

JP1 Version 10

JP1/IT Desktop Management 2 運用ガイド

手引・操作書

3021-3-276

JP1 *Version*
10

前書き

■ 対象製品

P-2642-78A4 JP1/IT Desktop Management 2 - Manager 10-50

製品構成一覧および内訳形名

- ・ P-CC2642-7AA4 JP1/IT Desktop Management 2 - Manager (適用 OS : Windows Server 2012、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows Server 2003)
- ・ P-CC2642-7BA4 JP1/IT Desktop Management 2 - Agent (適用 OS : Windows 8.1、Windows 8、Windows Server 2012、Windows 7 Enterprise、Windows 7 Professional、Windows 7 Ultimate、Windows 7 Home Premium、Windows 7 Starter、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows Vista、Windows Server 2003、Windows XP)
- ・ P-CC2642-7CA4 JP1/IT Desktop Management 2 - Network Monitor (適用 OS : Windows 8.1 Enterprise、Windows 8.1 Pro、Windows 8 Enterprise、Windows 8 Pro、Windows Server 2012、Windows 7 Enterprise、Windows 7 Professional、Windows 7 Ultimate、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows Server 2003(x86))
- ・ P-CC2642-7DA4 JP1/IT Desktop Management 2 - Asset Console (適用 OS : Windows Server 2012、Windows Server 2008 Datacenter、Windows Server 2008 Enterprise、Windows Server 2008 Standard、Windows Server 2003)

■ 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

Acrobat は、Adobe Systems Incorporated (アドビシステムズ社) の商標です。

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。

ActiveX 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。

Adobe、および Flash は、Adobe Systems Incorporated (アドビシステムズ社) の米国ならびに他の国における商標または登録商標です。

「B' s Recorder」の名称は、ソースネクスト株式会社の日本国内における登録商標です。

Firefox は Mozilla Foundation の登録商標です。

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。

Mac OS は、Apple Inc.の商標です。

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 Office 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 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。

MobileIron は、米国における MobileIron の登録商標です。

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。

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。

Symantec、Symantec AntiVirus は、Symantec Corporation 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。

VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。

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。

ウイルスバスターは、トレンドマイクロ株式会社の登録商標です。

秘文は、株式会社日立ソリューションズの登録商標です。

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

Microsoft Corporation のガイドラインに従って画面写真を使用しています。



■ 発行

2014 年 12 月 3021-3-276

■ 著作権

All Rights Reserved. Copyright (C) 2014, Hitachi, Ltd.

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

はじめに

このマニュアルは、JP1/IT Desktop Management 2 - Manager（以降、JP1/IT Desktop Management 2 と略す）の運用例、操作方法などを説明したものです。

なお、操作画面の詳細については、オンラインヘルプで説明しています。

■ 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。

- JP1/IT Desktop Management 2 を利用して、組織内のセキュリティ管理や資産管理をする管理者の方
- JP1/IT Desktop Management 2 の運用方法や操作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 製品を使った運用方法

JP1/IT Desktop Management 2 を使用した運用方法について説明しています。

第 2 章 製品ライセンスを登録する

製品ライセンスを登録する方法について説明しています。

第 3 章 操作画面にログインする

JP1/IT Desktop Management 2 の操作画面にログインする方法について説明しています。

第 4 章 ユーザーアカウントを管理する

ユーザーアカウントを管理する方法について説明しています。

第 5 章 操作画面を利用する

JP1/IT Desktop Management 2 の操作画面での共通操作について説明しています。

第 6 章 機器を管理する

組織内の機器から情報を収集して、現状を把握する方法について説明しています。

第 7 章 機器をリモートコントロールする

組織内の機器をリモートコントロールする方法について説明しています。

第 8 章 機器のネットワーク接続を管理する

組織内の機器のネットワークを接続したり遮断したりする方法について説明しています。

第 9 章 セキュリティ状況を管理する

組織内のセキュリティ管理およびセキュリティ状況の把握について説明しています。

第 10 章 操作ログを管理する

利用者の操作を把握および追跡する方法について説明しています。

第 11 章 資産を管理する

ハードウェア資産、ソフトウェアライセンス、契約の管理について説明しています。

第 12 章 ソフトウェアやファイルを配布する

ソフトウェアのインストール・アンインストールやファイルの配布について説明しています。

第 13 章 イベントを参照する

JP1/IT Desktop Management 2 で出力されるイベントの参照方法について説明しています。

第 14 章 レポートを参照する

レポートを表示して、組織内のセキュリティ管理や資産管理の状況を確認する方法について説明しています。

第 15 章 設定をカスタマイズする

設定画面およびセットアップでカスタマイズできる項目について説明しています。

第 16 章 データベースを管理する

データベースマネージャを使ってデータベースを管理する方法について説明しています。

第 17 章 コマンド

JP1/IT Desktop Management 2 のコマンドについて説明しています。

第 18 章 トラブルシューティング

JP1/IT Desktop Management 2 の運用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。

第 19 章 イベント

JP1/IT Desktop Management 2 のイベントを一覧で説明しています。

付録 A 参考情報

JP1/IT Desktop Management 2 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「JP1/IT Desktop Management 2 導入・設計ガイド」を参照してください。

目次

前書き 2

はじめに 6

1 製品を使った運用方法 22

1.1 エージェントの導入 23

1.1.1 組織内の機器を把握する 24

1.1.2 エージェントを手動でインストールする 31

1.1.3 エージェントを自動でインストールする 42

1.1.4 エージェントのインストール状況を確認する流れ 48

1.2 機器をオフラインで管理する 50

1.2.1 オフライン管理したいコンピュータにエージェントを導入する流れ 51

1.2.2 外部記憶媒体を利用してオフライン管理のコンピュータから機器情報を取得する流れ 52

1.2.3 ログオンスクリプトを利用してオフライン管理のコンピュータから機器情報を取得する流れ 54

1.3 複数の管理者で業務を分担する流れ 57

1.3.1 ユーザーアカウントの設定内容を検討する流れ 57

1.3.2 複数のユーザーアカウントを登録する流れ 59

1.3.3 複数の管理者で連携して業務を進める流れ 60

1.4 スマートデバイスを管理する 61

1.4.1 スマートデバイスの管理を始める流れ 63

1.4.2 スマートデバイスをリプレースする流れ 67

1.4.3 スマートデバイスの利用者を変更する流れ 70

1.4.4 スマートデバイスの紛失に対応する 74

1.4.5 利用者がスマートデバイスのパスコードを忘れた場合に対処する 76

1.4.6 スマートデバイスを滅却する流れ 78

1.5 機器のリモートコントロール 81

1.5.1 コンピュータをリモートコントロールして問い合わせに対処する流れ 82

1.5.2 遠隔地にあるサーバを運用する流れ 85

1.5.3 遠隔地にいる利用者に作業を指示する流れ 87

1.6 機器のネットワーク接続の管理 89

1.6.1 個人所有 PC のネットワーク接続を禁止する流れ 91

1.6.2 ウィルス感染時に機器のネットワーク接続を遮断する流れ 95

1.6.3 セキュリティポリシーに違反した機器のネットワーク接続を自動制御する流れ 97

1.6.4 一時的に機器のネットワーク接続を許可する流れ 100

1.7 セキュリティ状況の管理 102

1.7.1 セキュリティポリシーを設定する 104

1.7.2	セキュリティポリシー違反を対策する	106
1.7.3	自動で更新プログラムを配布する流れ	109
1.7.4	更新プログラムを手動で登録して配布する方法	113
1.7.5	ウィルス感染時に対策状況を確認する	116
1.7.6	許可したソフトウェアだけ利用できるようにする流れ	118
1.7.7	USB デバイスの使用を制限する	121
1.7.8	セキュリティ監査に対応する流れ	127
1.8	情報漏えいが起きていないか確認する	131
1.8.1	検知された不審操作を調査する流れ	131
1.8.2	情報が持ち出された形跡を調査する流れ	133
1.9	ハードウェア資産を管理する	137
1.9.1	手持ちの管理台帳の情報を登録する	138
1.9.2	ハードウェア資産情報をメンテナンスする方法	140
1.9.3	機器を購入する流れ	141
1.9.4	機器をリプレースする流れ	145
1.9.5	機器を棚卸する流れ	149
1.9.6	利用されていない機器を確認する流れ	152
1.9.7	機器を滅却する流れ	155
1.9.8	機器の障害に対応する流れ	157
1.9.9	機器情報の不審な変更を調査する流れ	161
1.10	ソフトウェアライセンスを管理する	162
1.10.1	ソフトウェアを購入する流れ	164
1.10.2	余剰ライセンスを有効利用する流れ	168
1.10.3	ソフトウェアライセンスを棚卸する流れ	173
1.10.4	ソフトウェアライセンスを滅却する流れ	175
1.11	資産に関する契約を管理する流れ	178
1.11.1	満了となる契約情報を把握する	178
1.11.2	契約を更改する	179
1.11.3	契約を終了する	180
1.12	資産のコスト削減を検討する流れ	181
1.12.1	毎月の資産に掛かるコストを確認する	181
1.12.2	利用されていない資産を確認する	182
1.12.3	余剰ライセンスを確認する	183
1.13	ソフトウェアやファイルの配布	185
1.13.1	ソフトウェアをインストールする流れ	186
1.13.2	ファイルを配布する流れ	191
1.13.3	ソフトウェアをアンインストールする流れ	195
1.14	職制変更に伴い部署の定義を変更する流れ	201
1.14.1	新体制の部署の規定を検討する	201

- 1.14.2 部署の定義を新体制に合わせて変更する流れ 202
- 1.14.3 資産情報を新体制に合わせて更新する 204
- 1.14.4 旧体制だけで使われていた情報を削除する流れ 205

2 製品ライセンスを登録する 206

- 2.1 製品ライセンスを登録する手順 207
- 2.2 製品ライセンスの情報を確認する方法 208
- 2.3 製品ライセンスを追加する手順 209

3 操作画面にログインする 210

- 3.1 ログインする手順 211
- 3.2 ユーザーアカウントの情報を設定する手順 212
- 3.3 デフォルトパスワードを変更する手順 213
- 3.4 ログアウトする手順 214

4 ユーザーアカウントを管理する 215

- 4.1 ユーザーアカウントを追加する手順 216
- 4.2 ユーザーアカウントを編集する手順 217
- 4.3 ユーザーアカウントを削除する手順 218
- 4.4 自分のパスワードを変更する手順 219
- 4.5 ほかの管理者のパスワードを変更する手順 220
- 4.6 パスワードを初期化する手順 221
- 4.7 管轄範囲を追加する手順 222
- 4.8 管轄範囲を削除する手順 223
- 4.9 ユーザーアカウントのロックを解除する手順 224

5 操作画面を利用する 225

- 5.1 表示されるパネルとレイアウトを設定する手順 226
- 5.2 表示中の画面の情報を更新する手順 227
- 5.3 一覧の表示項目を変更する手順 228
- 5.4 各画面での共通操作 230
- 5.5 ユーザー定義のグループを管理する 232
 - 5.5.1 ユーザー定義のグループを追加する手順 232
 - 5.5.2 ユーザー定義のグループ名を変更する手順 232
 - 5.5.3 ユーザー定義のグループを削除する手順 233
 - 5.5.4 ユーザー定義のグループ条件を変更する手順 234
- 5.6 カスタムグループを管理する 235
 - 5.6.1 カスタムグループを追加する手順 235
 - 5.6.2 カスタムグループ名を変更する手順 236
 - 5.6.3 カスタムグループを削除する手順 236

5.6.4	カスタムグループに情報を追加する手順	237
5.6.5	カスタムグループから情報を削除する手順	238
5.7	フィルタを管理する	239
5.7.1	フィルタを保存する手順	239
5.7.2	フィルタを削除する手順	239
5.8	操作画面利用時の注意事項	241
6	機器を管理する	243
6.1	機器の管理を始める方法	244
6.2	インストールセットを作成する手順	246
6.3	Active Directory に登録されている機器を探索する手順	248
6.4	ネットワークに接続されている機器を探索する手順	249
6.5	機器を管理対象にする手順	251
6.6	機器を除外対象にする手順	252
6.7	オフライン管理からオンライン管理に切り替える手順	253
6.8	オンライン管理からオフライン管理に切り替える手順	254
6.9	機器を削除する手順	255
6.10	機器情報を編集する手順	256
6.11	最新の機器情報を取得する手順	257
6.12	情報収集用ツールを生成する手順	259
6.13	情報収集用ツールで収集した機器情報を通知する手順	260
6.14	利用者情報を取得する手順	262
6.15	機器画面で【利用者情報の入力】画面の表示間隔を設定する手順	264
6.16	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	265
6.17	機器情報をエクスポートする手順	266
6.18	ソフトウェア情報をエクスポートする手順	267
6.19	ソフトウェア情報を削除する手順	268
6.20	使用禁止ソフトウェアを設定する手順	269
6.21	機器画面でコンピュータからソフトウェアをアンインストールする手順	270
6.22	利用者にメッセージを通知する手順	271
6.23	コンピュータの電源を制御する手順	272
6.24	スマートデバイスの情報を取得する手順	273
6.25	スマートデバイスをロックする手順	274
6.26	スマートデバイスのパスコードをリセットする手順	275
6.27	スマートデバイスを初期化する手順	276
6.28	部署・設置場所の定義を追加する手順	277
6.29	部署・設置場所の定義を編集する手順	278
6.30	部署・設置場所の定義を削除する手順	280
6.31	旧体制で使われていた階層だけを削除する手順	282

6.32 部署・設置場所の名称を変更する手順 283

6.33 部署・設置場所を削除する手順 284

7 機器をリモートコントロールする 285

7.1 コントローラをインストールする手順 286

7.2 コントローラをアンインストールする手順 288

7.3 コントローラ的环境設定を変更する手順 289

7.4 リモコンエージェントの動作環境を設定する手順 290

7.5 リモートコントロールを利用する 291

7.5.1 コントローラを直接起動する手順 291

7.5.2 コンピュータを選択してリモートコントロールを開始する手順 291

7.5.3 ホスト名または IP アドレスを直接指定してリモートコントロールを開始する手順 292

7.5.4 接続履歴を利用してリモートコントロールを開始する手順 293

7.5.5 コンピュータを検索してリモートコントロールを開始する手順 294

7.5.6 操作画面からリモートコントロールを開始する手順 295

7.5.7 リモートコントロール中のコンピュータとの接続を切断する手順 296

7.5.8 リモートコントロール中のコンピュータとの接続を自動切断する設定手順 296

7.5.9 コントローラを終了する手順 297

7.5.10 接続モードを変更する手順 297

7.5.11 電源が OFF のコンピュータをリモートコントロールする手順 298

7.5.12 リモートコントロール中のコンピュータの電源を OFF にする手順 298

7.5.13 リモートコントロール中のコンピュータを再起動する手順 299

7.5.14 リモートコントロール中に [Ctrl] + [Alt] + [Delete] キーを入力する手順 299

7.5.15 コントローラに特殊キーを登録する手順 300

7.5.16 リモートコントロール中に特殊キーを入力する手順 300

7.5.17 リモートコントロール中の送受信データを暗号化する手順 301

7.5.18 コントローラのウィンドウに合わせてコンピュータの画面を拡大、縮小する手順 301

7.5.19 フルスクリーン表示で機器をリモートコントロールする手順 301

7.5.20 複数のコントローラの画面を整列表示させる手順 303

7.5.21 コントローラのバーの表示を切り替える手順 303

7.5.22 オートスクロールでリモートコントロールする手順 303

7.5.23 リモートコントロール中のマウスホイールでのスクロールを制御する手順 304

7.5.24 リモートコントロール中の画面を画像として保存する手順 304

7.5.25 リモート CD-ROM を利用する手順 305

7.5.26 [リモートコントロール] ウィンドウから接続できるコンピュータを検索する手順 306

7.5.27 接続リストからリモートコントロールできるコンピュータを検索する手順 306

7.5.28 リモートコントロール接続できるコンピュータの検索方法をカスタマイズする手順 308

7.6 ファイル転送を利用する 309

7.6.1 [ファイル転送] ウィンドウを起動する手順 309

7.6.2	ファイル転送の接続を切断する手順	309
7.6.3	[ファイル転送] ウィンドウを終了する手順	310
7.6.4	ファイル転送先のコンピュータを追加する手順	310
7.6.5	転送するファイル情報を確認する手順	310
7.6.6	ファイル転送時のセキュリティ設定をする手順	311
7.6.7	ファイルを転送する手順	312
7.6.8	リモートコントロール中のコンピュータのファイルの操作手順	313
7.6.9	[ファイル転送] ウィンドウからファイルを編集する手順	314
7.6.10	ファイル転送のオプションを設定する手順	315
7.7	接続リストを利用する	317
7.7.1	コンピュータごとの接続環境を設定する手順	317
7.7.2	接続リストを表示・終了する手順	318
7.7.3	接続リストからコンピュータに接続する	319
7.7.4	接続リストを作成する手順	319
7.7.5	接続リストの項目を移動・コピーする	323
7.7.6	接続リストの項目を削除する手順	323
7.7.7	接続リストの項目名を変更する手順	324
7.7.8	接続リストの項目の属性を変更する手順	324
7.7.9	接続リストの項目を検索する手順	325
7.7.10	接続リストの項目の属性を確認する手順	325
7.7.11	リクエストサーバを作成する手順	326
7.7.12	リクエストサーバを開始または停止する手順	326
7.8	録画機能を利用する	328
7.8.1	再生時にできる操作手順	328
7.8.2	再生画面の表示手順	329
7.8.3	リモートコントロールを録画する手順	330
7.8.4	録画を一時停止・再開する手順	330
7.8.5	録画データを再生する手順	331
7.8.6	録画ファイルの情報を確認する	331
7.8.7	録画ファイルを AVI 形式に変換する手順	332
7.9	リモコンエージェントを利用する	333
7.9.1	リモコンエージェントのステータスウィンドウを表示する手順	333
7.9.2	リモコンエージェントを終了する手順	333
7.9.3	コントローラからの接続要求の許可、拒否	334
7.9.4	コンピュータ側で接続モードを変更する手順	334
7.9.5	リモートコントロールの対象のコンピュータから接続を切断する手順	335
7.9.6	コントローラに接続要求を出す	336
7.9.7	接続要求をキャンセルする手順	337
7.10	チャットを利用する	338

- 7.10.1 チャットサーバの動作環境を設定する手順 338
- 7.10.2 [チャット] ウィンドウの動作環境を設定する手順 338
- 7.10.3 チャットサーバを起動する手順 339
- 7.10.4 エージェントでの起動方法によるチャットサーバの機能差異 340
- 7.10.5 チャットを開始する手順 341
- 7.10.6 チャットでメッセージを送信する手順 342
- 7.10.7 チャットを終了する手順 342
- 7.10.8 チャットの内容を保存する手順 343
- 7.10.9 チャットの内容を印刷する手順 344
- 7.10.10 [チャット] ウィンドウからリモートコントロールを開始する手順 344
- 7.10.11 [チャットサーバ] アイコンから操作する手順 345

