Hitachi IT Operations Director を再インストールする場合や管理用サーバを変更したい場合は、Hitachi IT Operations Director をアンインストールします。

■ 注意事項

アンインストールの実行中に、OS をシャットダウンしないでください。シャットダウンすると、アンインストールを再実行した場合に、正常にアンインストールされないことがあります。

■ 注意事項

アンインストール前は、すべての Windows アプリケーションを終了させてください。誤って Hitachi IT Operations Director のプログラムを起動したままアンインストールを実行した場合は、アンインストールの実行結果に関係なく OS を再起動してください。

Hitachi IT Operations Director をアンインストールするには：

1. Windows のコントロールパネルで [プログラムと機能] を起動します。
2. 「Hitachi IT Operations Director」を選択し、[変更] ボタンをクリックします。
3. Hitachi IT Operations Director 用のインストールウィザードで [次へ] ボタンをクリックします。
4. アンインストールの確認画面で [削除] ボタンをクリックします。
5. アンインストールの終了画面で [完了] ボタンをクリックします。

Hitachi IT Operations Director がアンインストールされます。

■ ポイント

Hitachi IT Operations Director をアンインストールしても、各コンピュータのエージェントをアンインストールする必要はありません。ただし、コンピュータに常駐するプロセスがあるため、Hitachi IT Operations Director を利用しない場合は、エージェントはアンインストールすることをお勧めします。

関連リンク

- [6.5 コントローラをアンインストールする手順](#)
- [6.6 クラスタシステムで Hitachi IT Operations Director をアンインストールする手順](#)

6.3 エージェントをアンインストールする手順

Hitachi IT Operations Director で詳細な情報を管理する必要がなくなったコンピュータからは、エージェントをアンインストールします。エージェントをアンインストールしたオンライン管理のコンピュータは、自動的にエージェントレスのコンピュータになります。

ポイント

試用版のエージェントも同様の手順でアンインストールできます。試用期限が切れた場合も同様です。

注意事項

ネットワークモニタが有効になっていると、エージェントをアンインストールできません。対象のコンピュータのネットワークモニタを無効にしてから、エージェントをアンインストールしてください。

エージェントをアンインストールするには：

1. Windows のコントロールパネルで [プログラムと機能] を起動します。
2. [Hitachi IT Operations Director Agent] を選択し、[アンインストール] ボタンをクリックします。
3. アンインストールの確認画面で [はい] ボタンをクリックします。
Hitachi IT Operations Director のエージェントがアンインストールされます。
4. コンピュータを再起動します。

注意事項

エージェントのアンインストール後にコンピュータを再起動しない場合、ほかのアプリケーションのネットワーク通信が失敗することがあります。

コンピュータの廃棄やリース返却などに伴い、Hitachi IT Operations Director での管理が不要になったコンピュータは、機器情報を削除します。

注意事項

エージェントにパスワード保護が設定されている場合、手順 3.のあとにパスワードの入力画面が表示されます。該当するエージェント設定に設定したパスワードを入力してください。パスワードのデフォルトは「manager」です。

注意事項

オンライン管理用のエージェントをアンインストールする際、管理用サーバと接続できなかった場合は、アンインストール続行の確認画面が表示されます。再度管理用サーバに接続を試みるか、接続を確認しないでアンインストールを続行するかを選択できます。管理用サーバに接続しないでアンインストールした場合、管理用サーバでは対象のコンピュータをエージェント導入済みのコンピュータとして扱います。エージェントレスのコンピュータとして管理するためには、いったん機器情報を削除してから探索で発見するなどして、コンピュータを登録し直してください。

オフライン管理用のエージェントをアンインストールする際は、アンインストール続行の確認画面は表示されません。

関連リンク

- [6.4 ネットワークモニタを無効にする手順](#)

6.4 ネットワークモニタを無効にする手順

特定のネットワークセグメントだけネットワーク接続を監視しないで運用したい場合や、ネットワークの監視を中止したい場合は、ネットワークモニタを無効にします。

ネットワークモニタを無効にするには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】で、【機器一覧（ネットワーク）】から該当するネットワークセグメントのグループを選択します。
3. インフォメーションエリアでネットワークモニタを有効にしているコンピュータを選択します。
ネットワークモニタが有効になっているコンピュータは、管理種別に  が表示されています。
4. 【操作メニュー】の【ネットワークモニタを無効にする】を選択します。

選択したコンピュータのネットワークモニタが無効になり、ネットワークが監視されなくなります。

ポイント

ネットワークモニタを無効にすると、対象のコンピュータからネットワークモニタエージェントがアンインストールされます。

ネットワークモニタが無効になると、管理種別は  に戻ります。

なお、メニューエリアに表示されるネットワークモニタの動作状態が「ネットワークモニタを無効化しています」の場合は、ネットワークモニタを無効にできません。

注意事項

ネットワークモニタエージェントをインストールしているコンピュータの動作状態が「ネットワークモニタを無効化しています」または「ネットワークモニタの無効化に失敗しました」の場合は、コンピュータを「除外対象」にできません。

注意事項

ネットワークモニタを無効にする場合、あらかじめ管理用サーバにコンポーネント（ネットワークモニタエージェント）が登録されている必要があります。

ポイント

設定画面の [ネットワーク制御] – [ネットワークモニタ設定の割り当て] 画面でもネットワークモニタを無効にできます。

ポイント

ネットワークモニタを無効にしたコンピュータが複数のネットワークセグメントに所属している場合、所属しているすべてのネットワークセグメントでネットワークモニタが無効になります。

ポイント

ネットワークモニタエージェントをインストールしているコンピュータが管理用サーバに接続できない環境の場合、そのコンピュータで、Windows のコントロールパネルの [プログラムと機能] から [Hitachi IT Operations Director NM Agent] を選択して削除することで、ネットワークモニタを無効にできます。ただし、この方法で無効にするときも、まずは操作画面からの無効化の手順に従って操作し、管理用サーバ上の情報（対象のコンピュータの管理種別）を変更する必要があります。

関連リンク

- [2.6.2 ネットワークモニタを有効にする手順](#)

6.5 コントローラをアンインストールする手順

リモートコントロールを実行する必要のないコンピュータからは、コントローラをアンインストールします。

コントローラをアンインストールするには：

1. Windows のコントロールパネルで [プログラムと機能] を起動します。
2. [Hitachi IT Operations Director RC Manager] を選択し、[アンインストール] ボタンをクリックします。
3. 表示されるダイアログで [はい] ボタンをクリックします。

コントローラがアンインストールされます。

ポイント

リモコンエージェントは、エージェントをアンインストールすると自動的にアンインストールされます。

6.6 クラスタシステムで Hitachi IT Operations Director をアンインストールする手順

クラスタシステムで Hitachi IT Operations Director をアンインストールするには、現用系サーバでアンインストールしたあとで、待機系サーバでアンインストールします。

クラスタシステムで Hitachi IT Operations Director をアンインストールするには：

1. 現用系サーバの Hitachi IT Operations Director のサービスリソースをオフラインにします。
オフラインにするサービスリソースについては、「[2.7.2 現用系サーバでグループリソースを作成する手順](#)」の、グループに登録が必要なリソースの表にある「Hitachi IT Operations Director のサービスリソース（汎用サービス）」を参照してください。IP アドレスリソース、ネットワーク名リソース、および共有ディスク（物理ディスク）リソースは、オンラインのままです。
2. 現用系サーバで Hitachi IT Operations Director をアンインストールします。
3. グループリソースの所有者を待機系サーバに移動します。
4. 待機系サーバで Hitachi IT Operations Director をアンインストールします。

クラスタシステムでのアンインストールが完了します。

関連リンク

- [6.2 Hitachi IT Operations Director をアンインストールする手順](#)

7

環境の移行

ここでは、Hitachi IT Operations Director で環境を移行する方法について説明します。

7.1 管理用サーバをリプレースする手順

管理用サーバのリプレースとは、Hitachi IT Operations Director がインストールされているコンピュータとは別のコンピュータを、管理用サーバとして利用できるようにすることです。

以降の注意事項は、試用版から製品版へ移行する際に併せてリプレースを実施する場合も該当します。

注意事項

リプレース先のコンピュータにインストールする Hitachi IT Operations Director は、リプレース元と製品のバージョン情報が一致している必要があります。

注意事項

管理用サーバのリプレース時に Hitachi IT Operations Director のバージョンアップはできません。リプレース完了後にバージョンアップするか、バージョンアップ後にリプレースしてください。バージョンアップの手順については、「[5.4 Hitachi IT Operations Director をバージョンアップする手順](#)」を参照してください。

注意事項

コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、フォルダの設定時に次のフォルダは指定しないでください。

- システムドライブ:¥program files¥WindowsApps 配下のフォルダ
- 仮想プロビジョニングによって作成した記憶域のフォルダ

管理用サーバをリプレースする手順を次に示します。リプレース先のコンピュータに Hitachi IT Operations Director をインストールして、リプレース元のコンピュータからデータを移行することで、管理用サーバをリプレースします。

管理用サーバをリプレースするには：

1. Hitachi IT Operations Director のサービスを停止します。

データベースのバックアップ後に、エージェントから通知された操作ログが新規に保管されないよう、あらかじめサービスを停止しておきます。

Windows の [スタート] メニューから [管理ツール] - [サービス] を選択してください。表示されるダイアログで、サービス名を右クリックして [停止] を選択すると、サービスを停止できます。停止するサービスを次に示します。

- IT Operations Director Agent Control
- IT Operations Director Service

- IT Operations Director Web Container

2. データベースのバックアップを取得します。

リプレース元のコンピュータで、Windows の [スタート] メニュー – [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [データベースマネージャ] から Hitachi IT Operations Director のデータベースマネージャを起動して、データベースのバックアップを実行してください。バックアップ先フォルダのドライブは、目安として 20 ギガバイト以上の空き容量を確保してください。

3. 操作ログのバックアップデータを退避します。

操作ログを保管する設定にしている場合は、セットアップで指定している「操作ログの保管先フォルダ」に格納されているバックアップデータを退避してください。

操作ログを保管する設定にしているかどうかは、Windows の [スタート] メニュー – [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] から Hitachi IT Operations Director のセットアップを起動して、[操作ログの設定] 画面で [操作ログを保管する] がチェックされているかどうかで確認します。チェックされている場合は、操作ログを保管する設定になっています。

4. リプレース先のコンピュータに、操作ログのバックアップデータを格納します。

手順 3. で操作ログのバックアップデータを退避した場合は、インストール前に、リプレース先のコンピュータで「操作ログの保管先フォルダ」に指定する予定のフォルダに格納しておきます。なお、このフォルダには、操作ログのバックアップデータ以外のデータは格納しないでください。

5. リプレース元のコンピュータをネットワークから切断します。

6. リプレース先のコンピュータに、Hitachi IT Operations Director をインストールします。

7. Hitachi IT Operations Director をセットアップします。

リプレース先のコンピュータで、Windows の [スタート] メニュー – [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [セットアップ] から Hitachi IT Operations Director のセットアップを起動して、セットアップを実行してください。