8 機器のネットワーク接続を管理する 346

- 8.1 ネットワークモニタを有効にする手順 347
- 8.2 ネットワークモニタを無効にする手順 349
- 8.3 ネットワーク接続を許可する手順 351
- 8.4 ネットワーク接続を遮断する手順 352
- 8.5 自動的にネットワーク接続が遮断された機器を再接続する手順 354
- 8.6 ネットワークモニタ設定を管理する 356
 - 8.6.1 ネットワークモニタ設定を追加する手順 356
 - 8.6.2 ネットワークモニタ設定を編集する手順 356
 - 8.6.3 ネットワークモニタ設定を削除する手順 356
 - 8.6.4 ネットワークモニタ設定を割り当てる手順 357
 - 8.6.5 ネットワークモニタ設定の割り当てを変更する手順 358
- 8.7 ネットワーク制御リストを管理する 359
 - 8.7.1 ネットワーク制御リストに機器を追加する手順 359
 - 8.7.2 ネットワーク制御リストの機器を編集する手順 359
 - 8.7.3 ネットワーク制御リストから機器を削除する手順 360
 - 8.7.4 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 360
- 8.8 特例接続を管理する 362
 - 8.8.1 特例接続の設定を追加する手順 362
 - 8.8.2 特例接続の設定を編集する手順 362
 - 8.8.3 特例接続の設定を削除する手順 363
- 8.9 JP1/NETM/NM - Manager 連携の設定を有効にする手順 364

9 セキュリティ状況を管理する 365

- 9.1 セキュリティ状況を確認する 366
- 9.2 判定対象から除外するユーザーを設定する手順 372
- 9.3 セキュリティポリシーを利用する 373

- 9.3.1 セキュリティポリシーを追加する手順 373
- 9.3.2 セキュリティポリシーを編集する手順 373
- 9.3.3 セキュリティポリシーをコピーする手順 374
- 9.3.4 セキュリティポリシーを削除する手順 375
- 9.3.5 セキュリティポリシーを割り当てる手順 375
- 9.3.6 セキュリティポリシーの割り当てを解除する手順 376
- 9.3.7 セキュリティポリシーにユーザー定義のセキュリティ設定を追加する手順 377
- 9.3.8 セキュリティの判定結果に応じて機器のネットワーク接続を制御する手順 378
- 9.4 セキュリティポリシー違反を強制対策する手順 379
- 9.5 利用者にメッセージを通知する手順 380
- 9.6 デバイスの使用を抑止する手順 381
- 9.7 USB デバイスを登録する手順 383
- 9.8 更新プログラムを管理する 385
 - 9.8.1 更新プログラムを自動配布する手順 385
 - 9.8.2 更新プログラムを手動で登録して配布する手順 386
 - 9.8.3 更新プログラム一覧へ更新プログラムを手動で追加する手順 387
 - 9.8.4 更新プログラムの手動登録手順 387
 - 9.8.5 更新プログラムファイルを登録する手順 389
 - 9.8.6 更新プログラムグループを作成する手順 390
 - 9.8.7 更新プログラムグループ名を変更する手順 391
 - 9.8.8 更新プログラムグループを削除する手順 392
 - 9.8.9 更新プログラムグループに更新プログラムを追加する 手順 393
 - 9.8.10 更新プログラムグループから更新プログラムを削除する手順 394
- 9.9 禁止操作の抑止イベントと操作ログを上位システムに通知する間隔を設定する手順 395
- 9.10 禁止操作の抑止イベントと操作ログを保持する期間を設定する手順 396

10 操作ログを管理する 397

- 10.1 管理用サーバへの操作ログの収集を設定する手順 398
- 10.2 操作ログを確認する手順 399
- 10.3 不審と見なす操作を検知するための設定手順 401
- 10.4 不審操作のログを確認する手順 402
- 10.5 不審操作のイベントを確認する手順 403
- 10.6 操作ログを追跡調査する手順 404
- 10.7 過去の操作ログを取り込む 405
 - 10.7.1 管理用サーバに過去の操作ログを取り込む手順 405
 - 10.7.2 コンピュータを選択して操作ログを取り込む手順 406
- 10.8 操作ログのバックアップファイルを管理する 409
 - 10.8.1 操作ログの保管先フォルダからバックアップファイルを削除する手順 409
 - 10.8.2 操作ログをバックアップする手順 409

- 10.8.3 操作ログの保管先フォルダを一時的に変更する手順 410
- 10.8.4 操作ログの保管先のディスクを変更する手順 411
- 10.8.5 操作ログのディスクの空き容量のしきい値を変更する手順 411

11 資産を管理する 413

- 11.1 ハードウェア資産情報を利用する 414
 - 11.1.1 ハードウェア資産情報を追加する手順 414
 - 11.1.2 ハードウェア資産情報を編集する手順 415
 - 11.1.3 ハードウェア資産情報を削除する手順 416
 - 11.1.4 資産画面で【利用者情報の入力】画面の表示間隔を設定する手順 417
 - 11.1.5 資産状態を追加する手順 418
 - 11.1.6 資産状態を変更する手順 419
 - 11.1.7 予定資産状態を変更する手順 419
 - 11.1.8 手動で棚卸日を更新する手順 420
 - 11.1.9 CSV ファイルを基に棚卸日を一括更新する手順 422
 - 11.1.10 棚卸日の自動更新を設定する手順 423
 - 11.1.11 バーコードリーダーを使用して棚卸する 425
 - 11.1.12 ハードウェア資産に対する契約情報を関連づける手順 426
 - 11.1.13 複数のハードウェア資産情報を関連づける手順 427
 - 11.1.14 ハードウェア資産情報に対応する機器情報を変更する手順 427
 - 11.1.15 ハードウェア資産情報に関連づいた機器情報の代表を設定する手順 429
 - 11.1.16 部署・設置場所の定義を追加する手順 429
 - 11.1.17 部署・設置場所の定義を編集する手順 430
 - 11.1.18 部署・設置場所の定義を削除する手順 431
 - 11.1.19 旧体制で使われていた階層だけを削除する手順 432
 - 11.1.20 部署・設置場所の名称を変更する手順 433
 - 11.1.21 部署・設置場所を削除する手順 434
- 11.2 ソフトウェアライセンス情報を利用する 436
 - 11.2.1 管理ソフトウェア情報を追加する手順 436
 - 11.2.2 管理ソフトウェア情報を編集する手順 437
 - 11.2.3 管理ソフトウェア情報を削除する手順 437
 - 11.2.4 ソフトウェアライセンス情報を追加する手順 438
 - 11.2.5 ソフトウェアライセンス情報を編集する手順 439
 - 11.2.6 ソフトウェアライセンス情報を削除する手順 440
 - 11.2.7 ライセンス状態を追加する手順 441
 - 11.2.8 ライセンス状態を変更する手順 442
 - 11.2.9 予定ライセンス状態を変更する手順 443
 - 11.2.10 手動で棚卸日を更新する手順 444
 - 11.2.11 CSV ファイルを基に棚卸日を一括更新する手順 445

- 11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順 446
- 11.2.13 ソフトウェアライセンスを移管する手順 447
- 11.2.14 ソフトウェアライセンスに対する契約情報を関連づける手順 448
- 11.3 契約情報を利用する 449
 - 11.3.1 契約情報を追加する手順 449
 - 11.3.2 契約情報を編集する手順 449
 - 11.3.3 契約情報を削除する手順 450
 - 11.3.4 契約状態を追加する手順 451
 - 11.3.5 契約状態を変更する手順 452
 - 11.3.6 契約対象のハードウェア資産を関連づける手順 453
 - 11.3.7 契約対象のソフトウェアライセンスを関連づける手順 453
- 11.4 資産情報をインポートする 455
 - 11.4.1 ハードウェア資産情報をインポートする手順 455
 - 11.4.2 ソフトウェアライセンス情報をインポートする手順 456
 - 11.4.3 管理ソフトウェア情報をインポートする手順 458
 - 11.4.4 契約情報をインポートする手順 459
 - 11.4.5 契約会社リストをインポートする手順 461
- 11.5 資産情報をエクスポートする手順 463

12 ソフトウェアやファイルを配布する 464

- 12.1 コンピュータにソフトウェアをインストールする手順 465
- 12.2 コンピュータにファイルを配布する手順 467
- 12.3 コンピュータからソフトウェアをアンインストールする手順 469
- 12.4 パッケージを管理する 471
 - 12.4.1 パッケージを追加する手順 471
 - 12.4.2 パッケージを編集する手順 471
 - 12.4.3 パッケージを削除する手順 472
 - 12.4.4 パッケージ情報をエクスポートする手順 472
- 12.5 タスクを管理する 474
 - 12.5.1 タスクを追加する手順 474
 - 12.5.2 タスクを編集する手順 475
 - 12.5.3 タスクをコピーする手順 476
 - 12.5.4 タスクを削除する手順 476
 - 12.5.5 タスクを中止する手順 477
 - 12.5.6 タスクを再実行する手順 478
 - 12.5.7 タスク情報をエクスポートする手順 480
- 12.6 利用者側でダウンロードやインストールを延期する 481

13	イベントを参照する 483
13.1	イベントの詳細を確認する手順 484
13.2	イベント情報をエクスポートする手順 485
14	レポートを参照する 486
14.1	レポートを表示する手順 487
14.2	最新のデータでレポートを表示する手順 488
14.3	レポートを印刷する手順 489
14.4	レポートを PDF ファイルで保存する手順 490
15	設定をカスタマイズする 491
15.1	エージェントの設定 492
15.1.1	エージェント設定の管理 492
15.1.2	エージェント設定を追加する手順 493
15.1.3	エージェント設定を編集する手順 493
15.1.4	ネットワークモニタを有効化するコンピュータのエージェント設定を編集する手順 494
15.1.5	エージェント設定を削除する手順 494
15.1.6	エージェント設定を割り当てる手順 495
15.1.7	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 496
15.2	機器の探索の設定 498
15.2.1	探索条件を設定する手順（ネットワークの探索） 498
15.2.2	探索条件を設定する手順（Active Directory の探索） 499
15.2.3	ネットワークの探索時に使用する認証情報 500
15.2.4	機器の探索状況の確認 501
15.2.5	最新の探索状況を確認する手順 502
15.2.6	発見した機器を確認する手順 502
15.2.7	管理対象の機器を確認する手順 503
15.2.8	除外対象の機器を確認する手順 504
15.3	セキュリティ管理の設定 505
15.3.1	セキュリティ判定のスケジュールを変更する手順 505
15.3.2	操作ログを自動的に取り込む手順 505
15.3.3	操作ログを定期的にエクスポートする手順 506
15.4	資産管理の設定 507
15.4.1	資産管理項目を追加する手順 507
15.4.2	資産管理項目の入力方法やデータ型を変更する手順 507
15.4.3	部署・設置場所の定義を追加する手順 508
15.4.4	部署・設置場所の定義を編集する手順 509
15.4.5	部署・設置場所の定義を削除する手順 510
15.4.6	言語ごとの部署・設置場所の表示名を設定する手順 511

- 15.4.7 旧体制で使われていた階層だけを削除する手順 512
- 15.4.8 契約会社情報の管理 513
- 15.4.9 契約会社情報を追加する手順 513
- 15.4.10 契約会社情報を編集する手順 514
- 15.4.11 契約会社情報を削除する手順 514
- 15.4.12 契約会社リストをエクスポートする手順 515
- 15.5 機器管理の設定 517
 - 15.5.1 ソフトウェア検索条件を追加する手順 517
 - 15.5.2 ソフトウェア検索条件を編集する手順 517
 - 15.5.3 ソフトウェア検索条件を削除する手順 518
 - 15.5.4 ソフトウェア検索条件をインポートする手順 519
 - 15.5.5 ソフトウェア検索条件をエクスポートする手順 519
 - 15.5.6 AMT の認証情報を設定する手順 520
 - 15.5.7 機器の変更履歴の取得を設定する手順 521
- 15.6 レポートの設定 522
 - 15.6.1 レポートの保存期間と開始日を変更する手順 522
 - 15.6.2 ダイジェストレポートの送付先を設定する手順 522
- 15.7 イベントの設定 524
 - 15.7.1 イベント通知の設定をする手順 524
- 15.8 他システムとの接続情報の設定 526
 - 15.8.1 メールサーバを設定する手順 526
 - 15.8.2 Active Directory と接続するための情報を設定する手順 527
 - 15.8.3 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 528
 - 15.8.4 MDM システムと連携するための情報を設定する手順 529

16 データベースを管理する 532

- 16.1 データベースマネージャを起動する手順 533
- 16.2 データベースをバックアップする 535
- 16.3 データベースをリストアする 537
- 16.4 データベースを再編成する 540

17 コマンド 543

- 17.1 コマンドを実行する手順 544
- 17.2 コマンドの説明形式 546
- 17.3 コマンド一覧 547
- 17.4 ioutils exportasset (ハードウェア資産情報のエクスポート) 549
- 17.5 ioutils importasset (ハードウェア資産情報のインポート) 552
- 17.6 ioutils exportfield (追加管理項目の設定のエクスポート) 556
- 17.7 ioutils importfield (追加管理項目の設定のインポート) 559

17.8	ioutils exporttemplate (テンプレートのエクスポート)	562
17.9	ioutils importtemplate (テンプレートのインポート)	565
17.10	ioutils exportdevice (機器情報のエクスポート)	568
17.11	ioutils exportdevicedetail (詳細な機器情報のエクスポート)	571
17.12	ioutils exportpolicy (セキュリティポリシーの設定のエクスポート)	574
17.13	ioutils importpolicy (セキュリティポリシーの設定のインポート)	577
17.14	ioutils exportupdategroup (更新プログラムグループの設定のエクスポート)	580
17.15	ioutils importupdategroup (更新プログラムグループの設定のインポート)	583
17.16	ioutils exporttoplog (操作ログのエクスポート)	586
17.17	ioutils exportfilter (フィルタの設定のエクスポート)	590
17.18	ioutils importfilter (フィルタの設定のインポート)	594
17.19	updatesupportinfo (サポートサービスからの情報の登録)	597
17.20	exportdb (バックアップの取得)	600
17.21	importdb (バックアップデータのリストア)	604
17.22	reorgdb (データベースの再編成)	608
17.23	stopservice (サービス停止)	611
17.24	startservice (サービス開始)	613
17.25	getlogs (トラブルシュート用情報の取得)	615
17.26	getinstlogs (インストール時のトラブルシュート用情報の取得)	617
17.27	addfwlist.bat (Windows ファイアウォールの例外許可設定)	619
17.28	resetnid.vbs (ホスト識別子のリセット)	621
17.29	getinv.vbs (オフライン管理の情報収集)	624
17.30	ioassetsfieldutil export (共通管理項目と追加管理項目の定義のエクスポート)	626
17.31	ioassetsfieldutil import (共通管理項目と追加管理項目の定義のインポート)	629

18 **トラブルシューティング 633**

18.1	運用時のトラブルシューティングの流れ	634
18.2	機器が発見されない場合の対処方法	636
18.3	認証エラー発生時の対処方法	637
18.4	情報収集用ツールで収集した機器情報の通知に失敗した場合のトラブルシューティング	639
18.5	CSV ファイルが正しく表示されないときの対処方法	640
18.6	共通管理項目と追加管理項目の定義のインポートに失敗した場合のトラブルシューティング	641
18.7	ディスクの空き容量が少ないときの対処方法	642
18.8	フェールオーバー発生後の対処方法	643
18.9	管理用サーバのトラブルシューティング	645
18.10	エージェントのトラブルシューティング手順	665
18.11	リモートコントロール時のトラブルシューティング	668
18.12	ネットワーク制御時のトラブルシューティング	669
18.13	Active Directory 連携時のトラブルシューティング手順	670

- 18.14 MDM 連携時のトラブルシューティング 671
- 18.15 JP1/IM 連携時のトラブルシューティング 672
- 18.16 データベース障害のトラブルシューティング 673

19 イベント 674

- 19.1 イベント一覧 675
- 19.2 JP1 イベントの属性 699

付録 709

- 付録 A 参考情報 710
 - 付録 A.1 ポート番号一覧 710
 - 付録 A.2 管理用サーバとエージェント間の通信 715
 - 付録 A.3 セキュリティ状況の判定除外ユーザー設定ファイルの形式 715
 - 付録 A.4 エクスポートした操作ログの出力形式 716
 - 付録 A.5 共通管理項目と追加管理項目の定義のインポートファイルの設定項目 720
 - 付録 A.6 サポートサービスからの情報の取得 721
 - 付録 A.7 再起動によって設定が適用されるケース 723
 - 付録 A.8 時間の取り扱い 724
 - 付録 A.9 監査ログの出力 726
 - 付録 A.10 各バージョンの変更内容 732

索引 742

1

製品を使った運用方法

ここでは、JP1/IT Desktop Management 2 を使用した運用方法について説明します。

1.1 エージェントの導入

JP1/IT Desktop Management 2 で管理するコンピュータには、エージェントを導入します。

エージェントを導入することで、コンピュータが自動的に管理対象になり、機器情報が収集されるようになります。これによって、次のような管理ができるようになります。

セキュリティ状況の把握

セキュリティポリシーを割り当てて、コンピュータのセキュリティ状況を判定できます。また、セキュリティに問題があった場合には、自動的に対策できます。

資産の管理

コンピュータが管理対象になることで、自動的にハードウェア資産情報が登録されます。機器から収集された情報は自動的に資産情報にも反映されるので、機器から収集されない資産管理番号や利用者情報などとあわせて、組織内のハードウェア資産を最新状態で管理できます。また、ソフトウェアライセンスの利用状況も把握できます。

ソフトウェアやファイルの配布

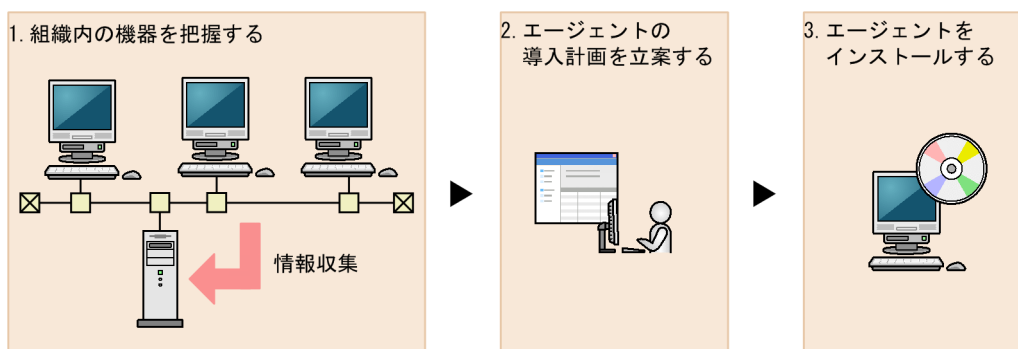
エージェントを導入したコンピュータには、管理用サーバからソフトウェアを配布してインストールしたり、ファイルを配布したり、ソフトウェアをアンインストールしたりできます。このため、組織内で利用するソフトウェアを効率良く保守できます。

JP1/IT Desktop Management 2 を利用して組織内の機器を管理する場合、すべて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ます。

ポイント

コンピュータ以外の機器を管理する場合は、エージェントを導入しないで管理対象にします。

コンピュータにエージェントを導入する流れを次の図に示します。



1. 組織内の機器を把握する

エージェントを導入する対象を決定するために、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、JP1/IT Desktop Management 2 を利用して機器を探索してください。

なお、Active Directory を使ってすべてのコンピュータを管理している、管理台帳が最新状態にメンテナンスされているなど、組織内の機器を把握できている場合はこの手順は不要です。

2. エージェントの導入計画を立案する

組織内の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。

JP1/IT Desktop Management 2 では、エージェントのインストーラーを利用してインストールする方法と、エージェントを配信して自動的にインストールする方法があります。

3. エージェントをインストールする

導入計画に従って、エージェントをインストールします。

また、エージェントを導入しない（エージェントレス）で機器を管理することもできます。この場合、エージェントレスのコンピュータに対しても、コンピュータの詳細情報の取得やセキュリティポリシーの適用、セキュリティ状況の判定、セキュリティ診断レポートの作成などを実行できます。

ただし、セキュリティポリシーによる自動対策やメッセージの通知機能、ソフトウェアやファイルの配布機能など、一部の機能が利用できません。

関連リンク

- [1.1.1 組織内の機器を把握する](#)
- [\(4\) エージェントの導入計画を立案する](#)
- [1.1.2 エージェントを手動でインストールする](#)
- [1.1.3 エージェントを自動でインストールする](#)
- [1.1.4 エージェントのインストール状況を確認する流れ](#)

1.1.1 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、JP1/IT Desktop Management 2 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

- [\(4\) エージェントの導入計画を立案する](#)

(1) 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

- [15.2.2 探索条件を設定する手順 \(Active Directory の探索\)](#)
- [15.2.4 機器の探索状況の確認](#)

(2) 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すため、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

- 15.2.1 探索条件を設定する手順（ネットワークの探索）
- 15.2.4 機器の探索状況の確認

(3) ネットワーク監視機能による機器の検知

機器画面の「機器情報」－「機器一覧（ネットワーク）」画面に表示される各ネットワークセグメントのグループで、ネットワークモニタを有効にすると、新規にネットワークに接続しようとした機器を検知できます。検知された機器には、自動的にネットワークの探索が実行されます。発見された機器は、ネットワークモニタ設定に従って、ネットワーク接続が制御されます。

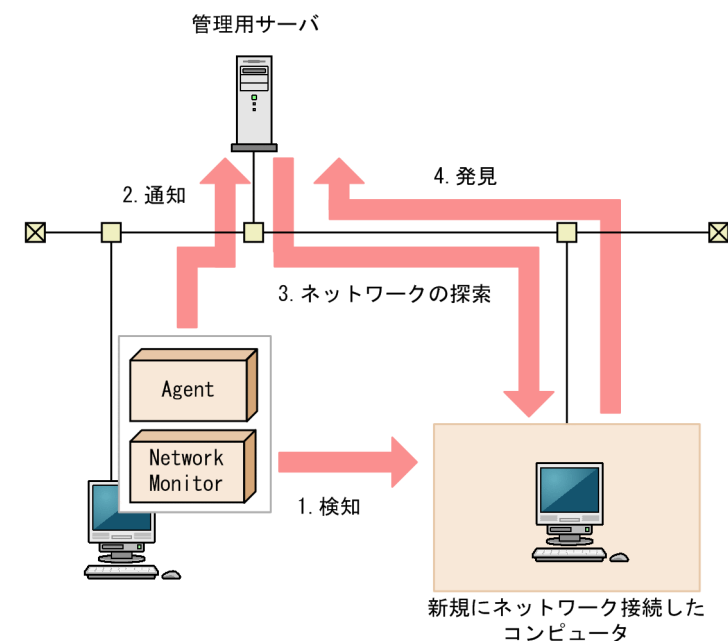
注意事項

ネットワークモニタ機能は、ネットワーク接続を許可する機器、および許可しない機器を十分に確認してから使用してください。ネットワークへの接続を制御する方法を誤ると、業務に使用している機器の接続が遮断されるなど、トラブルにつながるおそれがあります。

ポイント

機器を検知するためには、1つのネットワークセグメントに対して1台のエージェント導入済みコンピュータのネットワークモニタを有効にしてください。複数のネットワークカードを使って複数のネットワークに接続できるコンピュータであれば、ネットワークモニタを有効にしたエージェント導入済みコンピュータ1台で、複数のネットワークセグメントを監視できます。また、ネットワークセグメントの範囲の探索範囲を設定し、認証情報を対応づけてください。なお、探索範囲に含まれないネットワークアドレスで機器が検知された場合、認証情報を使用しない探索が実行されるため、MACアドレスとIPアドレスの情報だけ取得されます。

ネットワークに接続した機器を検知し、JP1/IT Desktop Management 2に登録する仕組みについて次の図に示します。



(凡例)

Agent : エージェント

Network Monitor : ネットワークモニタエージェント

1. 機器がネットワークに接続しようとする時、ネットワークモニタが有効になったエージェント導入済みのコンピュータが、その機器を検知します。
2. ネットワークモニタが有効になったエージェント導入済みのコンピュータから機器を検知したことが管理用サーバに通知されます。
3. 通知された情報を基に、その機器に対してネットワークの探索を実行します。

ポイント

発見時にエージェントレスの認証をしたい場合は、ネットワークモニタによって監視される IP アドレスを含む探索範囲と認証情報をあらかじめ設定してください。

4. 探索の結果、発見された機器は、探索条件によって自動的に管理対象になったりエージェントが自動配信されたりします。

注意事項

NAT を経由したネットワークなど、管理用サーバから直接通信できないネットワークセグメントは、ネットワークモニタ機能を利用しても機器を検知できません。

注意事項

ネットワークの探索で発見した機器に、自動でエージェントを配信するように設定している場合、発見されたコンピュータがネットワーク接続を許可されなくても、そのコンピュータにエージェントは配信されます。

このため、ネットワーク接続が許可されないコンピュータにエージェントが導入された場合、セキュリティポリシーのネットワーク制御の設定およびセキュリティの判定結果によっては、そのコンピュータがネットワーク接続できてしまうことがあります。

注意事項

ネットワークモニタ機能によって発見された機器を削除した場合、ネットワークをいったん切断して再接続しないと、その機器は再発見できません。また、ネットワークを切断してから再接続するまでの時間が短か過ぎた場合、機器を再発見できないことがあります。

ポイント

ネットワークモニタ設定が許可する/許可しないのどちらの設定でも、ネットワーク接続した機器を発見できます。ネットワークモニタによって発見された機器には、自動的にネットワークの探索が実行されます。このため、ネットワークの探索で、自動的に管理対象とする、またはエージェントを自動配信するよう設定されている場合は、ネットワークモニタによって機器が発見されると、自動的に管理対象になるか、エージェントが自動配信されます。この場合、機器が管理対象になって、製品ライセンスが消費されます。

自動で管理対象にしたいくない場合は、探索条件の設定で「自動的に管理対象とする」および「エージェントを自動配信する」のチェックを外して、手動で管理対象にするようにしてください。

ネットワーク監視機能の監視対象は次のとおりです。

- 監視対象のネットワークは IPv4 だけです。IPv6 には対応していません。
- 監視対象となるコンピュータの OS は、次のとおりです。これら以外の OS のコンピュータについては、標準 TCP/IP を使用している場合に限り、監視対象となります。
 - Windows 95
 - Windows 98
 - Windows Me
 - Windows XP
 - Windows NT 3.51 および 4.0
 - Windows 2000

- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2012
- Windows 8
- Windows 8.1
- 監視対象となるプロトコルは、TCP/IP のネットワークです。NetBEUI や IPX などには対応していません。
- 無線 LAN に接続したネットワーク接続機器を制御する場合は、MAC アドレスの情報を中継するアクセスポイントとしてください。MAC アドレスの情報を中継しない場合、ネットワーク制御はできません。

(4) 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、JP1/IT Desktop Management 2 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 JP1/IT Desktop Management 2 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 JP1/IT Desktop Management 2 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

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

1.1.2 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、「[6.2 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。

- (3) Web サーバでエージェントを公開する
- (4) ファイルサーバでエージェントを公開する
- (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
- (6) メールの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。

- (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。

- (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) 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、[次へ] 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。

コンポーネントの設定

インストールするコンポーネントの種別（エージェントとしてインストールするか、中継システムとしてインストールするかを選択）とサブコンポーネントのリモコンエージェントをインストールするかどうかを指定します。

登録先の ID の設定

エージェントを登録する ID（配布管理システムからのジョブを受け取るためのグループ）を指定します。

展開するファイルの設定

エージェントのインストールと同時に展開するファイルと展開先のフォルダを指定します。

自動実行するファイルの設定

エージェントのインストール後に自動実行するファイル、自動実行に必要なファイル、および引数を指定します。

上書きインストールの設定

エージェントがすでにインストールされている場合、上書きインストールするかどうかを設定します。

4. 設定内容を確認して、[作成] ボタンをクリックします。

インストールセットをダウンロードするダイアログが表示されます。

5. 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「ITDM2Agt.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。

ポイント

上位接続先情報ファイル (dmhost.txt) を作成して、JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておくと、インストールセットの作成時にインストールセットに取り込

まれます。上位接続先情報ファイルの詳細については、マニュアル「JP1 Version 10 JP1/IT Desktop Management 2 配布機能 運用ガイド」の、エージェントの接続先の自動変更についての説明を参照してください。

関連リンク

- [15.1.2 エージェント設定を追加する手順](#)
- [\(2\) エージェントをコンピュータに導入する方法](#)

(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

- [\(3\) Web サーバでエージェントを公開する](#)

- (4) ファイルサーバでエージェントを公開する
- (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
- (6) メール添付ファイルでエージェントを配布する
- (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
- (8) ディスクコピーでエージェントをインストールする

(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

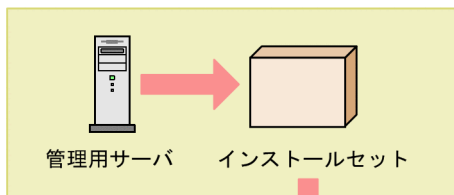
利用者にサイトの URL を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。また、Web システムを利用するので、アクセス制御しなくてもサーバ側にセキュリティ上の問題が発生しません。

デメリット

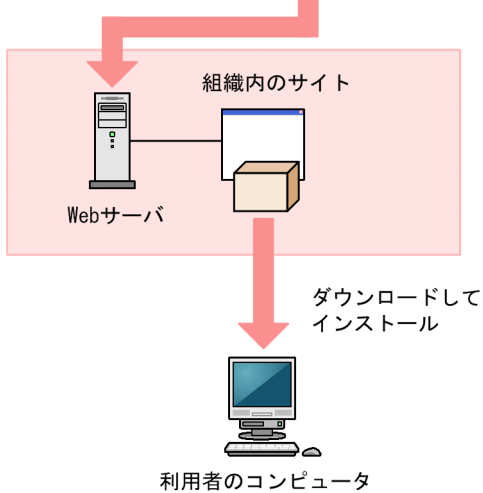
組織内に Web サーバを構築できる環境、および Web サーバにアクセスできる環境が必要です。

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

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

(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

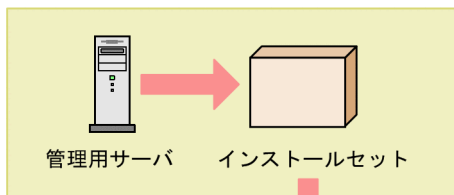
利用者にインストールセットの格納先を一斉展開することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

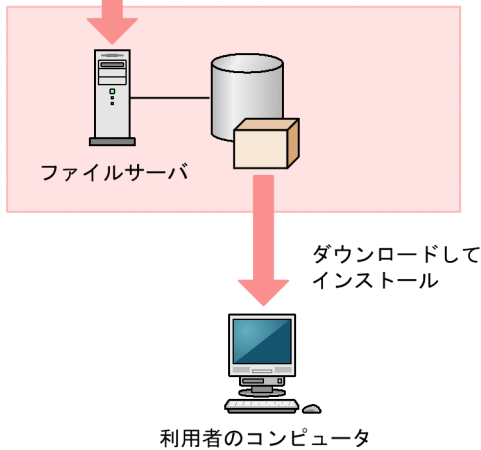
ファイル共有できる環境が必要です。また、ファイル共有の参照先を公開するため、公開の範囲や権限などサーバ側で確実にアクセス制御をしておく必要があります。

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

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

(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

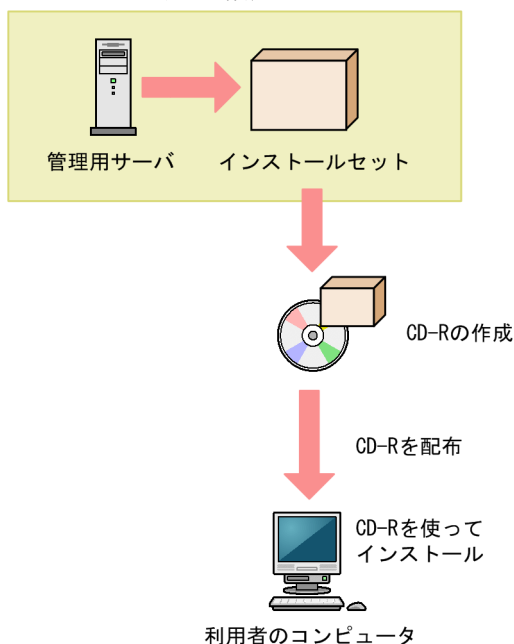
Web ページにセキュリティ管理用のページを作成したり、共有フォルダの環境を作成したりする必要がありません。この方法は、エージェントをインストールするコンピュータの台数が少ない場合に有効です。また、ネットワークの通信速度が遅い場合に、ネットワークに負荷をかけないでエージェントをインストールできます。利用者のコンピュータを構築するユーザー専用機に、エージェントのプログラムを保持できることにもなります。

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「ITDM2Agt.exe」の場合の Autorun.inf の作成例は次のとおりです。

```
[Autorun]
```

```
open=ITDM2Agt.exe
```

関連リンク

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

(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

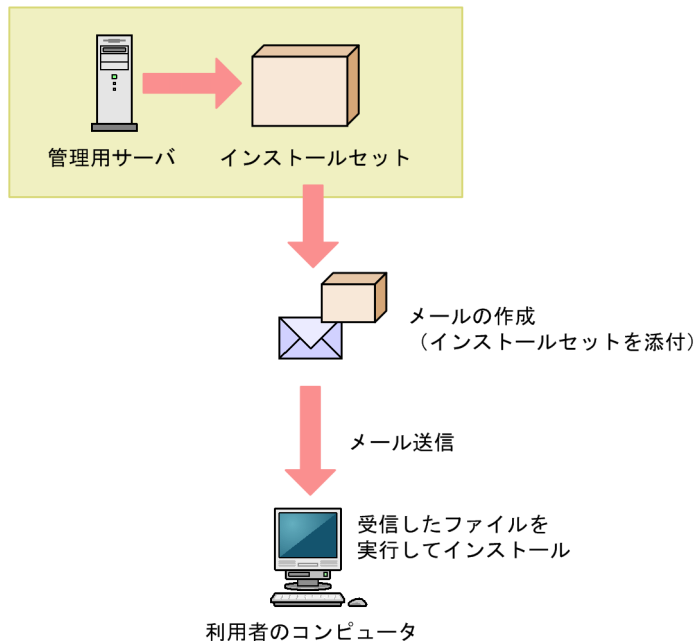
利用者にメールを一斉送信することで、多くのコンピュータに素早くエージェントをインストールできます。

デメリット

インストールセットの容量は、最小約 70 メガバイトで、設定に応じて増減します。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

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

(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¥jplitdma¥bin¥jdnnglogon.exe" (  
start /w ¥¥サーバ名¥共有フォルダ名¥ITDM2Agt.exe  
)  
) else (  
if not exist "%ProgramFiles%¥Hitachi¥jplitdma¥bin¥jdnnglogon.exe" (  

```