操作ログを保管する設定にしている場合は、[操作ログの自動保管の設定] 画面で「操作ログの保管先フォルダ」に、手順 4. でバックアップデータを格納したフォルダを指定してください。

8. 手順 2. でバックアップしたデータベースをリストアします。

リプレース先のコンピュータで、Windows の [スタート] メニュー – [すべてのプログラム] – [Hitachi IT Operations] – [Director Tools] – [データベースマネージャ] から Hitachi IT Operations Director のデータベースマネージャを起動して、データベースのリストアを実行してください。

9. ライセンスを認証します。

リプレース先のコンピュータにインストールした Hitachi IT Operations Director のログイン画面で、[ライセンス] ボタンをクリックします。表示されるダイアログで [ライセンス認証] ボタンをクリック

クして、表示されるウィザードからライセンス認証します。ライセンス認証には、リプレース元のコンピュータで認証済みのライセンス認証キーのどれか 1 つを使用します。

10. エージェントの接続先を変更します。

リプレース先のコンピュータにインストールした Hitachi IT Operations Director にログインし、エージェント設定の [エージェント基本動作] - [基本設定] - [管理用サーバ] にリプレース先のコンピュータの IP アドレスまたはホスト名を設定します。

なお、この手順は、リプレースの前後で管理用サーバの IP アドレスまたはホスト名が変更になる場合だけです。

11. 正しく運用できることを確認します。

リプレース先のコンピュータにインストールした Hitachi IT Operations Director で、エージェントが管理用サーバに接続されたかどうかを確認します。機器画面の [機器一覧] 画面で、[最終接続確認日時] が更新されていることを確認してください。

[最終接続確認日時] はデフォルトでは表示されていないため、表示されていない場合は [機器一覧] 画面の一覧の項目を右クリックして、[表示項目の選択] から表示されるダイアログで確認してください。[最終接続確認日時] が更新されない場合、利用者のコンピュータで、Windows の [スタート] メニュー - [すべてのプログラム] - [Hitachi IT Operations Director Agent] - [管理者ツール] - [セットアップ] からエージェントのセットアップを起動して、接続先にリプレース先の管理用サーバが設定されているかどうかを確認してください。

12. リプレース元のコンピュータで、Hitachi IT Operations Director をアンインストールします。

管理用サーバのリプレースが完了します。

ポイント

リプレース元のコンピュータで取得したバックアップは、リプレース完了後に、必要に応じて削除してください。

ポイント

リプレース完了後にエージェントが管理用サーバに接続されたかどうかは、機器画面の [機器一覧] 画面で、[最終接続確認日時] が更新されていることで確認できます。エージェントが接続されない場合、利用者のコンピュータで、エージェントのセットアップから接続先が正しく設定されているかどうか確認してください。

注意事項

コンピュータにライセンス情報を引き継ぐ必要があります。ライセンス情報を引き継ぐには、リプレイス元のコンピュータで認証済みのライセンス認証キーのどれか 1 つを使って、リプレイス先のコンピュータでライセンス認証します。

注意事項

管理用サーバのリプレイスは、不正利用防止のため 2 回までとしています。3 回目以降のリプレイスをしたい場合は、「ライセンス認証手順書」に従ってリプレイス回数の初期化をメールで依頼してください。「ライセンス認証手順書」の URL を次に示します。

<http://www.hitachi.co.jp/Prod/comp/soft1/itoperations/support/activation.pdf>

注意事項

管理用サーバを仮想コンピュータで構築している場合、その仮想コンピュータを複製したときは、別のコンピュータで管理用サーバが構築されたと見なされます。このため、複製した仮想コンピュータを管理用サーバとして利用するときは、ライセンス認証が必要です。また、物理的なリプレイス時と同様に、ライセンスを認証できる回数が 1 回減ります。

注意事項

Hitachi IT Operations Director をインストールしたコンピュータの UUID または SID が変更されると、リプレイスされたと見なされ、ライセンス認証が必要になります。例えば、UUID および SID は次の契機で変更されます。

UUID が変更される契機の例

- マザーボードを交換した。
- 仮想コンピュータを複製※して使用した。

SID が変更される契機の例

- Windows の OS を再インストールした。
- sysprep コマンドで SID を再割り当てした。

注※ 仮想コンピュータの複製に当たる操作の例を次に示します。

- VMware で、仮想マシンのクローン、またはテンプレートからデプロイを使用して複製した仮想マシンを使用する。
- VMware で、仮想マシンフォルダの内容を移動・コピーして、仮想マシンを起動する際に UUID を変更する操作をする (ESX 3.x では「作成」「常に作成」、ESX 4.x では「コピーしました」を選択する)。

リプレイス手順に関する注意事項

注意事項

リプレイス先のコンピュータの IP アドレスが、リプレイス元のコンピュータから変更になる場合、エージェントの接続先を変更するには、リプレイス先の管理用サーバとエージェントの間に互いに直接参照できるネットワーク構成が必要です。直接参照できるネットワークとは、ホスト名および IP アドレスで参照できる、相互に ICMP など通信できるネットワークです。また、管理用サーバとエージェントが使用する TCP プロトコルのポートを通過できるようにしておく必要があります。

注意事項

管理用サーバがリプレイス元のシステム構成を引き継ぐためには、管理対象の機器の IP アドレスがリプレイスの前後で一致している必要があります。

例えば、管理用サーバのリプレイス中に、設置場所の変更によって管理対象のコンピュータの IP アドレスが変更になる場合、そのコンピュータはリプレイス先の管理用サーバには接続されません。このようなときは、リプレイス先の管理用サーバでインストールセットを作成し、そのコンピュータにエージェントを導入し直してください。これによって、コンピュータが管理用サーバに接続されるようになります。

注意事項

リプレイス元のコンピュータで取得したデータベースのバックアップは、管理用サーバのユーザー ID/パスワードと同様に、管理者以外が参照できないように管理してください。このバックアップを不正に入手してリストアすれば、その管理用サーバから管理対象の機器の操作ができてしまうためです。

注意事項

リプレイス元の管理用サーバで管理していた機器を、リプレイス先の管理用サーバで引き続き管理する場合、リプレイス元のコンピュータでバックアップしたデータベースを、リプレイス先のコンピュータにリストアしてください。データベースのリストアを実施しないと、管理対象の機器にインストールされているエージェントがリプレイス先の管理用サーバに接続されません。

なお、リプレイス後の管理用サーバで新たに機器管理を始める場合は、データベースのバックアップとリストアは不要です。この場合、リプレイス前と同じ機器を管理するには、リプレイス完了後に次のように対処してください。

- エージェント導入済みのコンピュータ：リプレイス後の管理用サーバで作成したインストールセットを利用して、エージェントを再インストールしてください。
- エージェントレスの機器：探索を実行して、機器を管理対象にしてください。

■ 注意事項

Hitachi IT Operations Director をアンインストールしないで、リプレイス元の管理用サーバをネットワークに接続した場合、リプレイス先の管理用サーバで正しくエージェントを管理できなくなります。

これは、リプレイス元とリプレイス先の管理用サーバが、それぞれエージェントに接続できてしまうためです。それぞれの管理用サーバから異なる指示があると、エージェントが管理者の意図しない状態になることがあります。また、エージェントがリプレイス元の管理用サーバに接続して通知した情報は、リプレイス先の管理用サーバには通知されないため、管理している情報に差異が発生してしまいます。

関連リンク

- [1.2.2 Hitachi IT Operations Director をインストールする手順](#)
- [1.2.3 管理用サーバをセットアップする手順](#)
- [2.7.1 クラスタシステムを構築する流れ](#)

7.2 エージェント導入済みのコンピュータをリプレイスする手順

エージェント導入済みのコンピュータをリプレイスするには：

1. コンピュータから、エージェントをアンインストールします。
2. コンピュータをリプレイスします。
3. リプレイス後のコンピュータに、エージェントをインストールします。

エージェント導入済みのコンピュータのリプレイスが完了します。

7.3 ネットワークモニタを有効にしたコンピュータをリプレースする手順

ネットワークモニタを有効にしたコンピュータをリプレースするには、いったんネットワークモニタを無効にする必要があります。ネットワークモニタを無効にする手順および有効にする手順については、「[6.4 ネットワークモニタを無効にする手順](#)」および「[2.6.2 ネットワークモニタを有効にする手順](#)」を参照してください。

ネットワークモニタを有効にしたコンピュータをリプレースするには：

1. リプレース元のコンピュータのネットワークモニタを無効にします。
2. リプレース元のコンピュータから、エージェントをアンインストールします。
3. コンピュータをリプレースします。
4. リプレース先のコンピュータに、エージェントをインストールします。
5. リプレース先のコンピュータの、ネットワークモニタを有効にします。

ネットワークモニタを有効にしたコンピュータのリプレースが完了します。

7.4 システム構成要素のホスト名および IP アドレスを変更する

7.4.1 管理用サーバのホスト名を変更する手順

管理用サーバのホスト名を変更したい場合は、次の項目を再設定します。

- エージェントの接続先（接続先をホスト名で指定している場合）

エージェントの接続先（接続先をホスト名で指定している場合）

1. エージェント設定の [エージェント基本動作] - [基本設定] - [管理用サーバ] に、変更後のホスト名を設定します。

ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

7.4.2 管理用サーバの IP アドレスを変更する手順

管理用サーバの IP アドレスを変更したい場合は、次の項目を再設定します。

- エージェントの接続先（接続先を IP アドレスで指定している場合）
- ネットワークへの接続を許可しない機器の特例接続の設定

エージェントの接続先（接続先を IP アドレスで指定している場合）

1. エージェント設定の [エージェント基本動作] - [基本設定] - [管理用サーバ] に、変更後の IP アドレスを設定します。

ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

ネットワークへの接続を許可しない機器の特例接続の設定

[ネットワーク制御の設定] 画面で、[ネットワークへの接続を許可しない機器の特例接続] から変更前の管理用サーバの IP アドレスを削除し、変更後の管理用サーバの IP アドレスを追加してください。

7.4.3 クラスタシステムの論理ホスト名を変更する手順

クラスタシステムの論理ホスト名を変更したい場合は、セットアップでホスト名の設定を変更したあと、次の項目を再設定します。

- エージェントの接続先（接続先をホスト名で指定している場合）

クラスタシステムの論理ホスト名を変更するには：

1. [\[2.7.2 現用系サーバでグループリソースを作成する手順\]](#) に記載されているリソースをオフラインにします。
2. 現用系サーバのセットアップの **「クラスタ環境」** 画面で論理ホスト名を変更後のホスト名に設定し、セットアップを実行します。
3. セットアップで出力された次のセットアップファイルを待機系サーバにコピーします。
Hitachi IT Operations Director のインストールフォルダ¥mgr¥conf¥jdn_manager_setup.conf
4. クラスタグループの所有者を待機系サーバに移動します。
5. 待機系サーバでセットアップを起動し、手順 4. でコピーしたセットアップファイルを指定して、セットアップを実行します。
6. クラスタグループの所有者を現用系サーバに移動します。
7. [\[2.7.2 現用系サーバでグループリソースを作成する手順\]](#) に記載されているリソースをオフラインにします。

クラスタシステムの論理ホスト名が変更されます。引き続き、次のとおり各項目を再設定します。

エージェントの接続先（接続先をホスト名で指定している場合）

1. エージェント設定の **「エージェント基本動作」** - **「基本設定」** - **「管理用サーバ」** に、変更後のホスト名を設定します。

ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

7.4.4 クラスタシステムの論理 IP アドレスを変更する手順

クラスタシステムの論理 IP アドレスを変更したい場合は、セットアップで IP アドレスの設定を変更したあと、次の項目を再設定します。

- エージェントの接続先（接続先を IP アドレスで指定している場合）
- ネットワークへの接続を許可しない機器の特例接続の設定

クラスタシステムの論理 IP アドレスを変更するには：

1. [\[2.7.2 現用系サーバでグループリソースを作成する手順\]](#) に記載されているリソースをオフラインにします。

2. 現用系サーバのセットアップの [クラスタ環境] 画面で論理 IP アドレスを変更後の IP アドレスに設定し、セットアップを実行します。
3. セットアップで出力された次のセットアップファイルを待機系サーバにコピーします。
Hitachi IT Operations Director のインストールフォルダ¥mgr¥conf¥jdn_manager_setup.conf
4. クラスタグループの所有者を待機系サーバに移動します。
5. 待機系サーバでセットアップを起動し、手順 4. でコピーしたセットアップファイルを指定して、セットアップを実行します。
6. クラスタグループの所有者を現用系サーバに移動します。
7. 「[2.7.2 現用系サーバでグループリソースを作成する手順](#)」に記載されているリソースをオフラインにします。

クラスタシステムの論理 IP アドレスが変更されます。引き続き、次のとおり各項目を再設定します。

エージェントの接続先（接続先を IP アドレスで指定している場合）

1. エージェント設定の [エージェント基本動作] – [基本設定] – [管理用サーバ] に、変更後の IP アドレスを設定します。
ただし、エージェント設定を変更したときに電源が入っていないコンピュータは、個別にエージェントのセットアップ画面から設定を変更する必要があります。

エージェントの接続先が変更されます。

ネットワークへの接続を許可しない機器の特例接続の設定

[ネットワーク制御の設定] 画面で、[ネットワークへの接続を許可しない機器の特例接続] から変更前の管理用サーバの IP アドレスを削除し、変更後の管理用サーバの IP アドレスを追加してください。

7.5 エージェントが接続する管理用サーバを切り替える手順

エージェントが接続する管理用サーバを切り替えるには：

1. 設定画面を表示します。
2. メニューエリアで [エージェント] - [エージェント設定とインストールセットの作成] を選択します。
3. インフォメーションエリアで、切り替えたいエージェント設定の [編集] ボタンをクリックします。
4. [エージェント設定の編集] ダイアログで [エージェント基本動作] - [基本設定] - [管理用サーバ] を切り替え先の管理用サーバのホスト名または IP アドレスに変更します。

エージェントが接続する管理用サーバが切り替わります。

注意事項

管理用サーバを切り替えた直後は、割り当てられるエージェント設定が不定となります。切り替え先の管理用サーバに切り替えたエージェントの機器情報が登録されたあと、必ずエージェント設定を割り当て直してください。

8

構築関連で使用するコマンド

ここでは、システムの構築、設定変更、リプレイスなどで使用する Hitachi IT Operations Director のコマンドについて説明します。

8.1 コマンドを実行する手順

Hitachi IT Operations Director のコマンドは、専用のコマンドプロンプト ([Director Utility Console]) および Windows のコマンドプロンプトから実行できます。

管理用サーバでコマンドを実行する場合は、[Director Utility Console] を利用すると便利です。[Director Utility Console] を利用すると、コマンドを入力する際にコマンドの実行ファイルの格納先を指定する必要がありません。[Director Utility Console] 起動時に、自動的にコマンドの実行ファイルの格納先がカレントフォルダになります。Windows のコマンドプロンプトからもコマンドを実行できます。

`getinv.vbs` コマンド以外のコマンドは、Administrator 権限を持つユーザーで実行してください。コマンドを実行する OS が Windows 8.1、Windows 8、Windows Server 2012、Windows 7、または Windows Server 2008 の場合で、ユーザーアカウント制御 (UAC) が有効なときは、[Director Utility Console] または Windows のコマンドプロンプトを起動する際に、右クリックして [管理者として実行] を選択してください。`getinv.vbs` コマンドは、`getinv.vbs` コマンドが格納されているフォルダに対するフルコントロールのアクセス権限を持つユーザーで実行してください。

エージェントでコマンドを実行する場合は、Windows のコマンドプロンプトを利用してください。

管理用サーバでコマンドを実行するには：

1. Windows の [スタート] メニューから [すべてのプログラム] - [Hitachi IT Operations] - [Director コマンド] を選択します。
2. 表示されるウィンドウで、実行したいコマンドを入力します。

コマンドが実行されます。

エージェントでコマンドを実行するには：

1. Windows のコマンドプロンプトを起動します。
2. 表示されるウィンドウで、実行したいコマンドを入力します。

コマンドが実行されます。

ポイント

Windows のタスクにコマンドを登録することで、Hitachi IT Operations Director のコマンドをスケジュール実行できます。

データベースのバックアップ、リストア、および再編成をコマンドで実行する場合、管理用サーバのサービスを停止する必要があります。そのため、これらのコマンドを Windows のタスクに登録する際は、Hitachi IT Operations Director を使用しない曜日、時間などにコマンドが実行されるよう考慮してください。

注意事項

コマンド実行中には、コマンド実行元の管理用サーバで、次の操作をしないでください。コマンド実行中にこれらの操作をすると、コマンドが強制終了され、タイミングによってはデータベースなどの重要なデータが破損したりエージェント制御サービスが停止したりするおそれがあります。また、コマンドの戻り値が正しく出力されません。

- [Ctrl] + [c] キーを押す
- [Director Utility Console] または Windows のコマンドプロンプトを終了する
- Windows からログアウトする
- Windows をシャットダウンする

コマンド実行中にこれらの操作をした場合は、ログファイルのメッセージを確認してください。また、コマンドが正常終了したメッセージが出力されていない場合は、必要に応じてコマンドを再実行してください。エージェント制御サービスが停止したメッセージが出力されている場合は、エージェント制御サービスを起動してください。

この注意事項は、次のコマンドには適用されません。

- stopservice
- startservice
- getlogs
- getinstlogs
- addfwlist.bat
- resetnid.vbs
- getinv.vbs

8.2 コマンドの説明形式

コマンドは、機能、形式、引数などの項目に分けて説明しています。コマンドの説明形式を次の表に示します。

項番	説明項目	内容
1	機能	コマンドの機能について説明しています。
2	形式	コマンドの入力形式について説明しています。
3	引数	コマンドの引数について説明しています。
4	格納先	コマンドの実行ファイルの格納先について説明しています。
5	注意事項	コマンドを実行する上での注意事項について説明しています。
6	戻り値	コマンドの戻り値について説明しています。
7	使用例	コマンドの使用例について説明しています。

8.3 updatesupportinfo (サポートサービスからの情報の登録)

サポートサービスサイトからダウンロードした情報を管理用サーバに登録するupdatesupportinfo コマンドについて説明します。

機能

管理用サーバがサポートサービスサイトに接続できない場合や、SAMAC 辞書の情報を更新したい場合は、最新情報を手動で管理用サーバに登録する必要があります。

まず、外部のネットワークに接続できるコンピュータでサポートサービスサイトに接続して、サポートサービスから最新情報をダウンロードしてください。ダウンロードした情報を管理用サーバに手動でコピーしてこのコマンドを実行すると、最新情報を管理用サーバに登録できます。

なお、このコマンドは管理用サーバで実行してください。

形式

```
updatesupportinfo -i △サポート情報ファイル名またはSAMACソフトウェア辞書のオフライン更新用ファイル名
```

引数

-i △サポート情報ファイル名または SAMAC ソフトウェア辞書のオフライン更新用ファイル名

管理用サーバに登録するサポート情報ファイルまたは SAMAC ソフトウェア辞書のオフライン更新用ファイルの、ファイル名を絶対パスで指定します。空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲んでください。

格納先

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥bin¥

Hitachi IT Operations Director が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、次のコマンドと同時に実行できません。
 - exportdb
 - importdb
 - ioassetsfieldutil export
 - ioassetsfieldutil import
 - ioutils exportasset
 - ioutils exportdevice

- ioutils exportdevicedetail
 - ioutils exportfield
 - ioutils exportfilter
 - ioutils exporttoplog
 - ioutils exportpolicy
 - ioutils exporttemplate
 - ioutils exportupdategroup
 - ioutils importasset
 - ioutils importfield
 - ioutils importfilter
 - ioutils importpolicy
 - ioutils importtemplate
 - ioutils importupdategroup
 - reorgdb
 - startservice
 - stopservice
- このコマンドは、管理用サーバでセットアップまたはデータベースマネージャが実行されている場合は実行できません。

戻り値

updatesupportinfo コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたファイルが不正、またはファイルがありません。
31	ほかのコマンドを実行中です。
51	コマンドの実行権限がありません。
53	管理用サーバのサービスが開始されていません。
54	管理用サーバがセットアップされていません。
101	一部またはすべてのサポート情報の更新に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

C:\temp に格納したサポート情報ファイル supportinfo.zip を管理用サーバに登録する場合の使用例を次に示します。

```
updatesupportinfo -i C:\temp\supportinfo.zip
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.4 exportdb (バックアップの取得)

管理用サーバが管理するデータのバックアップを取得するexportdb コマンドについて説明します。

機能

管理用サーバが管理するデータのバックアップを取得します。取得したバックアップは、トラブル発生時のデータの復元に利用できます。

このコマンドを実行すると、引数に指定したバックアップ先フォルダに YYYYMMDDhhmmss[※]のフォルダ名でバックアップ格納先フォルダが作成され、そのフォルダ内にバックアップファイルが作成されます。

注※ YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

なお、このコマンドは管理用サーバで実行してください。

形式