```
start /w %¥¥サーバ名¥共有フォルダ名¥ITDM2Agt.exe
)
)
```

メリット

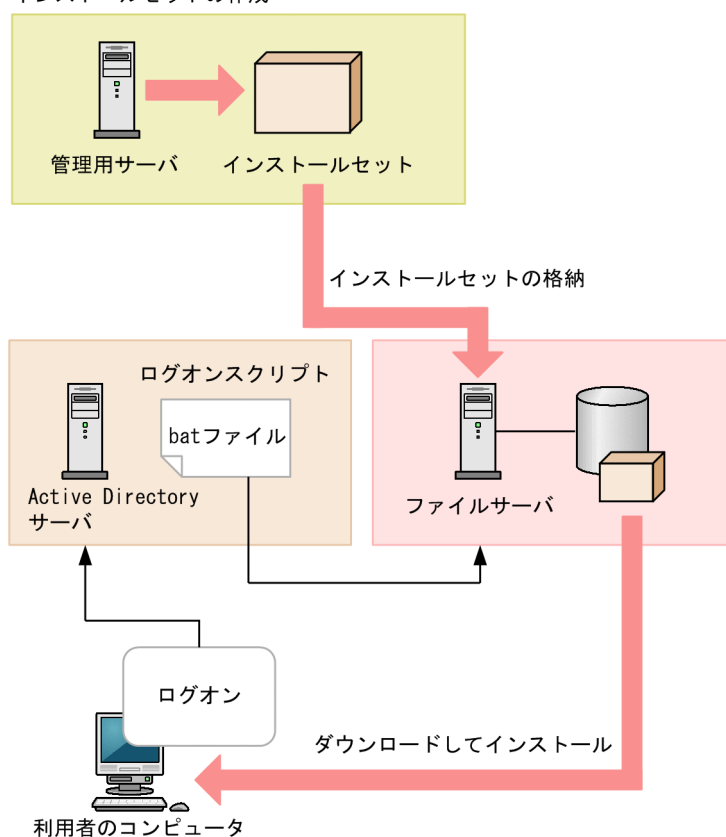
ログオンスクリプトを利用することで、利用者に作業してもらうことなくエージェントを自動的にインストールできます。そのため、利用者の操作ミスによるトラブルを避けられます。

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

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

(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

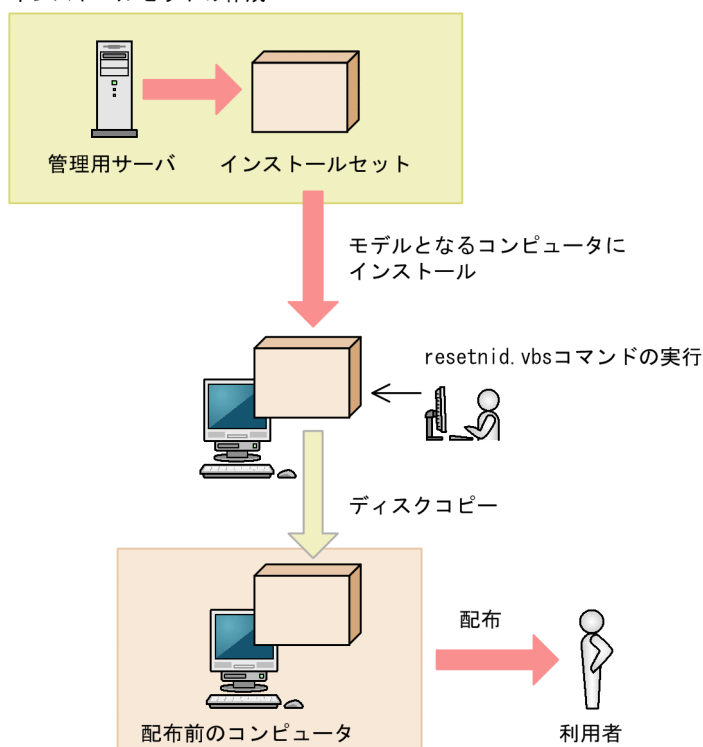
配布する時点でエージェントのインストールおよびセットアップがすでに完了しているため、利用者がエージェントをインストールする必要がありません。そのため、利用者の操作ミスによるトラブルを避けられます。

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

- 6.2 インストールセットを作成する手順

- 1.1.4 エージェントのインストール状況を確認する流れ
- 17.28 resetnid.vbs (ホスト識別子のリセット)

1.1.3 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) 探索と同時にエージェントを自動配信する手順 (Active Directory 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。Active Directory 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 70 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。インストールセットの容量は、設定に応じて増減します。

探索と同時にエージェントを自動配信するには (Active Directory の探索) :

1. 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。
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。

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。

(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 70 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。インストールセットの容量は、設定に応じて増減します。

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。

(3) 探索と同時にエージェントを自動配信する手順（機器のネットワーク接続の監視）

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。ネットワークモニタ機能によって実行される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 30 メガバイトのデータが送信されます。

探索と同時にエージェントを自動配信するには（機器のネットワーク接続の監視）：

ネットワーク接続の監視中に新規接続された機器が検知されると、検知された機器に対して、自動的に探索が実行されます。このとき、発見した機器にエージェントを自動配信するには、次の 2 種類の設定が必要になります。

- 新規接続された機器のネットワーク接続を許可する
- ネットワークの探索で、探索と同時にエージェントを自動配信するように設定する

新規接続された機器のネットワーク接続を許可する

1. 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] 画面を表示します。
2. エージェントを自動配信したいネットワークセグメント (パス) を選択します。
3. [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、[発見した機器への動作] に「ネットワークへの接続を許可する」が設定されているネットワークモニタ設定を選択します。
なお、デフォルトで準備されている「(標準設定)」は、「ネットワークへの接続を許可する」が設定されています。
5. [OK] ボタンをクリックします。

対象のネットワークセグメントで新規接続した機器が検知されると、自動的にネットワーク接続が許可され、探索が実行されます。

ネットワークの探索で、探索と同時にエージェントを自動配信するように設定する

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ます。

検知された機器に対して探索が実行されると、発見した機器に自動的にエージェントが配信されます。

(4) 機器の探索状況の確認

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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

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

(5) 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。

(6) 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

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

(7) 管理対象の機器を確認する手順

JP1/IT Desktop Management 2 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

- [15.2.8 除外対象の機器を確認する手順](#)

(8) 除外対象の機器を確認する手順

JP1/IT Desktop Management 2 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

- [15.2.7 管理対象の機器を確認する手順](#)

(9) 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 70 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せん。

1.1.4 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

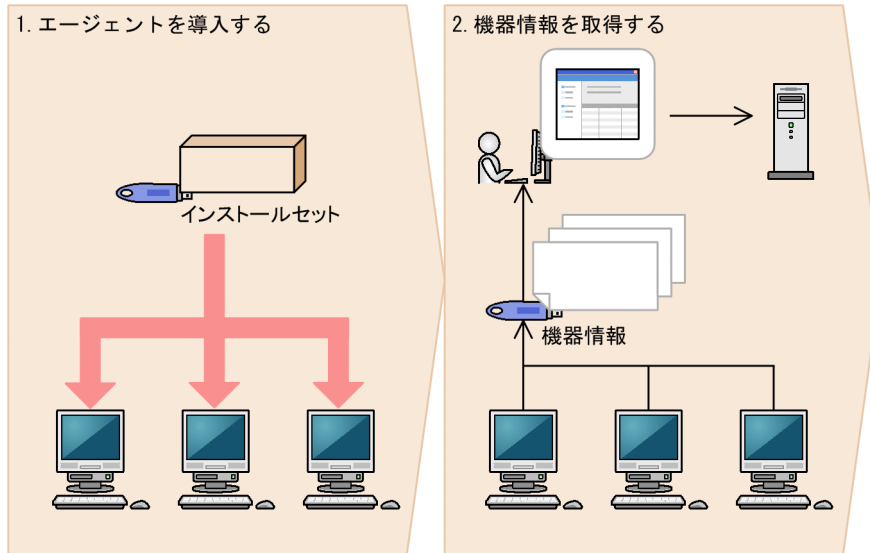
手持ちの管理台帳とエクスポートしたコンピュータの一覧を比較します。このとき、エクスポートした一覧にないコンピュータが、エージェントをインストールしていないコンピュータになります。

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。

1.2 機器をオフラインで管理する

JP1/IT Desktop Management 2 のオフライン管理機能を利用すると、管理用サーバに接続していないコンピュータを、オンライン管理のコンピュータと同様に管理できます。

機器をオフラインで管理する流れを次に示します。



(凡例)

——→ : 機器情報の流れ

1. エージェントを導入する

JP1/IT Desktop Management 2 でコンピュータをオフライン管理するために、オフライン管理用のエージェント設定を作成します。そのあと、インストールセットを作成し、外部記憶媒体を利用してコンピュータにインストールします。

2. 機器情報を取得する

機器情報を取得するために、エージェントを導入したコンピュータから、機器情報を収集します。そのあと、収集した機器情報を管理用サーバに通知します。機器情報を取得する方法には、次の 2 種類があります。

- 外部記憶媒体を利用して取得する方法
スタンドアロンのコンピュータの機器情報を取得する場合や、オフライン管理のコンピュータの台数が少ない場合に有効な方法です。
- ログオンスクリプトを利用して取得する方法
拠点内のネットワークに接続しているコンピュータの機器情報を取得する場合や、オフライン管理のコンピュータの台数が多い場合に有効な方法です。

エージェントを導入するための外部記憶媒体と、機器情報を取得するための外部記憶媒体をそれぞれ用意しておくことで、エージェントを導入したあとに、続けて機器情報を取得できます。

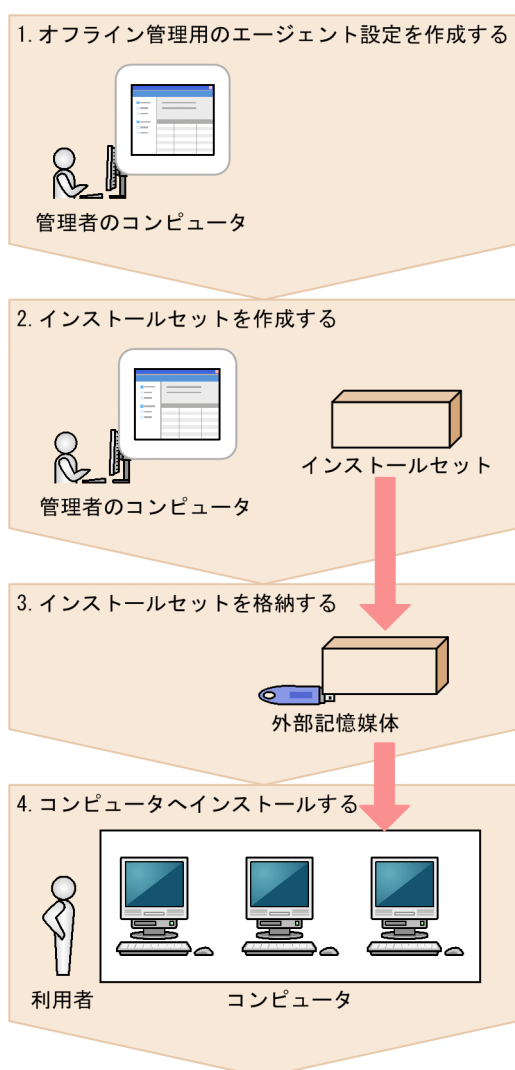
関連リンク

- 1.2.1 オフライン管理したいコンピュータにエージェントを導入する流れ
- 1.2.2 外部記憶媒体を利用してオフライン管理のコンピュータから機器情報を取得する流れ
- 1.2.3 ログオンスクリプトを利用してオフライン管理のコンピュータから機器情報を取得する流れ

1.2.1 オフライン管理したいコンピュータにエージェントを導入する流れ

JP1/IT Desktop Management 2 でコンピュータをオフライン管理するためには、まずオフライン管理用のエージェント設定を作成します。そのあと、インストールセットを作成し、外部記憶媒体を利用してコンピュータにインストールします。

オフライン管理したいコンピュータにエージェントを導入する流れを次の図に示します。



1. オフライン管理用のエージェント設定を作成する

システム管理者が、設定画面のエージェント設定で、[基本設定] – [上位システムと通信する] のチェックを外したエージェント設定を作成します。

2. インストールセットを作成する

オフライン管理用のエージェント設定のインストールセットを作成して、管理者のコンピュータにダウンロードします。

3. インストールセットを格納する

インストールセットを外部記憶媒体に格納して、利用者に渡します。

4. コンピュータへインストールする

利用者は、オフライン管理したいコンピュータに外部記憶媒体を接続して、インストールセットを実行してエージェントをインストールします。オフライン管理したいすべてのコンピュータに対して、同じ外部記憶媒体を利用してこの手順を実施します。

コンピュータへのエージェントの導入が完了します。エージェントの導入が完了したら、オフライン管理のコンピュータから機器情報を取得して、JP1/IT Desktop Management 2 の管理対象にします。

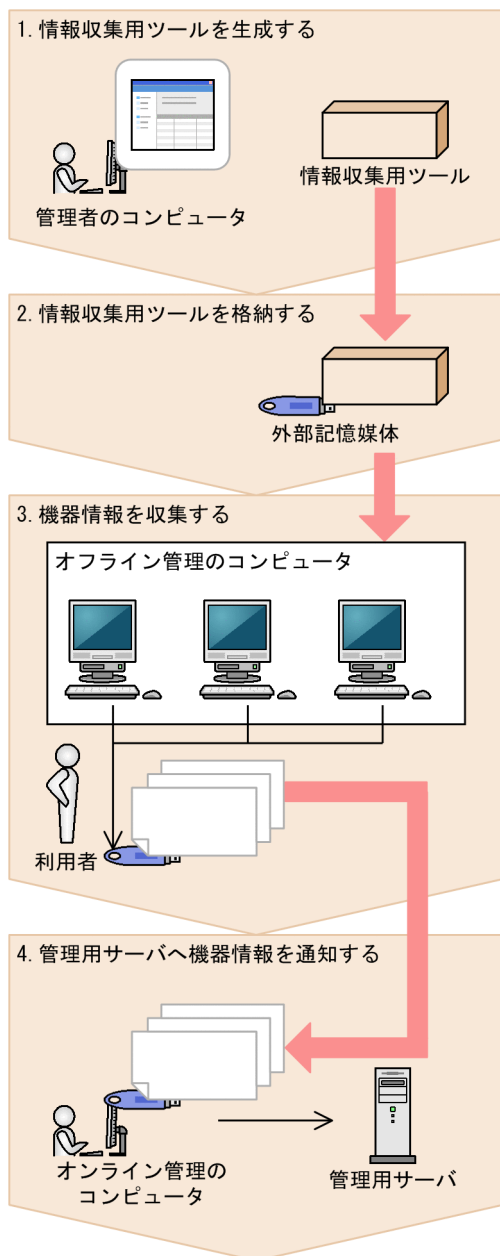
ポイント

オフライン管理とオンライン管理を頻繁に切り替えるコンピュータにエージェントを導入する場合は、ほかのオフライン管理のコンピュータに適用するエージェント設定とは別に、専用のエージェント設定を用意することをお勧めします。切り替えるときに、エージェント設定を変更する必要があるためです。

1.2.2 外部記憶媒体を利用してオフライン管理のコンピュータから機器情報を取得する流れ

オフライン管理のコンピュータからは、外部記憶媒体を利用して機器情報を取得します。

オフライン管理のコンピュータから機器情報を取得する流れを次の図に示します。



(凡例)

→ : 機器情報の流れ

1. 情報収集用ツールを生成する

システム管理者が、[機器一覧] 画面で [操作メニュー] の [情報収集用ツールを生成する] を選択して、情報収集用ツールを生成します。情報収集用ツールは、ZIP 形式で圧縮されています。

2. 情報収集用ツールを格納する

情報収集用ツールを解凍して外部記憶媒体に格納し、利用者に渡します。

3. 機器情報を収集する

利用者は、オフライン管理のコンピュータに外部記憶媒体を接続して、機器情報を収集します。機器情報を収集したいすべてのコンピュータに対して、同じ外部記憶媒体を利用してこの手順を実施します。機器情報の収集が完了したら、利用者はシステム管理者に外部記憶媒体を渡します。

4. 管理用サーバへ機器情報を通知する

システム管理者は、オンライン管理のコンピュータに外部記憶媒体を接続して、収集した機器情報を管理用サーバに通知します。

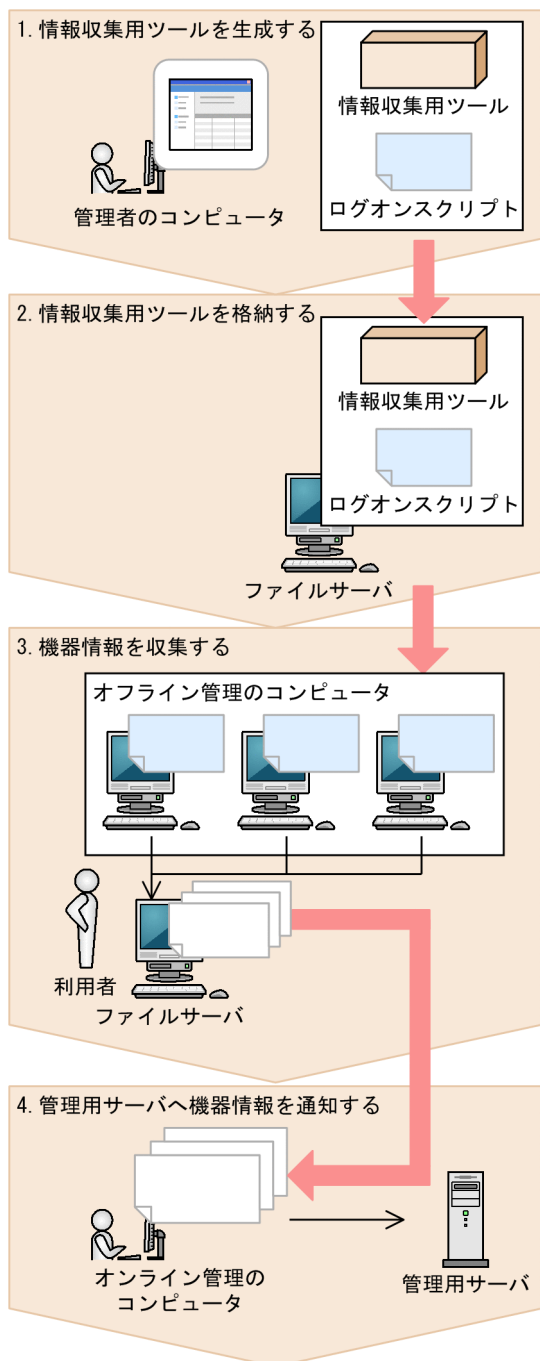
オフライン管理のコンピュータの機器情報の取得が完了します。

1.2.3 ログオンスクリプトを利用してオフライン管理のコンピュータから機器情報を取得する流れ

オフライン管理のコンピュータからは、ログオンスクリプトを利用して機器情報を取得することもできます。

オフライン管理のコンピュータの機器情報を取得する流れを次の図に示します。

なお、ログオンスクリプトを利用して機器情報を取得するには、各オフライン管理のコンピュータが、ファイルサーバの共有フォルダにアクセスする必要があります。



1. 情報収集用ツールを生成する

システム管理者が、[機器一覧] 画面で [操作メニュー] の [情報収集用ツールを生成する] を選択して、情報収集用ツールを生成します。情報収集用ツールは、ZIP 形式で圧縮されています。

そのあと、情報収集用ツールとログオンスクリプトを利用者に渡します。

2. 情報収集用ツールを格納する

利用者は、情報収集用ツールを解凍してファイルサーバの共有フォルダに格納します。また、ログオンスクリプトを各オフライン管理のコンピュータに配布します。

3. 機器情報を収集する

オフライン管理のコンピュータで Windows にログオンしたときに、自動的に機器情報が収集されます。機器情報の収集が完了したら、利用者は収集した機器情報をシステム管理者に渡します。

4. 管理用サーバへ機器情報を通知する

システム管理者は、オンライン管理のコンピュータから、オフライン管理のコンピュータの機器情報を管理用サーバに通知します。

オフライン管理のコンピュータの機器情報の取得が完了します。

■ ポイント

オフライン管理のコンピュータに配布するログオンスクリプトは、次のような内容で作成してください。

1. ファイルサーバの共有フォルダを、ネットワークドライブに割り当てる。
2. 共有フォルダから情報収集用ツールをコピーする。
3. `getinv.vbs` コマンドを実行する。
4. 収集した機器情報を共有フォルダにコピーする。
5. ネットワークドライブを切断する。

1.3 複数の管理者で業務を分担する流れ

システム管理者 1 人で社内全体の機器やハードウェア資産を管理している場合、従業員、分散拠点などの増加に伴い、管理が行き届かなくなることがあります。

このような場合、担当業務や部門ごとに別の管理者を配置してシステム管理の業務を分担すれば、社内全体の管理が行き届くようになります。各管理者のユーザーアカウントに権限、業務分掌、または管轄範囲を設定することで、各管理者は設定された範囲だけの情報を管理できるようになります。

システム管理者は、社内全体の機器やハードウェア資産の管理状況を確認して、必要に応じて各管理者に指示を出します。これによって、システム管理者の作業を軽減したり、社内全体の機器、ハードウェア資産などを円滑に管理したりできるようになります。

複数の管理者で作業を分担する流れを次に示します。

1.各管理者の担当業務を検討する

組織の構成や規則を基に、各管理者の担当業務を検討します。

2.各管理者が使用するユーザーアカウントを登録する

各管理者の担当業務に応じたユーザーアカウントを登録します。

3.複数の管理者で連携して業務を進める

各管理者は、担当業務に関係する情報が表示される画面を参照して管理します。

システム管理者は、社内全体の管理情報が表示される画面を参照して管理します。

1.3.1 ユーザーアカウントの設定内容を検討する流れ

組織内の従業員や分散拠点などが多く、社内全体の機器やハードウェア資産を 1 人のシステム管理者では管理できない場合、複数の管理者でシステム管理の業務を分担できます。また、各管理者のユーザーアカウントに権限、業務分掌、または管轄範囲を設定することで、各管理者は設定された範囲だけの情報を管理できるようになります。

ユーザーアカウントの権限、業務分掌、および管轄範囲の設定内容を検討する流れを次に示します。

1.各管理者の担当業務を決定する

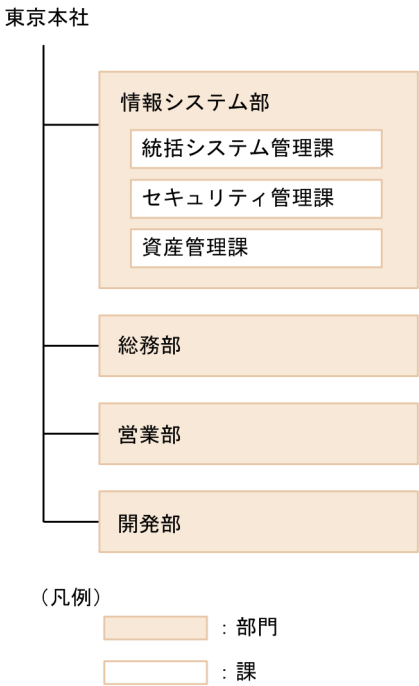
システム管理の業務のうち、どの業務を誰に担当させるかを決定します。例えば、システム管理の業務には、セキュリティポリシーの作成と割り当て、機器の管理、ソフトウェアライセンスの管理、ソフトウェアの配布、ユーザーアカウントの管理など、さまざまな業務があります。これらの業務を「セキュリティポリシーの作成と割り当てはセキュリティ課の B さんに担当させる」というように、各管理者に割り振ります。

2.ユーザーアカウントの設定内容を決定する

各管理者の担当業務を基に、ユーザーアカウントの設定内容を決定します。ユーザーアカウントに設定した権限、業務分掌、および管轄範囲の組み合わせによって、各管理者の操作範囲を限定できます。

ユーザーアカウントの設定例

ここでは、次の図に示す構成の組織を前提に説明します。



各管理者の担当業務と、それを基に決定したユーザーアカウントの設定例を、次の表に示します。

管理者名	情報システム部での所属	担当業務	ユーザーアカウントの設定内容		
			権限	業務分掌	管轄範囲
管理者A	統括システム管理課	- システム管理の取りまとめ - ユーザーアカウントの管理	- システム管理権限 - ユーザーアカウント権限	全業務分掌	全部門
管理者B	セキュリティ管理課	- セキュリティポリシーの作成と割り当て - セキュリティ対策 - 更新プログラムの配布 - ソフトウェアの配布	システム管理権限	- セキュリティ管理 - 資産管理 - 機器管理 - 配布管理	全部門
管理者C	資産管理課	- ハードウェア資産の購入、リプレイス、廃棄 - ソフトウェアライセンスの購入、移管、滅却 - 資産情報および契約情報の登録 - ソフトウェアライセンスの過不足の管理と対策	システム管理権限	- 資産管理 - 機器管理	情報システム部
管理者D		- ハードウェア資産の購入、リプレイス、廃棄 - ソフトウェアライセンスの購入、移管、滅却 - 資産情報および契約情報の登録 - ソフトウェアライセンスの過不足の管理と対策	システム管理権限	- 資産管理 - 機器管理	総務部

管理者名	情報システム部での所属	担当業務	ユーザーアカウントの設定内容		
			権限	業務分掌	管轄範囲
管理者 E	資産管理課	- ハードウェア資産の購入、リプレイス、廃棄 - ソフトウェアライセンスの購入、移管、滅却 - 資産情報および契約情報の登録 - ソフトウェアライセンスの過不足の管理と対策	システム管理権限	- 資産管理 - 機器管理	営業部
管理者 F		- ハードウェア資産の購入、リプレイス、廃棄 - ソフトウェアライセンスの購入、移管、滅却 - ソフトウェアライセンスの過不足の管理と対策	システム管理権限	- 資産管理 - 機器管理	開発部
管理者 G		資産情報および契約情報の登録	システム管理権限	資産管理	

例えば、管理者 A の場合は、システム管理の取りまとめやユーザーアカウントの管理など、システム全体の管理業務を担当します。そのため、ユーザーアカウントの設定では、権限、業務分掌、管轄範囲を限定しないようにします。一方、管理者 G の場合は、開発部の資産管理業務だけを担当します。そのため、ユーザーアカウントの設定では、権限を「システム管理権限」に、管轄範囲を「開発部」に限定します。また、開発部は規模が大きいため、管理者 G は管理者 F と担当業務を分担して資産情報および契約情報の登録だけを担当します。そのため、業務分掌は資産情報および契約情報の登録に必要な「資産管理」に限定します。

1.3.2 複数のユーザーアカウントを登録する流れ

JP1/IT Desktop Management 2 では、担当業務や部門に応じて複数のユーザーアカウントを登録できます。複数のユーザーアカウントを登録しておけば、従業員や分散拠点などが多く、社内全体の機器やハードウェア資産を 1 人のシステム管理者では管理できない場合に、複数の管理者でシステム管理の業務を分担できます。また、各管理者の操作範囲を担当業務や部門ごとに制限できるため、内部統制を意識した管理ができます。

複数のユーザーアカウントを登録する流れを次に示します。

1. ユーザーアカウントの登録情報の連絡を受ける

システム管理者は、各管理者からユーザーアカウントの登録に必要な情報（氏名、業務内容、所属する部門、メールアドレスなど）の連絡を受けます。

2. JP1/IT Desktop Management 2 にユーザーアカウントを登録する

システム管理者は、設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面で、ユーザーアカウントを登録します。このとき、各管理者の担当業務や所属する部門を基にして、ユーザーアカウントに権限、業務分掌、または管轄範囲を設定します。

3. ユーザーアカウントの登録が完了したことを連絡する

システム管理者は、各管理者に、JP1/IT Desktop Management 2 にログインするためのユーザー ID とパスワードをメールで通知します。

各管理者は、連絡されたユーザーアカウントで操作画面にログインすると、ユーザーアカウントに設定された範囲の情報だけを管理できます。

関連リンク

- [4.1 ユーザーアカウントを追加する手順](#)

1.3.3 複数の管理者で連携して業務を進める流れ

ユーザーアカウントに業務分掌または管轄範囲が設定されている場合、設定の内容に応じて操作画面の表示範囲が限定されます。これによって、複数の管理者が自分の担当業務や部門に関する情報だけを管理できます。

例えば、棚卸時期になると、システム管理者の作業負担が増大してしまうような場合、部門ごとに資産管理者を配置して作業することで、棚卸の作業負担を軽減できます。

部門ごとにハードウェア資産の棚卸を分担する流れを次に示します。

1. システム管理者は、各部門の資産管理者に、ハードウェア資産を棚卸するように連絡する

システム管理者は、各部門の資産管理者に、棚卸作業の指示と手順をメールで連絡します。

また、締め切り日までに棚卸を完了するように指示します。

2. 各部門の資産管理者は、担当する部門のハードウェア資産を棚卸する

各部門の資産管理者は、JP1/IT Desktop Management 2 にログインします。資産画面の [ハードウェア資産] 画面の一覧には、管轄範囲のハードウェア資産だけが表示されます。表示された一覧を CSV ファイルにエクスポートして印刷します。

一覧を基に現品確認したあと、エクスポートした CSV ファイルに棚卸結果を入力して、JP1/IT Desktop Management 2 にインポートします。その部門のハードウェア資産の棚卸日時が更新されます。

3. システム管理者は、更新日時を確認する

締め切り日の翌日に、資産画面の [ハードウェア資産] 画面の一覧の更新日時から、社内全体の棚卸が完了しているかどうか確認します。

更新されていない部門がある場合は、メールで各部門の資産管理者に連絡します。

社内全体の棚卸が完了します。

1.4 スマートデバイスを管理する

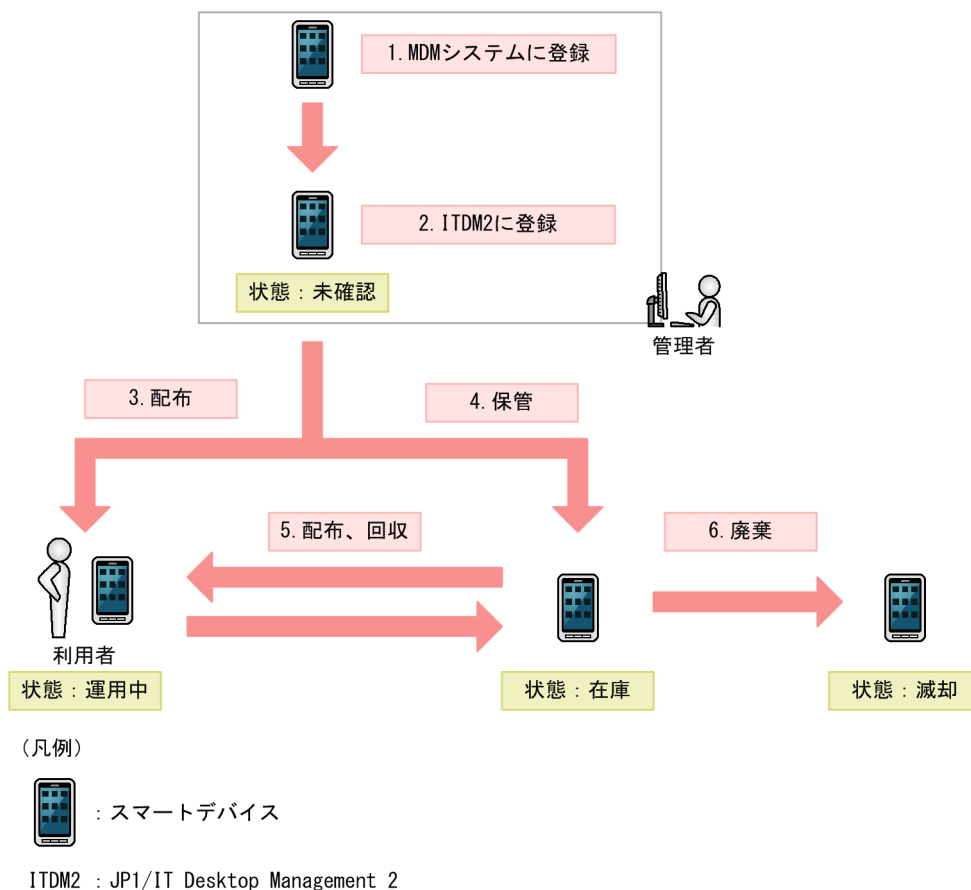
スマートデバイスの普及が進み、業務に利用するためにスマートデバイスを導入する企業が増えています。スマートデバイスの導入によって業務の効率化が期待される反面、情報漏えいのリスクが高まります。情報漏えいやスマートデバイスの盗難および紛失に対応するために、ほかの社内資産と同様にスマートデバイスを管理する必要があります。

JP1/IT Desktop Management 2 の MDM 連携機能を利用すると、次に示すように効率良くスマートデバイスを管理できます。

- 組織内のコンピュータ、サーバ、プリンタ、ネットワーク装置、USB デバイスなどと同様に、スマートデバイスを JP1/IT Desktop Management 2 で一元管理できる
- JP1/IT Desktop Management 2 で管理対象にしたスマートデバイスの機器情報、資産情報、およびセキュリティを管理できる
- JP1/IT Desktop Management 2 からスマートデバイスのロック、初期化およびパスコードのリセットができる

スマートデバイスの管理は、機器画面、資産画面および設定画面で実行します。スマートデバイスを管理するためには、MDM システムからスマートデバイスの情報を取得するよう設定して、JP1/IT Desktop Management 2 でスマートデバイスを管理対象にします。

スマートデバイスを管理する流れを次の図に示します。



スマートデバイスをMDMシステムに登録したら、JP1/IT Desktop Management 2でスマートデバイスを管理対象にします。その後、スマートデバイスを利用者に配布します。スマートデバイスを利用しない場合は在庫として保管しておきます。貸し出しやリプレイスなどの運用に応じて、運用中のスマートデバイスを回収したり、在庫のスマートデバイスを貸し出したりします。スマートデバイスが不要になった場合は、滅却処理をして廃棄します。

ここでは、次に示す業務でのJP1/IT Desktop Management 2の利用方法を説明します。

スマートデバイスの管理を始める

スマートデバイスの利用を開始する場合、購入したスマートデバイスをJP1/IT Desktop Management 2で管理できるようにしてから、利用者に配布します。

スマートデバイスをリプレイスする

従業員の異動やスマートデバイスの入れ替えに伴って組織内のスマートデバイスをリプレイスする場合、JP1/IT Desktop Management 2でリプレイス対象のスマートデバイスを調査して、スマートデバイスを配布・回収します。

スマートデバイスの利用者を変更する

従業員の異動に伴ってほかの利用者にスマートデバイスを引き継ぐ場合に、スマートデバイスの利用者を変更します。

スマートデバイスの紛失に対応する

スマートデバイスを紛失したときに、セキュリティ対策のためにスマートデバイスをロックしたり、初期化したりします。

利用者がスマートデバイスのパスコードを忘れた場合に対処する

スマートデバイスのパスコードをリセットします。連続してパスコードを間違えて、スマートデバイスが初期化されてしまった場合は、再びMDMシステムにスマートデバイスを登録し、JP1/IT Desktop Management 2 で管理対象にします。

スマートデバイスを滅却する

リプレイスや修理などに伴ってスマートデバイスを回収した場合に、古くなったり壊れたりして今後使用しないものがあるときは、スマートデバイスを滅却します。

1.4.1 スマートデバイスの管理を始める流れ

スマートデバイスの利用を開始する場合、購入したスマートデバイスを JP1/IT Desktop Management 2 で管理できるようにしてから、利用者に配布します。

スマートデバイスの管理を始める流れを次に示します。

1.MDM システムを導入する

JP1/IT Desktop Management 2 でスマートデバイスの管理を始めるために、MDM システムを導入し、スマートデバイスを登録します。

2.スマートデバイスを管理対象にする

スマートデバイスを JP1/IT Desktop Management 2 の管理対象にすると、組織内のほかの機器や資産と同様にスマートデバイスを管理できるようになります。

スマートデバイスを管理対象にするためには、MDM 連携の設定をして、MDM システムからスマートデバイスの情報を取得します。

3.スマートデバイスを配布する

スマートデバイスを JP1/IT Desktop Management 2 の管理対象にしたら、利用申請に応じて利用者に配布します。配布する前にスマートデバイスの一覧を作成し、その一覧を基に配布します。

ほかの機器やハードウェア資産と同様に、JP1/IT Desktop Management 2 でスマートデバイスの管理を始めます。

(1) MDM システムを導入する流れ

JP1/IT Desktop Management 2 でスマートデバイスの管理を始めるために、MDM システムを導入し、スマートデバイスを登録します。

MDM サービスを導入する場合：

1.MDM サービスを契約する

スマートデバイスの導入に伴い、MDM サービスを契約します。

2.MDM サービスを利用する準備をする

契約した MDM サービスの Web ポータルへアクセスし、MDM サービスの運用に必要な情報を設定します。

3.MDM サービスにスマートデバイスを登録する

MDM サービスのエージェントプログラムをスマートデバイスにインストールし、MDM サービスにスマートデバイスを登録します。また、MDM サービスのポリシーをスマートデバイスに適用します。

ポイント

JP1/IT Desktop Management 2 では、MDM サービスに登録されているスマートデバイスを管理できます。このため、管理したいスマートデバイスは MDM サービスに登録しておく必要があります。

MDM サービスの導入が完了します。

MDM 製品を導入する場合：

1.MDM 製品を購入する

スマートデバイスの導入に伴い、MDM 製品を購入します。

2.MDM サーバに MDM 製品をインストールする

組織内のサーバに、購入した MDM 製品をインストールします。

3.MDM 製品にスマートデバイスを登録する

MDM 製品のエージェントプログラムをスマートデバイスにインストールし、MDM 製品にスマートデバイスを登録します。また、MDM 製品のポリシーをスマートデバイスに適用します。

ポイント

JP1/IT Desktop Management 2 では、MDM 製品に登録されているスマートデバイスを管理できます。このため、管理したいスマートデバイスは MDM 製品に登録しておく必要があります。

MDM 製品の導入が完了します。

(2) スマートデバイスを管理対象にする流れ

スマートデバイスを JP1/IT Desktop Management 2 の管理対象にすると、組織内のほかの機器や資産と同様にスマートデバイスを管理できるようになります。

スマートデバイスを管理対象にするためには、MDM 連携の設定をして、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. JP1/IT Desktop Management 2 で MDM 連携の設定をする

初めて MDM 連携機能を利用する場合、設定画面の [MDM 連携の設定] 画面で、MDM システムからスマートデバイスの情報を取得するよう設定します。連携済みの場合は、この手順は不要です。

2. スマートデバイスを JP1/IT Desktop Management 2 の管理対象にする

設定画面の [MDM 連携の設定] 画面で、[操作メニュー] の [MDM システムから機器情報を取得する] を選択します。MDM システムから情報が取得され、発見されたスマートデバイスが自動的に JP1/IT Desktop Management 2 の管理対象になります。

なお、設定画面の [MDM 連携の設定] 画面に表示される [発見した機器への操作] に、「設定されていません。」と表示されている場合は、設定画面の [発見した機器] 画面から、発見されたスマートデバイスを手動で管理対象にしてください。

3. スマートデバイスが管理対象になったことを確認する

機器画面の [機器一覧] 画面に、管理対象にしたスマートデバイスが表示されていることを確認します。このとき、[機器種別] (スマートデバイス)、[登録日時] などの条件でフィルタを利用すると、目的のスマートデバイスを素早く探せます。

4. ハードウェア資産情報を編集する

スマートデバイスのハードウェア資産情報は、[資産状態] が「未確認」になっています。また、MDM システムから収集できた情報だけが登録されています。このため、自動的に収集されない [利用者名]、[部署]、[資産管理番号]、[資産状態] などを手動で登録します。

また、必要に応じて購入や通信契約などの契約情報を登録して、ハードウェア資産情報と関連づけます。

スマートデバイスを JP1/IT Desktop Management 2 で管理するための準備が完了します。情報の登録が完了したら、利用者にスマートデバイスを配布します。在庫として保管するスマートデバイスがある場合は、保管場所にスマートデバイスを移動します。

関連リンク

- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)

(3) スマートデバイスを利用者に配布する流れ

JP1/IT Desktop Management 2 で管理しているスマートデバイスは、利用申請に応じて利用者に配布します。配布する前にスマートデバイスの一覧を作成し、その一覧を基に配布します。

1. 利用者からの利用申請を受ける

利用申請と併せて、スマートデバイスの管理に必要な利用者情報を入手しておきます。次の情報を入手してください。

- 部署
- 設置場所

- 利用者名
- メールアドレス
- 電話番号

2. スマートデバイスを特定する

資産画面の [ハードウェア資産] 画面で、[資産状態] が「在庫」のスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

3. 利用者情報を変更する

資産画面の [ハードウェア資産] 画面で [状態を変更] ボタンをクリックし、スマートデバイスの利用者情報を変更します。また、[資産状態] を「運用中」に変更します。

4. 配布するスマートデバイスの一覧を作成する

スマートデバイスを配布するため、配布するスマートデバイスの一覧を作成します。配布するスマートデバイスのハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、配布時に必要な情報をエクスポートします。例えば、配布するスマートデバイスを識別するために [資産管理番号] を、設置場所を確認するために [部署]、[設置場所] を、利用者と連絡を取るために [利用者名]、[メールアドレス]、[電話番号] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く配布するために、[部署] や [設置場所]などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

5. スマートデバイスを配布する

エクスポートした一覧の情報を基に、スマートデバイスを配布します。配送業者にスマートデバイスの配布を依頼する場合は、一覧を渡して作業してもらいます。利用者に受理したことを示すサインを一覧に記入してもらおうと、配布が完了したことを確認できます。

スマートデバイスを配布したら、JP1/IT Desktop Management 2 で管理を始めます。発生する業務に応じて情報をメンテナンスし、常に最新の状態でハードウェア資産情報を管理してください。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)

1.4.2 スマートデバイスをリプレースする流れ

従業員の異動やスマートデバイスの入れ替えに伴って組織内のスマートデバイスをリプレースする場合、JP1/IT Desktop Management 2 でリプレース対象のスマートデバイスを調査して、スマートデバイスを配布・回収します。

スマートデバイスをリプレースする流れを次に示します。

1. リプレースの計画を立てる

JP1/IT Desktop Management 2 でリプレースが必要なスマートデバイスを調査して、回収するスマートデバイスを決定します。回収するスマートデバイスを決定したら、代わりに配布するスマートデバイスを準備します。

2. 新しいスマートデバイスを配布する

JP1/IT Desktop Management 2 で配布するスマートデバイスの設置場所の情報を出力します。出力した情報を基に、スマートデバイスを配布します。

スマートデバイスを配布したら、利用者に古いスマートデバイスのデータを新しいスマートデバイスに移行するよう指示します。

3. スマートデバイスを回収する

古いスマートデバイスのデータを新しいスマートデバイスに移行したら、古いスマートデバイスを回収します。

JP1/IT Desktop Management 2 で回収するスマートデバイスの設置場所の情報を出力します。出力した情報を基に、スマートデバイスを回収します。

スマートデバイスのリプレースが完了します。

(1) スマートデバイスのリプレースの計画を立てる流れ

従業員の異動や機器の入れ替えなどに伴って組織内の機器をリプレースする場合、リプレースが必要な機器を調査して、リプレースする機器を決定します。リプレースする機器が決定したら、代わりに配布する機器を準備します。また、事前に利用者にリプレースについて通知します。

1. リプレースする機器を決定する

資産画面の [ハードウェア資産] 画面で、リプレースが必要な機器がないか調査します。例えば、3 年以上使用した機器をリプレースする方針の場合は、フィルタを利用して [登録日時] が 3 年以上前の機器がないか確認します。

ポイント

よく業務で使用するフィルタ条件を保存しておく、毎回条件を指定する手間が省けます。保存したフィルタ条件は、メニューエリアで選択することで一覧に適用できます。

リプレースが必要な機器が見つかった場合は、回収予定の機器として把握できるように、資産画面の [ハードウェア資産] 画面で [予定資産状態] に「在庫」、[変更予定日] に回収日を設定します。

2. 配布する機器を準備する

回収する機器の代わりに新しく配布する機器を準備します。

- 在庫の機器を利用する場合

資産画面の[ハードウェア資産]画面で、[資産状態]が「在庫」の機器を確認します。フィルタを利用すると、表示する情報を絞り込めます。スペックなどを確認して問題がなければ、配布予定の機器として把握できるように、[予定資産状態]に「運用中」を、[変更予定日]に配布日を設定します。

- 新しく機器を購入する場合

新しく機器を購入したら、JP1/IT Desktop Management 2の管理対象にして、ハードウェア資産情報と契約情報を登録します。そのあと、配布予定の機器として把握できるように、[予定資産状態]に「運用中」を、[変更予定日]に配布日を設定します。

3. 利用者にリプレースを通知する

スムーズにリプレースできるように、リプレースする機器の利用者に、リプレースする理由とリプレース予定日を連絡します。

リプレースの準備が完了します。

関連リンク

- [11.1.7 予定資産状態を変更する手順](#)
- [1.9.3 機器を購入する流れ](#)

(2) 新しいスマートデバイスを利用者に配布する流れ