```
exportdb[△-f△バックアップ先フォルダ名][△-s]
```

引数

-f△バックアップ先フォルダ名

バックアップを取得するフォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。バックアップファイルの容量は運用内容や Hitachi IT Operations Director の利用期間によって異なります。バックアップ先フォルダのドライブは、データベースフォルダとデータフォルダのディスク占有量の合計値以上の空き容量を確保してください。

空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲ってください。フォルダ名は末尾の「¥」を除いて 135 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

Hitachi IT Operations Director のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。この引数を省略した場合は、次に示すフォルダがバックアップ先フォルダとなります。

- 引数を指定した場合

引数に指定したフォルダ¥YYYYMMDDhhmmss

- 引数を省略した場合

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥backup¥YYYYMMDDhhmmss

(例)

2011 年 1 月 1 日 2 時 30 分 00 秒にこのコマンドを実行した場合

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥backup¥20110101023000

管理用サーバのサービスの停止 (`stopservice` コマンド)、データのバックアップの取得 (`exportdb` コマンド)、および管理用サーバのサービスの開始 (`startservice` コマンド) を自動で実行する場合に指定します。

格納先

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥bin¥

Hitachi IT Operations Director が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了し、かつ管理用サーバが停止している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
 - `importdb`
 - `ioassetsfieldutil export`
 - `ioassetsfieldutil import`
 - `ioutils exportasset`
 - `ioutils exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils exporttoplog`
 - `ioutils exportpolicy`
 - `ioutils exporttemplate`
 - `ioutils exportupdategroup`
 - `ioutils importasset`
 - `ioutils importfield`
 - `ioutils importfilter`
 - `ioutils importpolicy`
 - `ioutils importtemplate`
 - `ioutils importupdategroup`

- reorgdb
 - startservice
 - stopservice
 - updatesupportinfo
- 引数「-s」は、クラスタ環境では指定できません。この引数を指定した場合、コマンドはエラーになります。

戻り値

exportdb コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	バックアップの取得に成功しましたが、管理用サーバの自動開始に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたフォルダが不正、またはフォルダがありません。
31	ほかのコマンドを実行中です。
32	同一時刻に作成されたバックアップ格納先フォルダがあります。
33	ディスク容量が不足しています。
34	データベースの開始に失敗しました。
35※	コマンド実行時に管理用サーバが開始処理中です。
36	コマンド実行時にデータベースが停止処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境で、引数「-s」が指定されています。
53	管理用サーバが停止していません。
54	管理用サーバがセットアップされていません。
55	デフォルトのバックアップ格納先フォルダが使用できません。
61	操作ログのバックアップ先フォルダに接続できません。
62	操作ログのバックアップ先フォルダにログインできません。
63	操作ログ関連のフォルダ容量が不足しています。
64	そのほかのエラーで操作ログのバックアップが中断しました。
101	バックアップの取得に失敗しました。
102	管理用サーバの自動停止に失敗しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。

戻り値	説明
150	そのほかのエラーでコマンドの実行が中断しました。

注※ 引数「-s」を指定した場合の戻り値です。

使用例

バックアップを C:¥tmp¥backup に取得し、管理用サーバのサービスの停止、データのバックアップの取得、および管理用サーバのサービスの開始を自動で実行する場合のコマンドの使用例を示します。

```
exportdb -f C:¥tmp¥backup -s
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.5 importdb (バックアップデータのリストア)

管理用サーバが管理するデータをバックアップ取得時の状態に復元（リストア）するimportdb コマンドについて説明します。

機能

ディスク障害などが発生した場合に、管理用サーバが管理するデータをバックアップ取得時の状態に復元します。データの復元には、exportdb コマンドで取得したバックアップファイルを使用します。

なお、このコマンドは管理用サーバで実行してください。

形式

```
importdb[△-f△データ格納フォルダ名][△-w△作業用フォルダ名][△-s]
```

引数

-f△データ格納フォルダ名

復元する時点のバックアップファイルが格納されているフォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。

空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」（ピリオド）、「@」、「¥」

Hitachi IT Operations Director のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。

この引数を指定した場合、および省略した場合に、コマンド実行時にデータの復元に使用されるデータ格納先フォルダを次に示します。

引数を指定した場合

引数で指定したフォルダをデータ格納先フォルダとして使用します。

引数を省略した場合

次のフォルダ下にあるフォルダのうち、フォルダ名から最新のデータ格納先フォルダを判断して使用します。

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥backup¥

例えば、「¥20110101023000」、「¥20110102023000」、および「¥20110103023000」のフォルダがある場合、「¥20110103023000」フォルダが復元に使用するデータ格納先フォルダになります。

-w△作業用フォルダ名

バックアップ取得時の状態に復元するときに使用する作業用フォルダを絶対パスで指定します。指定できるフォルダは、ローカルドライブのフォルダだけです。作業用フォルダのドライブには、1,000 台の機器を管理する場合は 1 ギガバイト以上の空き容量が必要です。

空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は、半角英数字、半角スペース、および次に示す半角記号です。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

Hitachi IT Operations Director のインストール先フォルダ名にこれらの文字以外の文字を使用している場合は、この引数を必ず指定してください。指定したフォルダがない場合はエラーとなります。

この引数を省略した場合は、次に示すフォルダが作業用フォルダとなります。

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥temp

-S

管理用サーバのサービスの停止 (stopservice コマンド)、バックアップからのリストア (importdb コマンド)、および管理用サーバのサービスの開始 (startservice コマンド) を自動で実行する場合に指定します。

格納先

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥bin¥

Hitachi IT Operations Director が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了し、かつ管理用サーバが停止している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
 - exportdb
 - ioassetsfieldutil export
 - ioassetsfieldutil import
 - ioutils exportasset
 - ioutils exportdevice
 - ioutils exportdevicedetail
 - ioutils exportfield
 - ioutils exportfilter
 - ioutils exporttoplog
 - ioutils exportpolicy
 - ioutils exporttemplate
 - ioutils exportupdategroup

- ioutils importasset
 - ioutils importfield
 - ioutils importfilter
 - ioutils importpolicy
 - ioutils importtemplate
 - ioutils importupdategroup
 - reorgdb
 - startservice
 - stopservice
 - updatesupportinfo
- 引数「-s」は、クラスタ環境では指定できません。この引数を指定した場合、コマンドはエラーになります。

戻り値

importdb コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	バックアップからのリストアに成功しましたが、管理用サーバの自動開始に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたデータ格納フォルダが不正、またはフォルダがありません。
13	指定されたデータ格納フォルダに、バックアップファイルがありません。
14	指定された作業用フォルダが不正、またはフォルダがありません。
15	ディスク容量が不足しています。
31	ほかのコマンドを実行中です。
34	データベースの開始に失敗しました。
35※	コマンド実行時に管理用サーバが開始処理中です。
36	コマンド実行時にデータベースが停止処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境で、引数「-s」が指定されています。
53	管理用サーバが停止していません。
54	管理用サーバがセットアップされていません。
55	デフォルトのデータ格納フォルダおよび作業用フォルダが使用できません。

戻り値	説明
56	古いバージョンのバックアップ情報です。
61	操作ログのバックアップ先フォルダに接続できません。
62	操作ログのバックアップ先フォルダにログインできません。
63	操作ログ関連のフォルダ容量が不足しています。
64	そのほかのエラーで操作ログのリストアが中断しました。
101	バックアップからのリストアに失敗しました。
102	管理用サーバの自動停止に失敗しました。
110	ライセンスに問題があるためコマンドの実行に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

注※ 引数「-s」を指定した場合の戻り値です。

使用例

2011 年 1 月 3 日 2 時 30 分 00 秒にバックアップを取得した時点のデータ（バックアップ格納先フォルダ：C:¥tmp¥backup¥20110103023000）を使用し、管理用サーバのサービスの停止、バックアップからのリストア、および管理用サーバのサービスの開始を自動で実行する場合のコマンドの使用例を示します。

```
importdb -f C:¥tmp¥backup¥20110103023000 -s
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.6 stopservice (サービス停止)

機能

管理用サーバの関連サービスを停止して、管理用サーバを停止状態にします。

なお、このコマンドは管理用サーバで実行してください。

形式

```
stopservice
```

引数

引数はありません。

格納先

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥bin¥

Hitachi IT Operations Director が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- このコマンドは、管理用サーバのセットアップが完了している状態で実行してください。
- このコマンドは、同時に複数実行できません。
- このコマンドは、次のコマンドと同時に実行できません。
 - exportdb
 - importdb
 - ioassetsfieldutil export
 - ioassetsfieldutil import
 - ioutils exportasset
 - ioutils exportdevice
 - ioutils exportdevicedetail
 - ioutils exportfield
 - ioutils exportfilter
 - ioutils exporttoplog
 - ioutils exportpolicy
 - ioutils exporttemplate
 - ioutils exportupdategroup

- ioutils importasset
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- updatesupportinfo

戻り値

stopservice コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	管理用サーバがすでに停止しています。
11	コマンドの引数の指定形式に誤りがあります。
31	ほかのコマンドを実行中です。
35	コマンド実行時に管理用サーバが開始処理中です。
51	コマンドの実行権限がありません。
52	クラスタ環境ではこのコマンドを実行できません。
54	管理用サーバがセットアップされていません。
101	管理用サーバのサービスの停止に失敗しました。
150	そのほかのエラーでコマンドの実行が中断しました。

使用例

管理用サーバのサービスを停止するコマンドの使用例を次に示します。

```
stopservice
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.7 getlogs (トラブルシューティング情報の取得)

機能

原因不明なトラブルや、解決が困難なトラブルなどが発生した場合に、サポートサービスに問い合わせるときに必要なトラブルシューティング情報を一括で取得します。

取得できるトラブルシューティング情報は、一次用ファイル (tsinf_1st.dat) と二次用ファイル (tsinf_2nd.dat) の 2 つのファイルに分けて出力されます。

なお、このコマンドは管理用サーバで実行してください。

形式

```
getlogs[△-f△トラブルシューティング情報格納先フォルダ名]
```

引数

-f△トラブルシューティング情報格納先フォルダ名

トラブルシューティング情報格納先フォルダを絶対パスで指定します。なお、指定できるフォルダは、ローカルドライブのフォルダだけです。

空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲ってください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は Windows でフォルダ名に使用できる文字です。

この引数を省略した場合、トラブルシューティング情報ファイルは次に示すフォルダに格納されます。

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥troubleshoot

なお、トラブルシューティング情報の取得時に、トラブルシューティング情報格納先フォルダに一時フォルダとして tsinf フォルダが作成され、コマンド終了時に削除されます。

格納先

Hitachi IT Operations Director のインストール先フォルダ¥mgr¥bin¥

Hitachi IT Operations Director が提供するコマンドプロンプトを使用すると、実行ファイルの格納先を指定しないでコマンドを実行できます。

注意事項

- トラブルシューティング情報格納先フォルダに次に示すフォルダまたはファイルがすでに存在した場合、これらのフォルダまたはファイルが削除されてから、コマンドが実行されます。
 - tsinf フォルダ
 - tsinf_1st.dat
 - tsinf_2nd.dat

- `getlogs` コマンドでは、一時フォルダとしてユーザー環境変数 `TEMP` に設定したフォルダを使用します。`getlogs` コマンドでメッセージ (KDEX4041-E) が出力される場合は、このフォルダの空き容量が十分かどうかを確認してください。

戻り値

`getlogs` コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	一部のトラブルシューティング情報の取得に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。
12	指定されたフォルダが不正、またはフォルダがありません。
51	コマンドの実行権限がありません。
101	そのほかのエラーでコマンドの実行が中断しました。