リプレースの準備ができれば、配布するスマートデバイスの一覧を作成して、一覧を基に配布します。スマートデバイスを配布したらハードウェア資産情報を最新の状態にメンテナンスします。

1. 配布するスマートデバイスの一覧を作成する

スマートデバイスを配布するため、配布するスマートデバイスの一覧を作成します。配布するスマートデバイスのハードウェア資産情報をCSVファイルにエクスポートしてください。ハードウェア資産情報のうち、配布時に必要な情報をエクスポートします。例えば、配布するスマートデバイスを識別するために[資産管理番号]を、設置場所を確認するために[部署]、[設置場所]を、利用者と連絡を取るために[利用者名]、[メールアドレス]、[電話番号]などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く配布するために、[部署]や[設置場所]などを基準に並べ替えておくと便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. スマートデバイスを配布する

エクスポートした一覧の情報を基に、スマートデバイスを配布します。配送業者にスマートデバイスの配布を依頼する場合は、一覧を渡して作業してもらいます。利用者に受取したことを示すサインを一覧に記入してもらうと、配布が完了したことを確認できます。

3. ハードウェア資産情報をメンテナンスする

配布が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の[ハードウェア資産]画面で、配布したスマートデバイスの[資産状態]を「在庫」から「運用中」に変更します。また、[部署]、[設置場所]、利用者情報を最新の情報に変更します。

スマートデバイスを配布したら、古いスマートデバイスのデータを新しいスマートデバイスに移行するように利用者に指示します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)

(3) 利用しなくなったスマートデバイスを回収する流れ

利用しなくなったスマートデバイスを在庫に戻す場合、回収予定日になったらスマートデバイスを回収します。回収前にスマートデバイスの一覧を作成し、一覧を基にスマートデバイスを回収してください。スマートデバイスを回収したらハードウェア資産情報を最新の状態にメンテナンスします。

ポイント

ダイジェストレポートの[ハードウェア資産の予定]で、回収予定([予定資産状態]が「在庫」)のスマートデバイスの台数を確認することもできます。また、ダイジェストレポートをメールで送付することもできます。

ポイント

スムーズに回収するため、回収するスマートデバイスの利用者に、スマートデバイスを回収する理由や回収予定日を事前に通知しておくことをお勧めします。

1. 回収するスマートデバイスの一覧を作成する

スマートデバイスを回収するため、回収するスマートデバイスの一覧を作成します。[予定資産状態]が「在庫」のハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、回収時に必要な情報をエクスポートします。例えば、回収するスマートデバイスを識別するために[資産管理番号]を、設置場所を確認するために[部署]、[設置場所]を、利用者と連絡を取るために[利用者名]、[メールアドレス]、[電話番号]などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く回収するために、[部署] や [設置場所]などを基準に並べ替えておく と 便利 です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. スマートデバイスを回収する

エクスポートした一覧を基にスマートデバイスを回収します。配送業者にスマートデバイスの回収を依頼する場合は、一覧を渡して作業してもらいます。

スマートデバイスを回収したら、エクスポートした一覧の情報と照らし合わせて、回収結果が正しいか確認します。

3. ハードウェア資産情報をメンテナンスする

回収が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の [ハードウェア資産] 画面で、回収したスマートデバイスの [資産状態] を「運用中」から「在庫」に変更します。また、[設置場所] にスマートデバイスの保管場所を指定して、[部署] や利用者情報をシステム管理者の情報に変更します。

回収したスマートデバイスは在庫として管理します。

関連リンク

- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)

1.4.3 スマートデバイスの利用者を変更する流れ

利用者が部署異動する場合、ほかの利用者にスマートデバイスを引き継ぐときは、スマートデバイスの利用者を変更します。

スマートデバイスの利用者を変更する場合、スマートデバイスをいったん初期化してから、MDM システムに再登録します。

スマートデバイスの利用者を変更する流れを次に示します。

1. スマートデバイスを回収する

使用しなくなったスマートデバイスを、現在の利用者から回収します。

2. スマートデバイスを再配布する準備をする

回収したスマートデバイスを初期化してから、MDM システムに再登録します。

3.スマートデバイスを配布する

利用申請に応じて、スマートデバイスをほかの利用者に配布します。

スマートデバイスの利用者の変更が完了します。

(1) 利用しなくなったスマートデバイスを回収する流れ

利用しなくなったスマートデバイスを在庫に戻す場合、回収予定日になったらスマートデバイスを回収します。回収前にスマートデバイスの一覧を作成し、一覧を基にスマートデバイスを回収してください。スマートデバイスを回収したらハードウェア資産情報を最新の状態にメンテナンスします。

ポイント

ダイジェストレポートの「ハードウェア資産の予定」で、回収予定（「予定資産状態」が「在庫」）のスマートデバイスの台数を確認することもできます。また、ダイジェストレポートをメールで送付することもできます。

ポイント

スムーズに回収するため、回収するスマートデバイスの利用者に、スマートデバイスを回収する理由や回収予定日を事前に通知しておくことをお勧めします。

1.回収するスマートデバイスの一覧を作成する

スマートデバイスを回収するため、回収するスマートデバイスの一覧を作成します。「予定資産状態」が「在庫」のハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、回収時に必要な情報をエクスポートします。例えば、回収するスマートデバイスを識別するために「資産管理番号」を、設置場所を確認するために「部署」、「設置場所」を、利用者と連絡を取るために「利用者名」、「メールアドレス」、「電話番号」などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く回収するために、「部署」や「設置場所」などを基準に並べ替えておくことが便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2.スマートデバイスを回収する

エクスポートした一覧を基にスマートデバイスを回収します。配送業者にスマートデバイスの回収を依頼する場合は、一覧を渡して作業してもらいます。

スマートデバイスを回収したら、エクスポートした一覧の情報と照らし合わせて、回収結果が正しいか確認します。

3.ハードウェア資産情報をメンテナンスする

回収が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の[ハードウェア資産]画面で、回収したスマートデバイスの[資産状態]を「運用中」から「在庫」に変更します。また、[設置場所]にスマートデバイスの保管場所を指定して、[部署]や利用者情報をシステム管理者の情報に変更します。

回収したスマートデバイスは在庫として管理します。

関連リンク

- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)

(2) スマートデバイスを再配布する準備をする流れ

回収したスマートデバイスをほかの利用者に貸し出すために、スマートデバイスを初期化してから、MDMシステムに再登録します。

1.スマートデバイスを特定する

回収したスマートデバイスの資産管理番号を基に、資産画面の[ハードウェア資産]画面でスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

2.スマートデバイスを初期化する

[ハードウェア資産]画面で[機器一覧へ]ボタンをクリックして機器画面に移動したあと、[操作メニュー]の[初期化する(スマートデバイス)]を選択します。

JP1/IT Desktop Management 2 にスマートデバイスの機器情報を残すため、表示されるダイアログで[初期化したスマートデバイスの機器情報を削除する。]のチェックを外して、スマートデバイスを初期化します。

ポイント

スマートデバイスを初期化すると、MDMシステムのエージェントプログラムもスマートデバイスから削除されます。

3.MDMシステムからスマートデバイスの情報を削除する

設定画面の[MDM連携の設定]画面で、連携しているMDMシステムのMDMサーバのホスト名をクリックし、MDMシステムにログインします。MDMシステムで、スマートデバイスの情報を削除します。

4.MDM システムに初期化したスマートデバイスを再登録する

MDM システムに初期化されたスマートデバイスを再登録します。そのあと、MDM システムのエージェントプログラムをスマートデバイスにインストールし、MDM システムのポリシーをスマートデバイスに適用します。

ポイント

MDM システムにスマートデバイスを再登録すると、MDM システムからスマートデバイスの情報が収集されるタイミングで、機器情報が更新されます。

スマートデバイスを再配布する準備が完了します。

関連リンク

- ・ [6.27 スマートデバイスを初期化する手順](#)

(3) スマートデバイスを利用者に配布する流れ

JP1/IT Desktop Management 2 で管理しているスマートデバイスは、利用申請に応じて利用者に配布します。配布する前にスマートデバイスの一覧を作成し、その一覧を基に配布します。

1.利用者からの利用申請を受ける

利用申請と併せて、スマートデバイスの管理に必要な利用者情報を入手しておきます。次の情報を入手してください。

- ・ 部署
- ・ 設置場所
- ・ 利用者名
- ・ メールアドレス
- ・ 電話番号

2.スマートデバイスを特定する

資産画面の [ハードウェア資産] 画面で、[資産状態] が「在庫」のスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

3.利用者情報を変更する

資産画面の [ハードウェア資産] 画面で [状態を変更] ボタンをクリックし、スマートデバイスの利用者情報を変更します。また、[資産状態] を「運用中」に変更します。

4.配布するスマートデバイスの一覧を作成する

スマートデバイスを配布するため、配布するスマートデバイスの一覧を作成します。配布するスマートデバイスのハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、配布時に必要な情報をエクスポートします。例えば、配布するスマートデバイスを識別するために [資産管理番号] を、設置場所を確認するために [部署]、[設置場所] を、利用者と連絡を取るために [利用者名]、[メールアドレス]、[電話番号] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く配布するために、[部署] や [設置場所]などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

5. スマートデバイスを配布する

エクスポートした一覧の情報を基に、スマートデバイスを配布します。配送業者にスマートデバイスの配布を依頼する場合は、一覧を渡して作業してもらいます。利用者に受理したことを示すサインを一覧に記入してもらおうと、配布が完了したことを確認できます。

スマートデバイスを配布したら、JP1/IT Desktop Management 2 で管理を始めます。発生する業務に応じて情報をメンテナンスし、常に最新の状態ではハードウェア資産情報を管理してください。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)

1.4.4 スマートデバイスの紛失に対応する

万が一、組織で利用しているスマートデバイスを紛失してしまった場合、スマートデバイスに顧客データ、売上データ、開発データなどの機密情報が格納されていると、情報漏えいにつながるおそれがあります。このため、スマートデバイスを紛失してしまった場合は早急に対策が必要です。

スマートデバイスの紛失に対応する方法には、次の2種類があります。

紛失したスマートデバイスを初期化する方法

紛失後、一定期間が経ってもスマートデバイスが発見されない場合、情報漏えいを避けるために、スマートデバイスを初期化します。

紛失したスマートデバイスをロックする方法

MDM システムのポリシーで、スマートデバイスを最後に操作してからロックするまでの時間を長く設定している場合、拾得者が操作できないように、スマートデバイスをロックします。

(1) 紛失したスマートデバイスを初期化する流れ

スマートデバイスを紛失してしまった場合、情報漏えいを避けるためにスマートデバイスを初期化します。

紛失したスマートデバイスを初期化する流れを次に示します。

1.利用者から紛失の連絡を受ける

利用者から、スマートデバイスを紛失した旨の連絡を受けます。その際、スマートデバイスを特定するために、利用者名、契約電話番号などの情報を入手します。

2.紛失したスマートデバイスが発見されるのを待つ

組織のセキュリティのルールに従って、紛失したスマートデバイスの発見を待ちます。一定期間が経っても発見されなかった場合、情報漏えいを避けるために、スマートデバイスの初期化を決定します。

3.スマートデバイスを特定する

入手した情報を基に、機器画面の[機器一覧]画面でスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

4.特定したスマートデバイスを初期化する

機器画面の[機器一覧]画面で、[操作メニュー]の[初期化する(スマートデバイス)]を選択し、紛失したスマートデバイスを初期化します。

ポイント

スマートデバイスを初期化すると、MDMシステムのエージェントプログラムもスマートデバイスから削除されます。

5.MDMシステムから、スマートデバイスの情報を削除する

設定画面の[MDM連携の設定]画面で、連携しているMDMシステムのMDMサーバのホスト名をクリックし、MDMシステムにログインします。MDMシステムで、紛失したスマートデバイスの情報を削除します。

6.スマートデバイスの資産情報を編集する

資産画面の[ハードウェア資産]画面で、紛失したスマートデバイスを選択して、[状態を変更]ボタンをクリックします。表示されるダイアログで、[資産状態]を「運用中」から「滅却」にします。

また、紛失理由や紛失日時などを[ノート]タブにメモしておきます。

紛失したスマートデバイスの初期化が完了します。

また、必要に応じて、紛失したスマートデバイスの通信契約などを解約し、契約情報に反映します。

ポイント

情報漏えいにつながるような問題が発生した場合は、全従業員に事例を展開して、セキュリティ対策を徹底するように通知しましょう。

関連リンク

- [6.27 スマートデバイスを初期化する手順](#)

(2) 紛失したスマートデバイスをロックする流れ

MDM システムのポリシーで、スマートデバイスを最後に操作してからロックするまでの時間を長く設定している場合、紛失したスマートデバイスから情報が漏えいしないように、JP1/IT Desktop Management 2 からスマートデバイスをロックします。

紛失したスマートデバイスをロックする流れを次に示します。

1. 利用者から紛失の連絡を受ける

利用者から、スマートデバイスを紛失した旨の連絡を受けます。その際、スマートデバイスを特定するために、利用者名、契約電話番号などの情報を入手します。

2. スマートデバイスを特定する

入手した情報を基に、機器画面の [機器一覧] 画面でスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

3. 特定したスマートデバイスをロックする

機器画面の [機器一覧] 画面で、[操作メニュー] の [ロックする (スマートデバイス)] を選択し、表示されるダイアログで [OK] ボタンをクリックします。

紛失したスマートデバイスのロックが完了します。

また、必要に応じて、紛失したスマートデバイスの通信契約などを解約し、契約情報に反映します。

ポイント

紛失したスマートデバイスが発見された場合、スマートデバイスが操作された形跡がないことを確認してください。一定期間が経ってもスマートデバイスが発見されなかった場合、情報漏えいを避けるために、スマートデバイスを初期化することをお勧めします。

関連リンク

- [6.25 スマートデバイスをロックする手順](#)

1.4.5 利用者がスマートデバイスのパスコードを忘れた場合に対処する

利用者がスマートデバイスのパスコードを忘れた場合の対処方法には、次の 2 種類があります。状況に応じて選択してください。

スマートデバイスのパスコードをリセットする方法

利用者がスマートデバイスのパスコードを忘れた場合、管理者がスマートデバイスのパスコードをリセットします。そのあと、利用者にスマートデバイスのパスコードを再設定するように指示します。

初期化されたスマートデバイスを再登録する方法

利用者がスマートデバイスに間違ったパスコードを連続で入力した場合、MDM システムのポリシーによってスマートデバイスが初期化されることがあります。初期化されたスマートデバイスを利用するには、スマートデバイスを MDM システムおよび JP1/IT Desktop Management 2 に再登録する必要があります。

(1) スマートデバイスのパスコードをリセットする流れ

利用者がスマートデバイスのパスコードを忘れた場合、管理者がスマートデバイスのパスコードをリセットします。そのあと、利用者にスマートデバイスのパスコードを再設定するように指示します。

スマートデバイスのパスコードをリセットする流れを次に示します。

1. 利用者からスマートデバイスのパスコードを忘れた旨の連絡を受ける

利用者から、スマートデバイスのパスコードを忘れた旨の連絡を受けます。その際、スマートデバイスを特定するために、資産管理番号を入手します。また、折り返し連絡するための連絡先を入手します。

2. スマートデバイスを特定する

入手した資産管理番号を基に、資産画面の [ハードウェア資産] 画面でスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

3. 特定したスマートデバイスの資産情報を確認する

資産情報から利用者名と連絡先を確認し、利用者本人であることを確認します。利用者本人であることが確認できたら、利用者にスマートデバイスのパスコードをリセットすることを連絡します。

4. 特定したスマートデバイスのパスコードをリセットする

機器画面の [機器一覧] 画面で、[操作メニュー] の [パスコードをリセットする (スマートデバイス)] を選択し、スマートデバイスをリセットします。

ポイント