使用例

トラブルシューティング情報を `C:\tmp\troubleshoot` に取得する場合のコマンドの使用例を次に示します。

```
getlogs -f C:\tmp\troubleshoot
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.8 getinstlogs（インストール時のトラブルシューティング情報の取得）

Hitachi IT Operations Director をインストールしたときの、トラブルシューティング情報を取得するための getinstlogs コマンドについて説明します。

機能

管理者が Hitachi IT Operations Director をインストールした際に、原因不明なトラブルや、解決が困難なトラブルなどが発生した場合に、サポートサービスに問い合わせるときに必要なトラブルシューティング情報を一括で取得します。

なお、このコマンドは管理用サーバで実行してください。

形式

```
getinstlogs[△-f△トラブルシューティング情報格納先フォルダ名]
```

引数

-f△トラブルシューティング情報格納先フォルダ名

トラブルシューティング情報格納先フォルダを絶対パスで指定します。ネットワークドライブも指定できます。

空白を含むパスを指定する場合は、パスをダブルクォーテーション (") で囲んでください。フォルダ名は末尾の「¥」を除いて 150 バイト以内で指定してください。また、使用できる文字は Windows でフォルダ名に使用できる文字です。

この引数を省略した場合、トラブルシューティング情報ファイルはデスクトップに格納されます。

格納先

Hitachi IT Operations Director の提供媒体のルート¥_PPDIR¥P0642855¥DISK1¥

注意事項

- トラブルシューティング情報格納先フォルダに JDNINST フォルダまたはファイルがすでに存在した場合、このフォルダまたはファイルが削除されてから、コマンドが実行されます。
- トラブルシューティング情報格納先フォルダを指定する場合、すでに存在するフォルダを指定してください。

戻り値

getinstlogs コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
1	一部のトラブルシューティング情報の取得に失敗しました。
11	コマンドの引数の指定形式に誤りがあります。

戻り値	説明
12	指定されたフォルダにアクセスできない、またはフォルダがありません。
13	指定されたデータ格納フォルダに、バックアップファイルを書き込めません。
51	コマンドの実行権限がありません。
101	そのほかのエラーでコマンドの実行が中断しました。

使用例

インストール時のトラブルシューティング情報を C:¥tmp¥troubleshoot¥install に取得する場合のコマンドの使用例を次に示します。

```
getinstlogs -f C:¥tmp¥troubleshoot¥install
```

関連リンク

- [8.1 コマンドを実行する手順](#)

8.9 resetnid.vbs（ホスト識別子のリセット）

エージェントによって生成された、機器を識別するためのユニークな ID（ホスト識別子）をリセットするための `resetnid.vbs` コマンドについて説明します。

機能

エージェントを導入すると、自動的にホスト識別子が生成されます。

ディスクコピーによってエージェントを導入する場合、コピー先のコンピュータのホスト識別子が新規に生成されるよう、あらかじめコピー元のコンピュータでホスト識別子をリセットしておく必要があります。コピー元のコンピュータで `resetnid.vbs` コマンドを実行することで、エージェントのホスト識別子がリセットされます。これによって、ディスクコピーを利用してエージェントを導入したときに、新規にホスト識別子が生成され、コンピュータがユニークに識別されるようになります。

ポイント

`resetnid.vbs` コマンドを実行しないままディスクコピーしてエージェントを導入した場合、ディスクコピー先のコンピュータが、ディスクコピー元のコンピュータと同一の機器として識別されます。複数のコンピュータが同一の機器として識別されてしまったときは、それらのコンピュータ上で `resetnid.vbs` コマンドを実行したあとに、設定画面の「機器の探索」－「管理対象機器」でコンピュータの機器情報をいったん削除してください。

一度 Hitachi IT Operations Director に識別されたコンピュータで `resetnid.vbs` コマンドを実行すると、コマンドの実行前と実行後のホスト識別子が Hitachi IT Operations Director に両方登録されます。そのため、1 台のコンピュータに対して 2 つの機器情報が表示されますが、設定画面の「機器の探索」－「管理対象機器」で 2 つの機器情報をいったん削除すれば、新しい機器情報だけが表示されるようになります。

注意事項

ネットワークモニタを導入している機器では `resetnid.vbs` コマンドを実行しないでください。

`resetnid.vbs` コマンドを実行すると、1 台のコンピュータに対して 2 つの機器情報が表示されますが、ネットワークモニタを導入している機器でこれを解消するためには、一度ネットワークモニタを無効にしたあとで、設定画面の「機器の探索」－「管理対象機器」で 2 つの機器情報をいったん削除する必要があります。

なお、このコマンドは、エージェント導入済みのコンピュータ上で実行してください。

また、リターンコードを表示させるには、後述の使用例のように Windows の `start` コマンドで `/wait` オプションを指定し、`Cscript.exe` を実行してください。

形式

```
resetnid.vbs△/nodeid [△/i]
```

引数

/nodeid

この引数は必ず指定してください。引数を省略した場合、コマンドは実行されません。

/i

利用者のコンピュータに、コマンドを実行するかどうかを選択させるダイアログと、実行結果を示すダイアログを表示します。

格納先

エージェントのインストール先フォルダ¥bin¥

注意事項

resetnid.vbs コマンドを実行してから新規のホスト識別子が生成されるまでには、エージェント設定の [エージェント基本動作] - [基本設定] に設定した次の項目のうち、最も短い間隔だけ時間が掛かります。

- [監視間隔 (セキュリティ項目) (分)]
- [監視間隔 (セキュリティ項目以外) (分)]
- [管理用サーバからの情報取得の間隔 (分)]

戻り値

resetnid.vbs コマンドの戻り値を次の表に示します。

戻り値	説明
0	コマンドが正常に終了しました。
10001	利用者のコンピュータで、コマンドの実行がキャンセルされました。
10011	コマンドの引数の指定形式に誤りがあります。
10051	コマンドの実行権限がありません。
10101	ホスト識別子のリセットに失敗しました。
10150	ホスト識別子のリセットに失敗しました。

使用例

エージェントのインストール先フォルダが「C:¥Program Files¥Hitachi¥Director Agent」の場合の、ホスト識別子をリセットするコマンドの使用例を次に示します。

```
cd "C:¥Program Files¥Hitachi¥Director Agent¥bin"
```

```
start /wait Cscript.exe resetnid.vbs /nodeid
```

```
echo %errorlevel%
```

関連リンク

- [8.1 コマンドを実行する手順](#)

9

トラブルシューティング

ここでは、Hitachi IT Operations Director の構築時にトラブルが発生した場合の対処方法について説明します。

9.1 構築時のトラブルシューティングの流れ

サーバおよびエージェントの環境を構築しているときにトラブルが発生した場合は、次の手順で対処してください。

1. エラーメッセージを確認する

ログファイルに出力されたエラーメッセージの内容を確認してください。

ポイント

エラーを通知するダイアログから、エラーメッセージの内容を確認することもできます。

2. トラブルの要因および対処方法を確認して、エラーを対処する

ログファイルに出力されたメッセージから、トラブルの要因およびエラーの対処方法を確認して、エラーを対処します。

発生したトラブルに対処できます。

メッセージの出力形式

出力されるメッセージの形式を次に示します。

- KDEXnnnn-Z メッセージテキスト
- KFPHnnnnn-Z メッセージテキスト

メッセージ ID は、次の内容を示しています。

K

システム識別子を示します。

DEX

Hitachi IT Operations Director のメッセージ（データベース以外）であることを示します。

FPH

Hitachi IT Operations Director のデータベースに関するメッセージであることを示します。

nnnn

メッセージの通し番号を示します。Hitachi IT Operations Director のデータベースに関するメッセージの通し番号は 5 けたです。

Z

メッセージの種類を示します。

- E：エラーメッセージを示します。
- W：警告メッセージを示します。
- I：通知メッセージを示します。

- Q：ユーザーが応答する必要のあるメッセージを示します。

関連リンク

- [9.2 最小構成システムの構築時のトラブルシューティング](#)
- [9.2.1 管理用サーバ構築時のトラブルシューティング](#)
- [9.2.2 エージェントインストール時のトラブルシューティング](#)
- [9.4 エージェントレス構成システムの構築時のトラブルシューティング](#)
- [9.5 サポートサービス連携構成システムの構築時のトラブルシューティング](#)
- [9.6 Active Directory 連携構成システムの構築時のトラブルシューティング](#)
- [9.7 MDM 連携構成システムの構築時のトラブルシューティング](#)
- [9.8 ネットワーク監視構成システムの構築時のトラブルシューティング](#)
- [9.9 クラスタシステムの構築時のトラブルシューティング](#)

9.2 最小構成システムの構築時のトラブルシューティング

機器を探索しても発見できない

ネットワークに接続した機器を探索しても発見できない場合は、設定画面の「機器の探索」－「探索条件の設定」画面で、探索範囲や認証情報の設定内容が正しいか確認してください。

管理対象の機器と管理用サーバ間で通信できない

提供媒体を使用して管理対象の機器にエージェントを導入した場合、エージェントのセットアップ情報は自動で設定されません。セットアップ情報が設定されていることを確認してください。設定されている場合は、次に示す内容を確認してください。

- 管理対象の機器に導入されているエージェントのセットアップ情報で、接続先の管理用サーバの名称およびポート番号の設定が正しいか。
- 管理用サーバのセットアップ情報で、ポート番号の設定が正しいか。

9.2.1 管理用サーバ構築時のトラブルシューティング

管理用サーバに Hitachi IT Operations Director をインストールできない場合は、次に示す内容を確認してください。

- Hitachi IT Operations Director に対応している OS かどうか。
- Administrator 権限を持つアカウントで Windows にログオンしたかどうか。

必要に応じて、インストール時のトラブルシュート用情報を `getinstlogs` コマンドで取得できます。

`getinstlogs` コマンドについては、「[8.8 getinstlogs \(インストール時のトラブルシュート用情報の取得\)](#)」を参照してください。

取得できるログの種類

ログの種類	出力先	ファイル名	説明
インストーラートレースログファイル	• 正常に Hitachi IT Operations Director がインストールされた場合 <i>Hitachi IT Operations Director</i> のインストール先フォルダ¥log • 正常に Hitachi IT Operations Director がインストールされなかった場合 %WINDIR%¥Temp ¥JDNINST	JDNINS01.log	インストーラのトレースログファイルです。Hitachi IT Operations Director をインストールするときに出力されます。

9.2.2 エージェントインストール時のトラブルシューティング

コンピュータにエージェントをインストールできない場合、次に示す内容を確認してください。

- エージェントを導入するコンピュータの前提となる OS かどうか。
- Administrator 権限を持つアカウントで Windows にログオンしたかどうか。
- すでにインストールされているエージェントより古いバージョンのエージェントをインストールしようとしていないか。

また、必要に応じてエージェントのトラブルシューティング用情報を採取してください。

エージェントのトラブルシューティング用情報を採取するには：

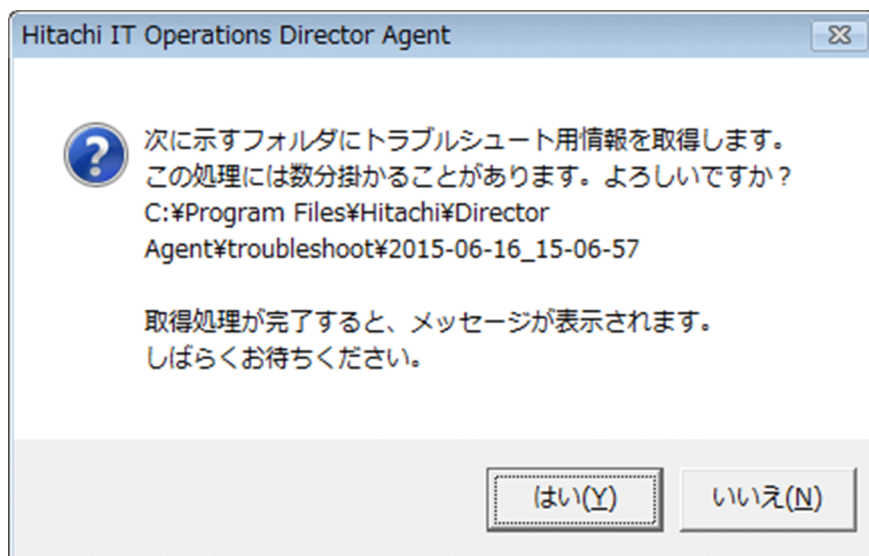
トラブルシューティング用情報の採取は、トラブルが発生したコンピュータで実行してください。なお、Administrator 権限を持つユーザーで実行してください。

1. getlogs.vbs をダブルクリックする

getlogs.vbs の格納場所を次に示します。

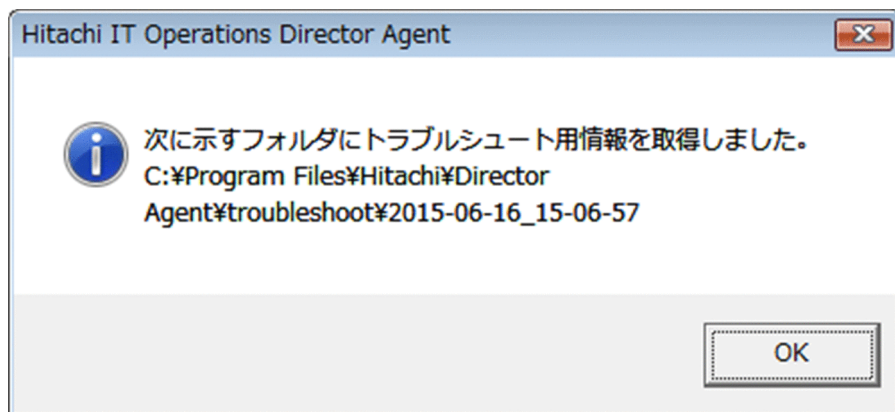
Hitachi IT Operations Director Agent のインストール先フォルダ¥bin

トラブルシューティング用情報の取得を確認するダイアログが表示されます。



2. [はい] ボタンをクリックする

トラブルシューティング用情報の採取が開始されます。トラブルシューティング用情報の採取が終了すると、トラブルシューティング用情報の採取が終了したことを示すダイアログが表示されます。



採取したトラブルシューティング情報は、次に示す場所に格納されます。

Hitachi IT Operations Director Agent のインストールフォルダ¥troubleshoot¥YYYY-MM-DD_hh-mm-ss※

注※ YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

3. [OK] ボタンをクリックする

トラブルシューティング情報の採取が終了したことを示すダイアログが閉じます。

上記の方法で採取できるトラブルシューティング情報を次の表に示します。

トラブルシューティング情報	採取内容
エージェントのログ	<i>Hitachi IT Operations Director Agent</i> のインストール先フォルダ¥log
システム情報	- システム情報 msinfo32/nfo の結果 - 環境変数 SET コマンドの結果 - レジストリ情報 - HKEY_LOCAL_MACHINE¥SOFTWARE¥Hitachi 以下のレジストリ - HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows ¥RemovableStorageDevices 以下のレジストリ - デバイス情報 デバイスのプロパティ、状態 - ファイル情報 <i>Hitachi IT Operations Director Agent</i> のインストール先フォルダ以下のサブフォルダおよびファイルの一覧 - イベントログ アプリケーション、システム、セキュリティ

9.2.3 1 台のコンピュータに対して 2 つの機器情報が表示される場合のトラブルシューティング

1 台のコンピュータに対して 2 つのホスト識別子が登録されていると、Hitachi IT Operations Director の操作画面では、1 台のコンピュータに対して 2 つの機器情報があるように表示されます。

この場合、設定画面の「機器の探索」－「管理対象機器」で 2 つの機器情報をいったん削除すれば、新しい機器情報だけが表示されるようになります。

9.3 オフライン管理構成システムの構築時のトラブルシューティング

次に示す場合は、管理形態を切り替えてください。管理形態を切り替える手順については、「[9.3.1 オフライン管理からオンライン管理に切り替える手順](#)」または「[9.3.2 オンライン管理からオフライン管理に切り替える手順](#)」を参照してください。

- オフライン管理したいコンピュータに対して、誤ってオンライン管理用のエージェントをインストールした場合
- オンライン管理したいコンピュータに対して、誤ってオフライン管理用のエージェントをインストールした場合

誤ったエージェントをインストールしたかどうかを判断するには、エージェントのセットアップ内容を確認してください。

また、ネットワークモニタを有効化するコンピュータに対して、誤ったエージェント設定を割り当てた場合は、設定の内容に応じて次の手順で対処してください。

【管理用サーバと接続する】のチェックを外したエージェント設定を割り当てた場合に対処するには：

1. 管理形態をオフライン管理からオンライン管理に切り替えます。
2. ネットワークモニタのサービスを、手動で開始します。

【コンピュータから収集した情報を、定期的に管理用サーバに通知する】のチェックを外したエージェント設定を割り当てた場合に対処するには：

1. エージェント設定の【エージェント基本動作】で、【コンピュータから収集した情報を、定期的に管理用サーバに通知する】をチェックします。

9.3.1 オフライン管理からオンライン管理に切り替える手順

利用者のコンピュータをオフライン管理からオンライン管理に切り替える場合は、エージェント設定を変更してから、利用者のコンピュータでセットアップを実行する必要があります。オンライン管理に切り替える手順を次に示します。

オンライン管理に切り替えるには（エージェント設定の変更）：

1. エージェント設定の【エージェント基本動作】で、【管理用サーバと接続する】をチェックして【OK】ボタンをクリックします。

エージェント設定の変更が完了したら、利用者のコンピュータでのセットアップを実行します。

オンライン管理に切り替えるには（利用者のコンピュータでのセットアップ）：

1. エージェントをインストールしているコンピュータにログインします。

2. Windows の [スタート] メニューから [すべてのプログラム] – [Hitachi IT Operations Director Agent] – [管理者ツール] – [セットアップ] を選択します。
3. [セットアップ] ダイアログで、[管理用サーバと接続する] をチェックして [OK] ボタンをクリックします。
4. 表示される確認ダイアログで [はい] ボタンをクリックします。

設定が完了し、対象のコンピュータはオンライン管理となります。

9.3.2 オンライン管理からオフライン管理に切り替える手順

利用者のコンピュータをオンライン管理からオフライン管理に切り替える場合は、エージェント設定を変更します。オフライン管理に切り替える手順を次に示します。

注意事項

オフライン管理に切り替える場合、再度オンライン管理に切り替える際の作業を考慮しておく必要があります。ネットワークに接続されていないコンピュータをオフライン管理からオンライン管理に切り替える場合は、切り替え対象となるすべてのコンピュータの、エージェントのセットアップでも変更が必要です。

オフライン管理に切り替えるには（エージェント設定の変更）：

注意事項

対象のコンピュータに操作ログの取得を有効にしたセキュリティポリシーを割り当てている場合は、操作ログの取得を無効にしたセキュリティポリシーを割り当てたあとで、オンライン管理に切り替えてください。操作ログの取得を有効にしたセキュリティポリシーを割り当てたままにした場合、利用者のコンピュータに操作ログのファイルが取得され続けます。

1. エージェント設定の [エージェント基本動作] で、[管理用サーバと接続する] のチェックを外して [OK] ボタンをクリックします。
2. 表示されるダイアログで、[OK] ボタンをクリックします。

設定が完了し、対象のコンピュータはオフライン管理となります。

9.4 エージェントレス構成システムの構築時のトラブルシューティング

エージェントレスのコンピュータを認証できない場合は、次に示す内容を確認してください。

管理用サーバの確認

- SNMP を利用して機器に接続するためのコミュニティ名が正しいか。
- Windows の管理共有のユーザー ID やパスワードが正しいか。

コンピュータの確認

- SNMP エージェントのサービスが正しく動作しているか。
- エージェントレスでの管理に必要な条件が満たされているか。

9.5 サポートサービス連携構成システムの構築時のトラブルシューティング

更新プログラム情報やウィルス対策製品情報を取得する際に、サポートサービスサイトに接続できない場合は、設定画面の〔他システムとの接続〕－〔サポートサービスの設定〕画面で設定した URL、ダウンロードご利用 ID、パスワードなどが正しいか確認してください。設定内容を変更した場合、〔接続テスト〕ボタンをクリックして、接続できるかどうか確認してください。

9.6 Active Directory 連携構成システムの構築時のトラブルシューティング