一度にパスコードをリセットできるのは 1 台のスマートデバイスだけです。複数のスマートデバイスのパスコードをリセットしたい場合は、1 台ずつリセットしてください。

スマートデバイスのパスコードのリセットが完了します。

利用者にスマートデバイスのパスコードをリセットした旨を連絡して、パスコードを再設定するように指示してください。

関連リンク

- [6.26 スマートデバイスのパスコードをリセットする手順](#)

(2) 初期化されたスマートデバイスを再登録する流れ

利用者がスマートデバイスに間違ったパスコードを連続で入力した場合、MDM システムのポリシーによってスマートデバイスが初期化されることがあります。初期化されたスマートデバイスを利用するには、スマートデバイスを MDM システムおよび JP1/IT Desktop Management 2 に再登録する必要があります。

初期化されたスマートデバイスを再登録する流れを次に示します。

1. 利用者からスマートデバイスが初期化された旨の連絡を受ける

利用者から、スマートデバイスが初期化された旨の連絡を受けます。その際、スマートデバイスを特定するために、資産管理番号を入手します。また、MDM システムに再登録し、MDM システムのエージェントプログラムをインストールするため、初期化されたスマートデバイスを利用者から回収します。

2. スマートデバイスを特定する

入手した資産管理番号を基に、資産画面の [ハードウェア資産] 画面でスマートデバイスを特定します。このとき、フィルタを利用すると素早く探せます。

3. 必要に応じて、初期化したスマートデバイスの情報を MDM システムから削除する

設定画面の [MDM 連携の設定] 画面で、連携している MDM システムの [MDM サーバのホスト名] をクリックし、MDM システムにログインします。MDM システムに初期化したスマートデバイスの情報が残っている場合は削除します。

4. MDM システムに初期化したスマートデバイスを再登録する

MDM システムに初期化したスマートデバイスを再登録します。そのあと、MDM システムのエージェントプログラムをスマートデバイスにインストールし、MDM システムのポリシーをスマートデバイスに適用します。

ポイント

MDM システムにスマートデバイスを再登録すると、MDM システムからスマートデバイスの情報が収集されるタイミングで、機器情報が更新されます。

5. スマートデバイスを配布する

再登録が完了したスマートデバイスを利用者に配布します。

初期化したスマートデバイスの再登録が完了します。

関連リンク

- ・ (3) [利用しなくなったスマートデバイスを回収する流れ](#)

1.4.6 スマートデバイスを滅却する流れ

リプレイスや修理などに伴ってスマートデバイスを回収した場合に、古くなったり壊れたりして今後使用しないものがあるときは、スマートデバイスを滅却します。

スマートデバイスを滅却する流れを次に示します。

1. 滅却対象の機器を決定する

回収したスマートデバイスのうち、今後使用しないものは滅却対象にします。滅却対象のスマートデバイスは、情報漏えいを防ぐために初期化します。

2. 機器を廃棄する

滅却予定日になったら機器を廃棄します。

故障したスマートデバイスの滅却が完了します。

(1) 滅却対象の機器を決定する流れ

リプレースや修理などに伴って機器を回収した場合に、古くなったり壊れたりして今後使用しない機器があるときは、滅却対象にします。今後も使用することがある機器は在庫として保管します。

1. 今後使用しない機器がないか確認する

回収した機器の中に、今後使用しない機器がないかを確認します。

例えば、利用年数が5年以上経過している機器を滅却する方針の場合は、資産画面の[ハードウェア資産]画面で、回収した機器の[登録日時]または[契約日]から、機器の利用年数を確認します。フィルタを利用すると、表示する情報を絞り込めます。

表示項目に[登録日時]または[契約日]が表示されていない場合は、一覧の項目名を右クリックして[表示項目の選択]を選択してください。表示されるダイアログで[登録日時]または[契約日]をチェックして[OK] ボタンをクリックすると、表示項目に[登録日時]または[契約日]が表示されます。なお、ハードウェア資産の契約情報が登録されていない場合は、[契約日]には「-」が表示されます。

2. 滅却対象にする

今後使用しない機器がある場合は、滅却予定の機器として把握できるように、[予定資産状態]を「滅却」にして、[変更予定日]に滅却予定日を設定します。

3. ハードディスクに格納されているデータを完全に消去する

滅却対象の機器は、情報漏えいを防ぐため、専用のツールを使用してハードディスクに格納されているデータを完全に消去します。

スマートデバイスを滅却する場合は、[ハードウェア資産]画面で[機器一覧へ] ボタンをクリックして機器画面に移動したあと、[操作メニュー]の[初期化する(スマートデバイス)]を選択してスマートデバイスを初期化します。

在庫として残す機器は、必要なときにすぐに利用できるようにディスクコピーします。

滅却対象の機器は、いつでも廃棄できる状態になります。

関連リンク

- [11.1.7 予定資産状態を変更する手順](#)
- [1.11 資産に関する契約を管理する流れ](#)

(2) 機器を廃棄する流れ

今後使用しない機器は、滅却予定日になったら廃棄します。廃棄前に機器の一覧を作成して、一覧を基に機器を廃棄します。機器を廃棄したらハードウェア資産情報を最新の状態にメンテナンスします。

1. 廃棄する機器の一覧を作成する

機器を廃棄するため、廃棄する機器の一覧を作成します。[予定資産状態]が「滅却」のハードウェア資産情報をCSVファイルにエクスポートしてください。ハードウェア資産情報のうち、廃棄時に必要な情報をエクスポートします。例えば、廃棄する機器を識別するために[資産管理番号]などの項目をエクスポートしてください。

2. 機器を廃棄する

エクスポートした一覧を基に機器を廃棄します。廃棄業者に廃棄を依頼する場合は、一覧を渡して作業してもらいます。

3. ハードウェア資産情報をメンテナンスする

廃棄が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の[ハードウェア資産]画面で、廃棄した機器の[資産状態]を「在庫」から「滅却」に変更します。

ポイント

ハードウェア資産の[資産状態]を「滅却」にすると、対応する機器情報は削除されます。

ポイント

ネットワークモニタを有効にしている場合、ハードウェア資産の[資産状態]を「滅却」にすると、対応する機器の情報がネットワーク制御リストから削除されます。ただし、対応する機器にエージェントが導入されていて、ネットワークに接続している場合、自動的に、機器が再び管理対象になってネットワーク制御リストに再登録されます。

機器の廃棄が完了します。なお、廃棄した機器のハードウェア資産情報は、[資産状態]が「滅却」の機器として残ります。

また、滅却した機器に関する契約は、必要に応じて解約します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [11.1.6 資産状態を変更する手順](#)

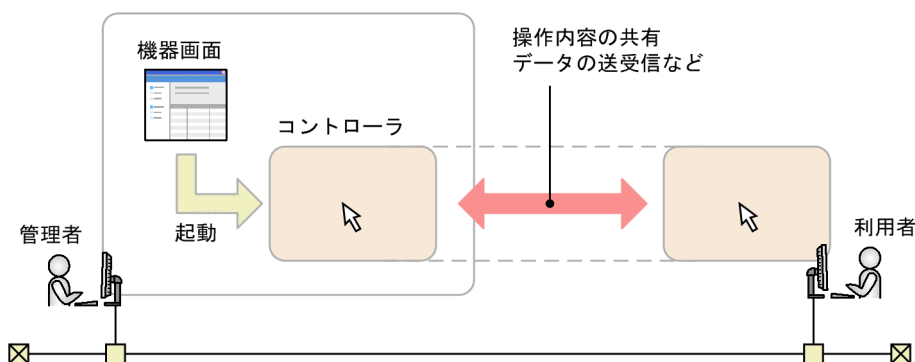
1.5 機器のリモートコントロール

組織内で、利用者のコンピュータに障害が発生したり、利用者からの問い合わせを受けたりした場合、管理者はその対応をする必要があります。しかし、そのたびに利用者の席に赴き、状況を確認して対処に当たると、1件の対応に非常に時間が掛かります。また、組織内のサーバが離れた場所にある場合、作業のたびにサーバルームへ移動したり、データを持ち運びしたりする手間も発生します。

リモートコントロール機能を利用すると、次に示すように効率良く機器の障害対応や、遠隔地のサーバ運用ができます。

- 遠隔地のコンピュータやサーバをリモートで操作できる
- 特別なソフトウェアや設定なしに、ファイル転送機能を利用してデータを送受信できる
- 操作内容を録画したり、接続中の複数の機器と同時にチャットしたりできる

リモートコントロールは、機器画面からコントローラを起動して実行します。一度コントローラを起動したコンピュータは、次回からはJP1/IT Desktop Management 2にログインしないでコントローラを起動することもできます。機器をリモートコントロールする流れを次の図に示します。



機器画面で接続先のコンピュータを選択し、接続します。接続が確立すると、リモートコントロールが開始されます。リモートコントロール中は、管理者と利用者で画面を共有できます。また、管理者側では、ファイル転送機能や録画機能など便利な機能を利用できます。

ここでは、次に示す業務でのJP1/IT Desktop Management 2の利用方法を説明します。

コンピュータに接続して問い合わせに対処する

利用者のコンピュータで障害が発生し、管理者に対処依頼があった場合、管理者のコンピュータから利用者のコンピュータをリモートコントロールして原因調査および対処します。

遠隔地にあるサーバを運用する

別のフロアや拠点など遠隔地にあるサーバを、管理者のコンピュータからリモートコントロールして運用します。

遠隔地にいる利用者に作業を指示する

遠隔地にいる利用者に対して作業を説明する場合に、リモートコントロールで作業内容を確認しながら指示を出します。

関連リンク

- [1.5.1 コンピュータをリモートコントロールして問い合わせに対処する流れ](#)
- [1.5.2 遠隔地にあるサーバを運用する流れ](#)
- [1.5.3 遠隔地にいる利用者に作業を指示する流れ](#)

1.5.1 コンピュータをリモートコントロールして問い合わせに対処する流れ

利用者のコンピュータで障害が発生した場合など、利用者から管理者に問い合わせがあったときに、管理者のコンピュータから利用者のコンピュータをリモートコントロールして原因調査および対処ができます。

コンピュータをリモートコントロールして、問い合わせに対処する流れを次に示します。

1.接続先のコンピュータを特定する

利用者から対処依頼があった際に、利用者名や資産管理番号などのコンピュータを特定するための利用者情報を入手します。その情報を基に、リモートコントロールするコンピュータを特定します。

2.コンピュータに接続する

コンピュータに接続する旨を利用者に連絡したあと、利用者のコンピュータに接続します。利用者が接続を許可すると、管理者のコンピュータから利用者のコンピュータをリモートコントロールできるようになります。

3.コンピュータを調査し問題点に対処する

リモート操作で利用者のコンピュータのログなどを調査し、問題点を特定して対処します。対処が完了したら、リモートコントロールを終了します。

利用者からの問い合わせの対処が完了します。

(1) リモートコントロールの対象のコンピュータを特定する流れ

コンピュータに接続する場合、対象のコンピュータを特定するために利用者情報を入手します。入手した利用者情報を基に接続先のコンピュータを特定します。

1.利用者情報を入手する

接続するコンピュータを特定するために利用者情報を入手します。例えば、利用者から障害対処依頼の連絡があった際に確認します。次の情報を入手してください。

- 資産管理番号
- 利用者名
- 部署
- 設置場所
- 電話番号

2.コンピュータを特定する

入手した利用者情報を基に、機器画面の［機器情報］画面でコンピュータを特定します。このとき、フィルタを利用すると素早く探せます。

コンピュータに接続する準備が完了します。

(2) リモートコントロールの対象のコンピュータに接続する流れ

コンピュータに接続します。コンピュータに接続する流れを説明します。

1.コンピュータに接続することを利用者に連絡する

接続の前に、電話などで利用者に次の2点を連絡しておきます。

- 今から利用者のコンピュータに接続すること
- 利用者のコンピュータに接続許可の確認ダイアログが表示されたら許可してほしいこと

2.コンピュータに接続する

機器画面の［機器情報］画面でコンピュータを選択し、接続します。認証画面が表示された場合は、ユーザーIDとパスワードを入力する必要があります。

接続時には、エージェントの設定に応じて、利用者のコンピュータに接続許可の確認ダイアログが表示されます。この場合、リモートコントロールを開始するためには、利用者に許可してもらう必要があります。これによって利用者は、リモートコントロールが開始されることを確認できます。

ポイント

コンピュータに接続するためには、管理者のコンピュータにコントローラがインストールされている必要があります。未インストールの場合は、操作画面からの接続開始時にインストールできます。すでにコントローラがインストールされている場合、コントローラを［スタート］メニューから直接起動して接続することもできます。

ポイント

OSがLinuxやMac OSなどのエージェントレスのコンピュータにも接続できます。

利用者のコンピュータに接続し、リモートコントロールが開始されます。

なお、コンピュータをリモートコントロールするときは、あらかじめ接続モードを設定しておきます。例えば、利用者のコンピュータの障害対処に当たる場合は、利用者に操作されないように「制御モード」で接続します。逆に、作業を指示して利用者の操作内容を監視する場合は、利用者が操作できるように「監視モード」で接続します。目的に応じて、適切な接続モードを設定してください。

ポイント

コントローラは複数起動できます。このため、複数のコンピュータの画面を並べて比較したり、監視したりできます。

ポイント

通信速度が遅いコンピュータに接続する場合、データ転送量を減らしてリモートコントロールを高速化できます。リモートコントロールの高速化は、コントローラの「環境の設定」ダイアログで設定できます。

ポイント

NAT 環境など、管理者のコンピュータから利用者のコンピュータを参照できない場合、利用者のコンピュータから接続要求を出せます。

ポイント

接続先のコンピュータが AMT または Wake on Lan に対応している場合、電源が OFF の状態でも自動的に電源を ON にして、リモートコントロールを開始できます。

関連リンク

- [7.1 コントローラをインストールする手順](#)
- [15.1.1 エージェント設定の管理](#)

(3) コンピュータをリモートコントロールして問題点を調査する

リモートコントロールで利用者のコンピュータを調査し、問題点に対処します。リモートコントロール中は、次のような操作ができます。

- ファイルを送受信する
リモートコントロール中のコンピュータとファイルを送受信できます。ログファイルを収集して解析したり、接続先のコンピュータに必要なデータを転送したりする場合に便利です。
- 接続先のコンピュータを再起動した場合に、自動的に再度接続する
接続先のコンピュータを再起動したあとで、自動的に接続を再開できます。メンテナンスなどで、再起動が必要な場合に便利です。
- チャットで利用者と会話する

チャット機能を使用して、画面上で管理者と複数の利用者が同時に会話できます。また、チャットの内容は保存や印刷ができるので記録として残せます。電話が利用できない環境で連絡を取り合ったり、複数人に同時に指示を出したりするのに便利です。

- 操作内容を動画ファイルに保存する
リモートコントロール中の操作内容を録画して、動画ファイルに保存できます。障害対処の手順をほかの利用者に説明する手間を省きたい場合に便利です。

調査および対処が完了したら、リモートコントロールを終了して結果を利用者に連絡します。

関連リンク

- [7.5.13 リモートコントロール中のコンピュータを再起動する手順](#)

1.5.2 遠隔地にあるサーバを運用する流れ

別のフロアや拠点など遠隔地にあるサーバを運用する場合、管理者のコンピュータからサーバをリモートコントロールすることで、作業のたびに設置場所へ行ったり、サーバのデータメンテナンスのために拠点へ出張したりするような手間を軽減できます。

ここでは、サーバの業務システムの環境設定をリモートコントロールで変更する場合を例に、遠隔地にあるサーバを運用する流れについて説明します。

1.サーバに接続する

管理者のコンピュータから、遠隔地に設置されているサーバに接続します。

2.サーバの環境設定を変更する

サーバの環境設定ファイルを管理者のコンピュータに転送し、設定を変更します。

設定変更したファイルは、いったんテスト用サーバに転送して動作確認します。その後、問題がなければ本番用サーバへ環境設定ファイルを転送して適用します。

このように作業することで、サーバ上でファイル編集ができない環境でもデータを持ち運びする手間を省けます。

リモートコントロールでサーバの環境設定変更が完了します。

(1) 遠隔地にあるサーバに接続する流れ

サーバの環境設定ファイルの内容を変更する場合、いったんサーバに接続して、環境設定ファイルを管理者のコンピュータに転送します。

また、日々の運用でサーバに接続する場合は、接続リストにサーバを登録しておき、コントローラから直接接続します。毎回のように操作画面から機器を探して接続する手間を省けます。

サーバに接続する流れを次に示します。

1. コントローラを起動する

[スタート] メニューから、コントローラを直接起動します。

ポイント

コンピュータに接続するためには、管理者のコンピュータにコントローラがインストールされている必要があります。未インストールの場合は、操作画面からの接続開始時にインストールできます。

2. 接続リストに接続先のサーバを登録する

コントローラから接続リストを表示して、接続先の機器を登録します。

3. サーバに接続する

接続リストから接続先のサーバを選択して接続します。認証画面が表示された場合、認証情報を入力します。認証に成功すると、サーバに接続できます。

ポイント

認証の有無はエージェント設定で設定します。デフォルトでは、認証画面が表示される設定になっています。管理者以外はサーバに接続できないように、サーバ接続時は認証画面が表示される設定にすることをお勧めします。エージェントレスのコンピュータに接続する場合は、接続先のリモートコントロール機能の設定に依存します。

サーバに接続し、リモートコントロールが開始されます。

関連リンク

- ・ [7.1 コントローラをインストールする手順](#)

(2) 遠隔地にあるサーバの環境設定を変更する流れ

サーバに接続したら、サーバの環境設定を変更します。

サーバ上で環境設定ファイルを直接編集してもかまいません。サーバ上で作業ができない場合や、管理者のコンピュータ上のツールを利用した方が効率が良い場合は、サーバの環境設定ファイルをいったん管理者のコンピュータに転送します。その後、編集した環境設定ファイルをサーバに転送し、適用します。

ポイント

例えば、環境設定ファイルが複雑な CSV ファイルの場合、管理者のコンピュータに効率良く編集できるソフトウェアがインストールされているときは、管理者のコンピュータ上で環境設定ファイルを編集した方が便利です。

リモートコントロールでサーバの環境設定を変更する流れを次に示します。

1.環境設定ファイルを管理者のコンピュータに転送する

管理者のコンピュータで環境設定ファイルを編集するため、環境設定ファイルをサーバから管理者のコンピュータに転送します。

2.環境設定ファイルを編集する

管理者のコンピュータで、環境設定ファイルを編集します。

3.環境設定ファイルをテスト用サーバに転送する

管理者のコンピュータで編集した環境設定ファイルをテスト用サーバに転送します。

4.環境設定ファイルを本番用サーバに転送する

テスト用サーバで運用テストをして、問題がなければ本番用サーバに環境設定ファイルを転送し、適用します。