Active Directory に接続できない場合は、設定画面の [他システムとの接続] – [Active Directory の設定] 画面で設定した内容が正しいか確認してください。

9.7 MDM 連携構成システムの構築時のトラブルシューティング

MDM 連携構成システムの構築時に、トラブルが発生した場合の対処方法について説明します。

スマートデバイスの情報が取得されない

接続先の MDM システムで認証できていない場合、スマートデバイスの情報は取得できません。

対処方法

イベント番号「1118」のイベント、またはメッセージ ID「KDEX5427-E」のメッセージが出力されていないか確認してください。出力されていた場合は、設定画面の「MDM 連携の設定」画面で設定したパスワードが誤っているおそれがあります。正しいパスワードを設定してください。

9.8 ネットワーク監視構成システムの構築時のトラブルシューティング

ネットワークモニタを有効にした場合に、ネットワークセグメント内に設置されているすべての機器がネットワーク接続できなくなったときは、ルータなどのネットワーク機器のネットワーク接続が許可されているか確認してください。許可されていない場合は、ルータなどのネットワーク機器のネットワーク接続を許可するように設定してください。

9.9 クラスタシステムの構築時のトラブルシューティング

稼働中の管理用サーバにトラブルが発生した場合に、バックアップ用のサーバへ自動的に運用が切り替わらない場合、セットアップで設定した内容を確認してください。

【クラスタ環境】 画面での設定内容の確認

- [クラスタ構成で Hitachi IT Operations Director を運用する] がチェックされているか。
- 一方の管理用サーバで [現用系] が、もう一方の管理用サーバで [待機系] が選択されているか。
- 指定されている論理ホスト名、論理 IP アドレスは正しいか。

【フォルダの設定】 画面での設定内容の確認

- 共有ディスクのフォルダが指定されているか。
- 指定されているフォルダのパスが正しいか。

付録

付録 A 参考情報

ここでは、Hitachi IT Operations Director を使用する上での参考情報について説明します。

付録 A.1 ポート番号一覧

Hitachi IT Operations Director で使用するポート番号について説明します。

Hitachi IT Operations Director のポート番号一覧

管理用サーバ

管理用サーバの ポート番号	接続方向	接続対象 [ポート 番号]	プロトコル	用途
31080	←	管理者のコン ピュータ [ephemeral]	TCP	操作画面の参照または操作時に、管理者のコン ピュータから管理用サーバへの通信に使用されま す。
31000	←	エージェント [ephemeral]	TCP	エージェントから管理用サーバへの通信に使用さ れます。
31006～31009、 31011、31012	なし	なし	TCP	管理サーバ上で行われる内部処理の通信に使用さ れます。
ephemeral	→	エージェント [16992]	TCP	AMT を使用したコンピュータの電源制御に使用 されます。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、セットアップで、重複しないポート番号に変更してください。

管理用サーバで、Windows ファイアウォールによってポート番号を制御している場合は、これらのポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境に Hitachi IT Operations Director をインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

コントローラおよびリモコンエージェントのポート番号一覧

コントローラまたはリ モコンエージェント [ポート番号]	接続方向	接続対象 [ポート番 号]	プロトコル	用途
リモコンエージェント [31016]	←	コントローラ [ephemeral]	TCP	コントローラからリモコンエージェントへの 画面操作に使用されます。
リモコンエージェント [31017]	←	コントローラ [ephemeral]	TCP	コントローラからリモコンエージェントへの ファイル転送に使用されます。

コントローラまたはリモコンエージェント [ポート番号]	接続方向	接続対象 [ポート番号]	プロトコル	用途
リモコンエージェントまたはコントローラ [31018] (チャットサーバとして使用している場合)	↔	リモコンエージェントまたはコントローラ [ephemeral]	TCP	チャットに使用されます。
リモコンエージェント [ephemeral]	➡	コントローラ [31019]	TCP	リモコンエージェントからコントローラへのリモート接続の要求に使用されます。
リモコンエージェント [ephemeral]	➡	コントローラ [31020]	TCP	リモコンエージェントからコントローラへのコールバックによるファイル転送に使用されます。

コントローラをインストールしたコンピュータおよびリモートコントロールの対象のコンピュータで、Windows ファイアウォールによってポート番号を制御している場合は、これらのポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境にコントローラおよびリモコンエージェントをインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます (例外設定に登録されます)。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、次のようにして重複しないポート番号に変更してください。

- コントローラのポート番号
コントローラの [環境の設定] ダイアログで設定する。
- リモコンエージェントのポート番号
エージェント設定の [リモートコントロールの動作設定] で設定する。
- チャット機能のポート番号
[チャット] ウィンドウの [環境の設定] ダイアログの [接続] タブで設定する。

Hitachi IT Operations Director Agent のポート番号一覧

エージェントの ポート番号	接続方向	接続対象 [ポート番号]	プロトコル	用途
31001	←	管理用サーバ [ephemeral]	TCP	管理用サーバからエージェントへの通信に使用されます。
16992	←	管理用サーバ [ephemeral]	TCP	AMT を使用したコンピュータの電源制御に使用されます。

各ポート番号は、製品の提供時にデフォルトとして設定されています。ご利用のシステム環境で、表に示すポート番号をすでに使用している場合は、管理用サーバのセットアップで重複しないポート番号に変更してください。

エージェント導入済みのコンピュータで、Windows ファイアウォールによってポート番号を制御している場合は、ポートを通過できるように設定してください。なお、Windows ファイアウォールが有効になっている環境にエージェントをインストールすると、自動的に Windows ファイアウォールを通過できるように設定されます（例外設定に登録されます）。

また、Hitachi IT Operations Director と Hitachi IT Operations Director Agent の間のネットワークで、ファイアウォールによってポートを制御している場合は、表に示すポートを通過できるように設定してください。

エージェントレスの機器のポート番号

エージェントレスの機器の場合、機器の認証状態によって、Windows の管理共有または SNMP のポート番号が使用されます。

付録 A.2 エージェントの環境を変更した場合の認識方法

エージェントを導入したコンピュータは、機器を識別するためのユニークな ID（ホスト識別子）が生成されます。

コンピュータの環境を変更した場合、変更方法によってホスト識別子が再生成されるかどうか異なります。ホスト識別子が再生成されると、環境を変更する前の機器とは異なる機器として認識されます。

ホスト識別子は、次のような場合に再生成されます。

- OS を再インストールした場合
- OS がインストールされたハードディスクを交換した場合
- マザーボードを交換した場合※
- ディスクコピーを利用して、ほかのコンピュータにエージェントを導入した場合※

注※ すでにホスト識別子が再生成されていた場合は、環境を変更する前の機器と同じ機器として認識されます。

上記以外の場合は、ホスト識別子は再生成されません。例えば、次のような場合は、ホスト識別子は再生成されません。

- エージェントをアンインストールした場合
- エージェントをアンインストールしたあとに、エージェントを再インストールした場合
- エージェントを上書きインストールした場合
- CPU、メモリ、またはネットワークカードを交換した場合
- OS をアップグレードした場合
- ハードディスクを増設した場合

ポイント

異なる機器として認識された場合は、環境を変更する前の機器情報やハードウェア資産情報が管理用サーバに残った状態になります。必要に応じて情報を削除してください。

付録 A.3 各バージョンの変更内容

04-00 の変更内容 (3021-3-291、3021-3-292、3021-3-293)

- ・ マニュアル体系を次のとおり変更した。

03-00 のマニュアル

- ・ 基本の流れで運用開始 Hitachi IT Operations Director スターターガイド (3020-3-T93)
- ・ したいことからすばやく探せる Hitachi IT Operations Director クイックリファレンス (3020-3-T94)

04-00 のマニュアル

- ・ Hitachi IT Operations Director 導入・設計ガイド (3021-3-291)
- ・ Hitachi IT Operations Director 構築ガイド (3021-3-292)
- ・ Hitachi IT Operations Director 運用ガイド (3021-3-293)
- ・ Hitachi IT Operations Director および Hitachi IT Operations Director Agent の適用 OS に、Windows 8 および Windows Server 2012 を追加した。
- ・ 同じ管理ソフトウェアに対応するソフトウェアが 1 台のコンピュータに複数インストールされている場合、1 ライセンスの消費としてカウントするようにした。
- ・ Hitachi IT Operations Director のインストール時に、エージェントおよびネットワークモニターエージェントをコンポーネントとして登録できるようにした。
- ・ オフライン管理機能によって、管理用サーバにネットワーク接続していないコンピュータも管理できるようにした。
- ・ ユーザーアカウントに設定した管轄範囲や業務分掌に合わせて、表示される情報や実行できる操作を制限できるようにした。
- ・ MDM システムと連携してスマートデバイスを管理できるようにした。
- ・ Windows Vista 以降で、USB デバイスとリムーバブルディスクの操作抑止を同時に有効化できるようにした。
- ・ Windows Vista 以降で、FD ドライブおよびリムーバブルディスクも書き込みだけを抑止できるようにした。
- ・ 資産管理時に、ソフトウェア種別と、一部のソフトウェアの購入形態およびプロダクト ID を管理できるようにした。また、ソフトウェア種別を管理するために、SAMAC ソフトウェア辞書のオフライン更

新用ファイルを含むサポートサービスの情報を取得して、Hitachi IT Operations Director の情報を更新できるようにした。

- 操作ログを取得できる Web ブラウザに Windows Internet Explorer 10 を追加した。
- 無線 LAN に接続したネットワーク接続機器を制御できるようにした。
- サポートするウィルス対策製品に次の製品を追加した。
 - Norton AntiVirus (32bit、64bit)
 - ウイルスバスター クラウド (32bit、64bit)
 - ウイルスバスター ビジネスセキュリティ 7.0 (32bit、64bit)
 - Kaspersky Endpoint Security 8 for Windows 8.1 (32bit、64bit)
 - ESET NOD32 Antivirus 5.2 (32bit、64bit)
 - F-Secure Client Security 9.31 (32bit、64bit)
 - F-Secure Client Security 9.32 (32bit、64bit)
- サポートするウィルス対策製品から次の製品を削除した。
 - ウイルスバスター 2010 (32bit、64bit)
 - F-Secure Client Security 8.0 (32bit、64bit)
- 機器情報の取得時に、プリンタのホスト名を IP アドレスから取得するようにした。
- 機器画面の [ソフトウェア情報] 画面から、ソフトウェアを管理ソフトウェアに追加できるようにした。
- [エージェント設定の追加] ダイアログおよび [エージェント設定の編集] ダイアログで、コンピュータの再起動のタイミングを設定できるようにした。
- 次のダイアログで、操作対象のコンピュータが稼働していない場合に起動させるよう設定できるようにした。
 - [利用者へのメッセージ通知] ダイアログ
 - [最新情報の取得] ダイアログ
 - [セキュリティ対策の実施] ダイアログ
- 部署および設置場所の定義の仕組みを記載した。また、メニューエリアから部署および設置場所の名称を変更できるようにした。
- インフォメーションエリアに「-」が表示されている場合、エクスポートすると空の値が出力されることを記載した。
- ioutils exportdevice コマンドを使用して、機器情報をエクスポートできるようにした。
- ioutils exportdevicedetail コマンドを使用して、詳細な機器情報をエクスポートできるようにした。
- 簡易フィルタを適用および解除する方法を変更した。
- 操作画面の一覧をページごとに表示できるようにした。

索引

記号

「ライセンス認証をしましょう」ウィザード 19

数字

1 台のコンピュータに対して 2 つの機器情報が表示される場合のトラブルシューティング 168

A

Active Directory に登録されている機器の探索手順 96

Active Directory の接続設定手順 95

Active Directory の探索条件の設定手順 97

Active Directory 連携構成システムの構築 54

Active Directory 連携構成システムの構築時の設定 95

Active Directory 連携構成システムの構築時のトラブルシューティング 173

Active Directory 連携構成システムを構築する流れ 54

E

exportdb コマンド 145

G

getinstlogs コマンド 157

getlogs コマンド 155

H

Hitachi IT Operations Director のアンインストール手順 118

Hitachi IT Operations Director のアンインストール手順〔クラスタシステム〕 124

Hitachi IT Operations Director のインストールタイプ 15

Hitachi IT Operations Director のインストール手順 15

Hitachi IT Operations Director の上書きインストール手順 105

Hitachi IT Operations Director のシステム全体をバージョンアップする流れ 108

Hitachi IT Operations Director のセットアップ〔クラスタシステム（現用系サーバ）〕 64

Hitachi IT Operations Director のセットアップ〔クラスタシステム（待機系サーバ）〕 67

I

importdb コマンド 149

IP アドレスの変更手順〔管理用サーバ〕 134

IP アドレスの変更〔システム構成要素〕 134

M

MDM システムと連携するための情報を設定する手順 99

MDM 連携構成システムの構築 55

MDM 連携構成システムの構築時の設定 99

MDM 連携構成システムの構築時のトラブルシューティング 174

MDM 連携構成システムを構築する流れ 55

R

resetnid.vbs コマンド 159

S

SNMP の認証情報 88

stopservice コマンド 153

U

updatesupportinfo コマンド 142

W

Windows の管理共有の認証情報 88

あ

アップデート〔コンポーネント〕 104

アンインストール手順〔Hitachi IT Operations Director〕 118

アンインストール手順〔エージェント〕 119

アンインストール手順〔コントローラ〕 123

アンインストールの流れ〔システム全体〕 117

アンインストール〔クラスタシステム〕 124

い

- インストール時のトラブルシューティング情報の取得
[getinstlogs コマンド] 157
- インストールセットの作成手順 30
- インストールタイプ [Hitachi IT Operations
Director] 15
- インストール手順 [Hitachi IT Operations
Director] 15
- インストール手順 [エージェント (提供媒体)] 40

う

- ウィザード [ライセンス認証をしましょう] 19
- 上書きインストール手順 [Hitachi IT Operations
Director] 105
- 上書きインストール手順 [エージェント (提供媒体)]
107
- 上書きインストール [クラスタシステム] 115
- 上書きインストール [製品] 104

え

- エージェントインストール時のトラブルシューティ
ング 166
- エージェント設定の追加手順 89
- エージェント導入済みのコンピュータのリプレイス
手順 132
- エージェントのアンインストール手順 119
- エージェントのインストール状況を確認する流れ 44
- エージェントのインストール [自動] 44
- エージェントのインストール [手動] 30
- エージェントの環境を変更した場合の認識方法 180
- エージェントのセットアップ手順 42
- エージェントの提供媒体からのインストール手順 40
- エージェントの提供媒体からの上書きインストール
手順 107
- エージェントの導入計画 28
- エージェントの導入方法 32
- エージェントの導入 [Web サーバで公開] 33
- エージェントの導入 [ディスクコピー] 39
- エージェントの導入 [媒体で配布] 35
- エージェントの導入 [ファイルサーバで公開] 34

- エージェントの導入 [メールで配布] 36
- エージェントの導入 [ログオンスクリプト] 37
- エージェント未導入のコンピュータに配信する手順
[個別配信] 49
- エージェントレス構成システムの構築 52
- エージェントレス構成システムの構築時の設定 92
- エージェントレス構成システムの構築時のトラブル
シューティング 171
- エージェントレス構成システムを構築する流れ 52
- エージェントが接続する管理用サーバを切り替える
手順 137
- エージェントの監視項目を変更する手順 90

お

- オフライン管理からオンライン管理への切り替え手順
169
- オフライン管理構成システムの構築 51
- オフライン管理構成システムの構築時のトラブルシュー
ティング 169
- オフライン管理構成システムを構築する流れ 51
- オフラインでの認証 20
- オンライン管理からオフライン管理への切り替え手順
170
- オンラインでの認証 19

か

- 各システム構成の構築 50
- 環境構築 [管理用サーバ] 15
- 環境の移行 125
- 監視項目の変更手順 [エージェント] 90
- 管理対象の機器の確認手順 48
- 管理対象の設定手順 98
- 管理用サーバ構築時のトラブルシューティング 165
- 管理用サーバの環境構築 15
- 管理用サーバのセットアップ手順 17
- 管理用サーバのリプレイス手順 126
- 管理用サーバの IP アドレスを変更する手順 134
- 管理用サーバのホスト名を変更する手順 134

き

機器の把握 26

く

クラスタシステムで上書きインストールする流れ 115

クラスタシステムの構築 59

クラスタシステムの構築時のトラブルシューティング 176

クラスタシステムの構築の流れ 59

クラスタシステムの論理 IP アドレスを変更する手順 135

クラスタシステムの論理ホスト名を変更する手順 134

グループリソースの作成手順 (現用系サーバ) 60

こ

更新頻度の設定手順 (エージェントレス) 92

構築関連で使用するコマンド 138

構築時の設定のカスタマイズ 86

構築時の設定 (Active Directory 連携構成システム) 95

構築時の設定 (MDM 連携構成システム) 99

構築時の設定 (エージェントレス構成システム) 92

構築時の設定 (最小構成システム) 87

構築時の設定 (サポートサービス連携構成システム) 93

構築時の設定 (ネットワーク監視構成システム) 101

構築時のトラブルシューティングの流れ 163

構築の流れ (Active Directory 連携構成システム) 54

構築の流れ (MDM 連携構成システム) 55

構築の流れ (エージェントレス構成システム) 52

構築の流れ (オフライン管理構成システム) 51

構築の流れ (クラスタシステム) 59

構築の流れ (最小構成システム) 14

構築の流れ (サポートサービス連携構成システム) 53

構築の流れ (ネットワーク監視構成システム) 56

構築 (Active Directory 連携構成システム) 54

構築 (MDM 連携構成システム) 55

構築 (エージェントレス構成システム) 52

構築 (オフライン管理構成システム) 51

構築 (各システム構成) 50

構築 (クラスタシステム) 59

構築 (最小構成システム) 13

構築 (サポートサービス連携構成システム) 53

構築 (ネットワーク監視構成システム) 56

コマンドの実行手順 139

コマンドの説明形式 141

コマンド (構築関連) 138

コントローラのアンインストール手順 123

コンフィグレーションファイルで処理の設定を変更する手順 89

コンポーネントのアップデート 104

コンポーネントのアップデート方法 112

コンポーネントの登録手順 114

さ

サービス停止 (stopservice コマンド) 153

最小構成システム (管理用サーバとエージェント) の構築 13

最小構成システムの構築時の設定 87

最小構成システムの構築時のトラブルシューティング 165

最小構成システムを構築する流れ 14

最新の探索状況の確認手順 46

サポートサービスからの情報の登録 142

サポートサービスの接続設定手順 93

サポートサービス連携構成システムの構築 53

サポートサービス連携構成システムの構築時の設定 93

サポートサービス連携構成システムの構築時のトラブルシューティング 172

サポートサービス連携構成システムを構築する流れ 53

参考情報 178

し

システム構成要素のホスト名および IP アドレスを変更する 134

システム全体でのアンインストールの流れ 117

使用するフォルダの変更手順 69

除外対象の機器の確認手順 48

せ

- 製品のアンインストール 116
- 製品の上書きインストール 104
- 製品ライセンスの追加手順 20
- 製品ライセンスの認証 19
- セットアップ手順〔エージェント〕 42
- セットアップ手順〔管理用サーバ〕 17
- セットアップ内容の変更 68

そ

- 操作画面へのログイン 22
- 操作ログの取得手順 70
- 組織内の機器の把握 26

た

- 探索状況の確認 46
- 探索条件の設定手順〔Active Directory の探索〕 97
- 探索条件の設定手順〔ネットワークの探索〕 87
- 探索手順〔Active Directory に登録されている機器〕 96
- 探索手順〔ネットワークに接続されている機器〕 26
- 探索と同時にエージェントを配信する手順（ネットワークの探索）〔自動配信〕 45

つ

- 追加管理項目の設定手順〔Active Directory から取得する情報〕 95
- 追加手順〔エージェント設定〕 89
- 追加手順〔製品ライセンス〕 20
- 追加手順〔ネットワークモニタ設定〕 102
- 通貨単位の変更手順 78

て

- データベースのアップグレード手順 84
- データベースの初期化手順 85
- デフォルトパスワードの変更手順 23

と

- トラブルシューティング 162

トラブルシューティング〔1 台のコンピュータに対して 2 つの機器情報が表示される場合〕 168

トラブルシューティング〔Active Directory 連携構成システムの構築時〕 173

トラブルシューティング〔MDM 連携構成システムの構築時〕 174

トラブルシューティング〔エージェントインストール時〕 166

トラブルシューティング〔エージェントレス構成システムの構築時〕 171

トラブルシューティング〔オフライン管理構成システムの構築時〕 169

トラブルシューティング〔管理用サーバ構築時〕 165

トラブルシューティング〔クラスタシステムの構築時〕 176

トラブルシューティング〔構築時〕 163

トラブルシューティング〔最小構成システムの構築時〕 165

トラブルシューティング〔サポートサービス連携構成システムの構築〕 172

トラブルシューティング〔ネットワーク監視構成システムの構築時〕 175

トラブルシューティング用情報 166

トラブルシューティング用情報の取得〔getlogs コマンド〕 155

に

認証情報〔SNMP〕 88

認証情報〔Windows の管理共有〕 88

認証情報〔ネットワークの探索〕 88

ね

ネットワーク監視構成システムの構築 56

ネットワーク監視構成システムの構築時の設定 101

ネットワーク監視構成システムの構築時のトラブルシューティング 175

ネットワーク監視構成システムを構築する流れ 56

ネットワーク制御リストの自動更新の設定を編集する手順 101

ネットワーク制御リストの編集手順 101

ネットワーク帯域の制御手順 80

ネットワークに接続されている機器の探索手順 26
ネットワークの探索時に使用する認証情報 88
ネットワークの探索条件の設定手順 87
ネットワークモニタ設定の追加手順 102
ネットワークモニタ設定の割り当ての変更手順 102
ネットワークモニタの無効化手順 121
ネットワークモニタの有効化手順 57
ネットワークモニタを有効にしたコンピュータをリ
プレイスする手順 133

は

バージョンアップ手順 109
バージョンアップの流れ [Hitachi IT Operations
Director のシステム全体] 108
バックアップデータのリストア [importdb コマ
ンド] 149
バックアップの取得 [exportdb コマンド] 145
発見した機器の確認手順 47

へ

編集手順 [ネットワーク制御リスト] 101

ほ

ポート番号一覧 178
ポート番号の変更手順 76
ホスト識別子のリセット [resrtnid.vbs コマンド]
159
ホスト名の変更手順 [管理用サーバ] 134
ホスト名の変更 [システム構成要素] 134

め

メール通知 [Active Directory の探索] 97
メール通知 [ネットワークの探索] 87
メッセージの出力形式 163

ゆ

ユーザーアカウントの情報の設定手順 24
ユーザーアカウントのロックの解除手順 24

ら

ライセンス認証手順 19

り

リプレイス手順 [エージェント導入済みのコンピュ
ータ] 132
リプレイス手順 [管理用サーバ] 126
リプレイス手順 [ネットワークモニタを有効にしたコ
ンピュータ] 133

ろ

ログイン 22
ログイン制限情報を変更する手順 82
ログイン手順 22
ロックの解除 [ユーザーアカウント] 24
論理 IP アドレスを変更する手順 [クラスタシステム]
135
論理ホスト名の変更手順 [クラスタシステム] 134