サーバの環境設定が更新されます。管理者が場所を移動することなくサーバの環境設定を変更できます。

1.5.3 遠隔地にいる利用者に作業を指示する流れ

管理者が離れた場所にいる利用者に対して作業を説明する場合、電話による指示だけでは、作業が正確に行われたかどうか確認することが困難です。管理者が現地に向かう場合も、移動時間が掛かったり、作業に必要なデータを持ち出す必要があったりと、非常に手間が掛かります。

このような場合、リモートコントロール機能を利用すれば、画面上で利用者の作業内容を確認しながら電話で指示を出せるため、作業を正確に完了できます。また、移動の手間をなくしたり、持ち出しによる情報漏えいのリスクを回避したりもできます。

管理者が、離れた場所にいる利用者に対して作業をレクチャーする流れを次に示します。

1.コンピュータに接続する

利用者に連絡し、コンピュータに接続します。このとき、利用者が指示どおりに作業しているかを確認するために、リモートコントロールモードを「監視モード」で接続します。「監視モード」で接続すると、リモートコントロール中に利用者が操作できますが、管理者は操作できません。

2.利用者に作業を指示する

利用者の操作を確認しながら、電話で指示を出します。作業に必要なデータが利用者のコンピュータにない場合は、管理者のコンピュータから必要なデータを転送します。

(1) 利用者に作業を指示する

遠隔地にいる利用者に対して作業を指示する場合、リモートコントロール機能を利用してコンピュータに接続したあと、コントローラの画面を確認しながら電話で作業を説明します。

作業に必要なデータが利用者のコンピュータにない場合は、ファイル転送機能を利用して、管理者のコンピュータからデータを転送できます。データを転送する場合は、リモートコントロールモードを「共有モード」または「制御モード」にしてください。「監視モード」の場合は、ファイル転送機能は利用できません。

ポイント

作業中に利用者が操作できない状況になった場合は、リモートコントロールモードを「共有モード」または「制御モード」に変更することで途中から管理者が作業を続行できます。

関連リンク

- [7.5.10 接続モードを変更する手順](#)

1.6 機器のネットワーク接続の管理

組織内のネットワークに個人所有のコンピュータやセキュリティが不十分なコンピュータが接続されると、そこからウィルスの感染や情報漏えいが発生するおそれがあります。組織内の機器を管理する場合は、不正なネットワーク接続を未然に防いだり、セキュリティが不十分な機器を即座にネットワークから遮断したりするために、機器のネットワーク接続を管理する必要があります。

JP1/IT Desktop Management 2 では、次に示すような機能を利用して機器のネットワーク接続を管理できます。

- 接続を許可しない機器を指定する（ブラックリスト方式）

機器の新規接続を許可している場合、セキュリティに問題がある機器だけネットワーク接続を遮断したいときなどに利用します。指定したコンピュータのネットワーク接続を遮断できるため、個々のコンピュータのネットワーク接続を制御できます。

- 接続を許可する機器を指定する（ホワイトリスト方式）

組織内のネットワークに、個人所有のコンピュータなどからのネットワーク接続を許可したくない場合などに利用します。指定した機器以外のネットワーク接続を遮断できるため、より強固にセキュリティを保てます。

- 任意のタイミングで機器のネットワーク接続の遮断や接続許可を実施する

ブラックリスト方式およびホワイトリスト方式のケースで、セキュリティに問題がある機器を見つけた場合に、その機器だけネットワーク接続を遮断したい場合に利用します。

注意事項

ネットワークモニタ機能は、接続を許可する機器、および許可しない機器を十分に確認してから使用してください。ネットワークへの接続を制御する方法を誤ると、業務に使用している機器の接続が遮断されるなど、トラブルにつながるおそれがあります。

注意事項

ホワイトリスト方式でネットワーク接続を管理する場合、ルータ、スイッチ、ネットワークプリンタなど、JP1/IT Desktop Management 2 が管理対象としない機器に対しても、ネットワーク接続を許可するように登録してください。特に、ルータやスイッチなどのネットワーク装置が接続を許可するよう設定されていないと、その配下に接続された機器もネットワークに接続できないため、注意してください。

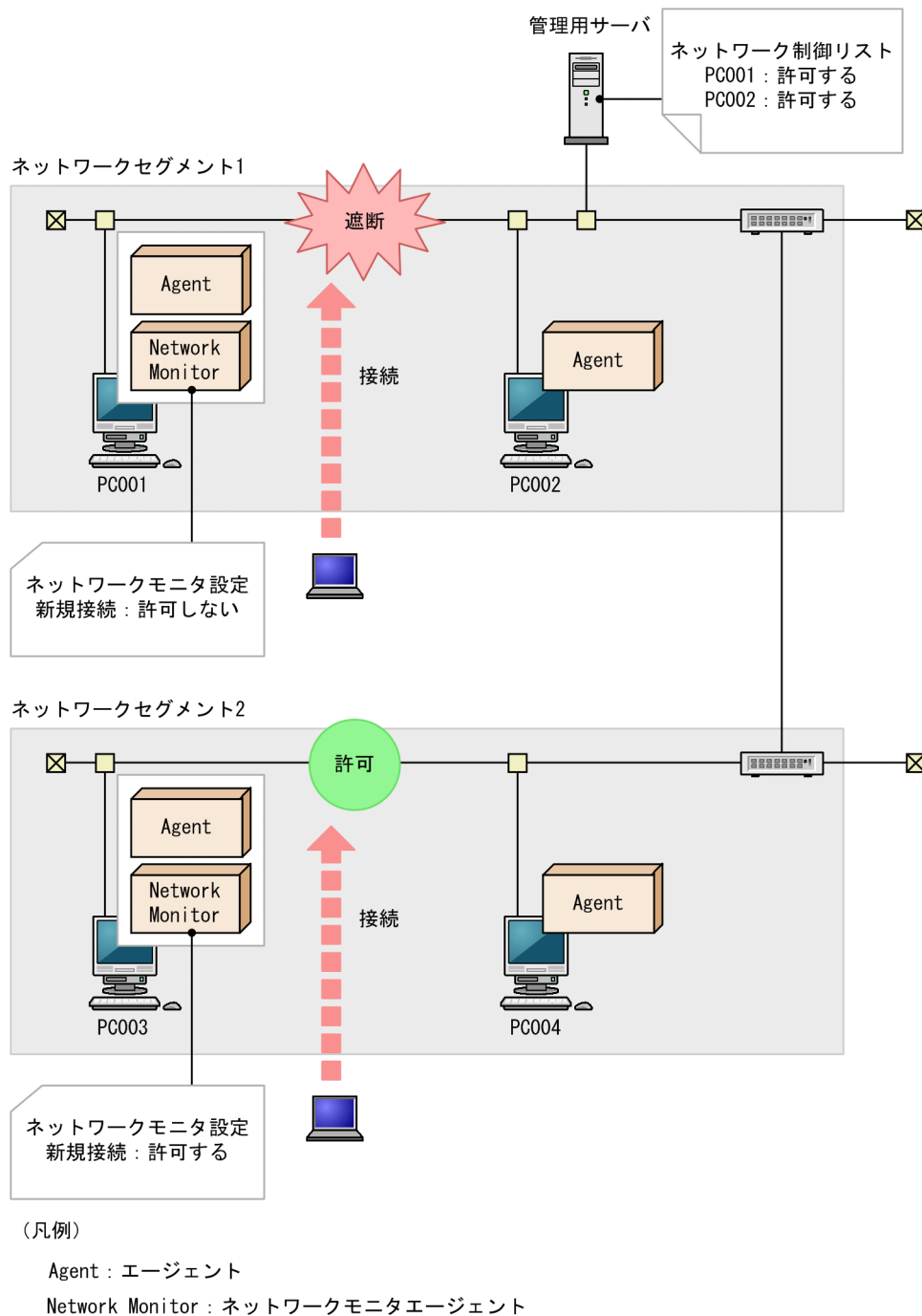
注意事項

ルータ、プリンタ、サーバなどの業務上重要な機器については、ネットワーク制御リストの自動更新によって機器が遮断されないよう、ネットワーク制御リストに、その機器の IP アドレスを手動

で登録することを推奨します。この際、MAC アドレスを入力すると、機器情報の更新によってネットワーク制御リストから削除されるおそれがあるため、[MAC アドレス] 欄を空白にしてください。

機器のネットワーク接続の管理は、機器画面および設定画面で実行します。

機器のネットワーク接続を管理する概念を次の図に示します。



機器のネットワーク接続を管理するためには、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たエージェントを配置します。そうすると、管理用サーバから割り当てられたネットワークモニタ設

定に従って、ネットワークの接続可否が制御されます。また、ネットワーク制御リストでは、機器ごとのネットワーク接続の可否を設定できます。

例えば、個人所有のコンピュータのネットワーク接続を禁止する場合、あらかじめネットワーク接続を許可する組織内の機器をネットワーク制御リストに登録し、そのあとでネットワークモニタ設定で新規機器の接続を禁止します。このように設定することで、個人所有のコンピュータがネットワークに接続しても自動的に遮断され、組織内のシステムを安全に保てます。

なお、管理用サーバ、または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は、ネットワーク接続を遮断できません。

ここでは、次に示す業務での JP1/IT Desktop Management 2 の利用方法を説明しています。目的の業務に応じて説明を参照してください。

個人所有のコンピュータのネットワーク接続を禁止する

許可したコンピュータだけネットワークに接続できるようにします。

ウィルス感染時に機器のネットワーク接続を遮断する

ウィルスに感染した機器のネットワーク接続を遮断します。対策が完了したらネットワーク接続を回復します。

セキュリティポリシーに違反した機器のネットワーク接続を自動制御する

セキュリティポリシーの判定結果に従って、自動的にネットワーク接続を遮断および回復します。

一時的に機器のネットワーク接続を許可する

新規機器のネットワーク接続が禁止されている場合に、指定したコンピュータだけ一時的にネットワーク接続を許可します。

関連リンク

- [1.6.1 個人所有 PC のネットワーク接続を禁止する流れ](#)
- [1.6.2 ウィルス感染時に機器のネットワーク接続を遮断する流れ](#)
- [1.6.3 セキュリティポリシーに違反した機器のネットワーク接続を自動制御する流れ](#)
- [1.6.4 一時的に機器のネットワーク接続を許可する流れ](#)

1.6.1 個人所有 PC のネットワーク接続を禁止する流れ

組織内のネットワークに個人所有のコンピュータが自由に接続できるようになっていると、接続されたコンピュータによってウィルスの感染や情報漏えいが発生するおそれがあります。そこで、個人所有のコンピュータを組織内のネットワークに接続できないようにするために、ネットワーク接続を許可する機器を登録して、登録された機器だけが接続できるようにします。

ネットワーク制御リストに登録されていない機器をネットワークに接続できないようにすることで、個人所有のコンピュータの接続によるセキュリティのリスクを回避できます。

個人所有のコンピュータのネットワーク接続を禁止する流れを次に示します。

1. 機器をネットワーク制御リストに登録する

ネットワーク接続を許可する機器をネットワーク制御リストに登録します。

2. 未登録の機器のネットワーク接続を禁止する

ネットワーク制御リストに登録されていない機器がネットワーク接続できないように設定します。

3. ネットワーク接続した機器を確認する

新規に接続された機器を確認します。

(1) 機器をネットワーク制御リストに登録する

組織内のネットワークに接続されている機器をネットワーク制御リストに登録します。ネットワーク制御リストは、設定画面の [ネットワーク制御リストの設定] 画面で確認できます。組織内の機器のうち、ネットワーク接続を許可するすべての機器をネットワーク制御リストに登録してください。

注意事項

ルータやスイッチなどのネットワーク装置もネットワーク接続が制御されます。ネットワーク装置のネットワーク接続が遮断されてしまうと、機器のネットワーク接続ができなくなります。このため、ネットワーク制御リストにはネットワーク制御をする範囲のネットワーク装置を登録してください。

ポイント

設定画面の [ネットワーク制御リストの設定] 画面では、ネットワーク接続を許可するかどうかを機器ごとに設定できます。デフォルトでは、表示されている機器のネットワーク接続は許可に設定されています。

ポイント

ネットワークモニタを有効にすると、定期的に探索しなくても、電源が ON にされている機器を発見できます。

JP1/IT Desktop Management 2 で管理している機器

機器が管理対象または除外対象になると、自動的にネットワーク制御リストに登録されます。このため、すでに管理対象または除外対象の機器はネットワーク接続が許可されています。ネットワーク制御リストへの追加作業は不要です。

JP1/IT Desktop Management 2 で管理していない機器

すべての機器を登録するために、定期的にネットワークの探索を実行してください。定期的に探索することで、電源が OFF だった機器の電源が ON になったタイミングや、出張で持ち出されているノート PC がネットワークに接続されたタイミングなどで機器を発見できます。

また、各ネットワークセグメントに対してネットワークモニタを有効にすると、ネットワーク接続されている機器や新規に接続した機器を発見できます。このとき、ネットワークモニタの設定はデフォルトのまま（新規に発見された機器を接続許可する）にしておきます。

管理対象または除外対象にすることで自動的にネットワーク制御リストに登録されます。

注意事項

ルータなどのネットワーク機器をリプレースすると、MAC アドレスが変更されるため、リプレース後はネットワーク接続を遮断されます。リプレース後もネットワーク接続を許可されるようにするためには、リプレースするネットワーク機器の MAC アドレスを先に登録するか、機器の IP アドレスを固定にしてネットワーク制御リストに登録してください。

関連リンク

- [8.1 ネットワークモニタを有効にする手順](#)

(2) 未登録の機器のネットワーク接続を禁止する流れ

組織内の機器をすべてネットワーク制御リストに登録したら、ネットワーク制御リストに登録されていない機器がネットワーク接続できないように設定します。

ポイント

組織内の機器がすべてネットワーク制御リストに登録されたかどうかは、ネットワーク探索やネットワークモニタによって機器が発見されなくなり、発見された機器がすべて管理対象か除外対象になっているかどうかで判断します。

未登録の機器のネットワーク接続を禁止する流れを次に示します。

1. ネットワークモニタを有効にする

ネットワーク制御をする範囲のネットワークセグメントに対して、ネットワークモニタを有効にします。

2. ネットワークモニタ設定を変更する

デフォルトでは、ネットワークモニタを有効にしても、未許可の機器がネットワーク接続できるようになっています。ネットワーク制御リストに登録されていない機器がネットワーク接続できないようにするには、ネットワークモニタ設定を「ネットワークへの接続を許可しない」に設定して、すべての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

あらかじめ、すべてのネットワークセグメントに割り当てるネットワークモニタ設定を統一しておくと、そのネットワークモニタ設定を変更することでネットワーク制御の設定を一括で変更できます。

ネットワーク制御リストに登録されていない機器がネットワーク接続できなくなります。

関連リンク

- [8.1 ネットワークモニタを有効にする手順](#)

(3) ネットワーク接続した機器を確認する

ネットワークモニタ設定によって新規接続の機器のネットワーク接続を許可しない環境でも、新規にネットワーク接続した機器を管理者が確認できます。

機器がネットワーク接続したタイミングで新規機器として発見されます。発見された機器は、ホーム画面の［システムサマリ］パネルや、設定画面の［発見した機器］画面から確認できます。このとき、機器のネットワーク接続は自動的に遮断されます。機器がネットワーク接続を遮断されたかどうかは、イベントで確認できます。

個人所有のコンピュータなどが接続されたことを確認したら、発見された機器の情報を基に利用者に接続理由を確認します。業務に不要な理由だった場合は、個人所有の機器を持ち込まないように利用者を指導します。

(4) 機器のネットワーク接続状況をリアルタイムに監視する

ネットワークモニタを有効にして機器のネットワーク接続を管理している場合、ネットワークに新規に機器が接続されたことをリアルタイムに発見できます。さらに、発見された機器に対してはエージェントを自動的に配信してインストールできます。この機能を利用することで、組織内のネットワークに接続されている機器の現状を把握できます。

ネットワークの探索で機器を発見するには、探索のタイミングで機器が次の条件を満たしている必要があります。

- ネットワークに接続されている
- 電源が ON になっている

そのため、長期間ネットワークに接続されていなかったり、ネットワークに接続されているが長期間電源が OFF になっていたたりする場合は、機器を発見できません。

ネットワークモニタを有効にしておくと、機器がネットワークに接続されたり、電源が ON になったりしたタイミングで、自動的に機器を発見できます。また、発見された機器に対しては、ネットワーク探索の探索設定に基づいて、自動的に管理対象にしたりエージェントを配信したりできます。

注意事項

ネットワークモニタの設定で未登録機器のネットワーク接続を禁止している場合でも、機器は発見されてエージェントも配信されます。エージェント配信後の機器のネットワーク接続可否は、セキュリティポリシーなどの設定に依存します。機器画面の機器一覧などでネットワークの接続設定を確認してください。

組織内の機器のネットワーク接続状況をリアルタイムに監視するためには、各ネットワークセグメントで次の条件をすべて満たすコンピュータを1台用意してください。

- エージェントをインストールしている
- ネットワークモニタを有効にしている
- 24時間稼働している

1.6.2 ウィルス感染時に機器のネットワーク接続を遮断する流れ

組織内のネットワークに接続されているコンピュータにウィルスが発見された場合、ほかのコンピュータへの感染を防ぐため、迅速にネットワーク接続を遮断する必要があります。

ネットワークモニタ機能を利用すると、任意のタイミングで機器のネットワーク接続を遮断したり、遮断したネットワーク接続を回復したりできます。この機能を利用することで、ウィルスが発見されたコンピュータを一時的にネットワークから切り離し、対策が完了したらネットワークに接続するなどの運用ができます。

ウィルスが発見されたコンピュータのネットワーク接続を制御する流れを次に示します。

1. ウィルスが発見されたコンピュータのネットワーク接続を遮断する

ウィルスが発見された場合、そのコンピュータのネットワーク接続を遮断して、ウィルスの被害がほかのコンピュータに拡大しないように対処します。

2. 対策が完了したコンピュータのネットワーク接続を許可する

ウィルス対策が完了したら、コンピュータのネットワーク接続を許可します。

ウィルス対策が完了したコンピュータが、ネットワーク接続を再開できます。

ポイント

セキュリティ対策のためにコンピュータのネットワーク接続が遮断中でも、特定のサーバには接続できるように設定できます。

関連リンク

- [1.7.5 ウィルス感染時に対策状況を確認する](#)

(1) ウィルスが発見された機器のネットワーク接続を遮断する流れ

組織内のコンピュータでウィルスが発見された場合、そのコンピュータのネットワーク接続を遮断して、ウィルスの被害がほかのコンピュータに拡大しないように対処する必要があります。

1. 利用者からウィルス感染の連絡を受け取る

利用者から、ウィルス感染の連絡を受け取ります。コンピュータの LAN ケーブルを抜いていること、感染したウィルスがウィルス対策製品によって検疫、駆除されていることを利用者に確認します。

2. コンピュータのネットワーク接続を遮断する

ウィルス対策の確認が完了するまで、コンピュータのネットワーク接続を遮断します。

機器画面の [機器情報] 画面で、ウィルスが発見されたコンピュータを選択し、[操作メニュー] - [接続を許可しない] を選択します。

ポイント

[OS]、[利用者名]、[部署]、[設置場所] などの条件でフィルタを利用すると、目的のコンピュータを素早く探せます。

3. ウィルス対策の状況を確認する

ウィルスが検疫・駆除されていることは確認済みですが、ウィルスの感染につながるような不審なソフトウェアが利用されていないか、ウィルス対策状況が最新になっているかなどを確認する必要があります。

コンピュータのウィルス対策が完了します。

関連リンク

- (1) ウィルスが発見されたコンピュータに問題がないか確認する
- (2) コンピュータのウィルス対策状況を確認する

(2) 対策が完了した機器のネットワーク接続を許可する流れ

ウィルスが発見された機器の対策状況に問題がないことを確認したら、遮断したネットワーク接続を回復します。

1. 遮断したネットワーク接続を回復する

ウィルス対策が完了したことを確認したら、コンピュータのネットワーク接続を許可します。遮断中の機器のネットワーク接続を回復するためには、機器画面の [機器情報] 画面で機器を選択し、[操作メニュー] - [接続を許可する] を選択してください。

2. 利用者に連絡する

コンピュータのネットワーク接続を許可したことを利用者に連絡します。

利用者が LAN ケーブルを再度接続することで、コンピュータがネットワーク接続され業務を再開できます。

ウィルスを駆除したコンピュータが再度ネットワーク接続できます。

1.6.3 セキュリティポリシーに違反した機器のネットワーク接続を自動制御する流れ

セキュリティポリシーに違反している機器は、セキュリティ対策が不十分です。このような機器をそのままネットワーク接続させておくと、セキュリティ対策の不備を原因とする情報漏えいや不正操作、ウィルス感染被害などのリスクがあります。

セキュリティポリシーにネットワーク制御の条件を設定しておく、セキュリティの判定結果に応じて、自動的にコンピュータのネットワーク接続を遮断したり、回復したりできます。この機能を利用することで、セキュリティ対策を実施していないコンピュータを、セキュリティ対策が完了するまでネットワーク接続させない運用ができます。

セキュリティポリシーに違反した機器のネットワーク接続を自動制御する流れを次に示します。

1. セキュリティポリシーにネットワーク制御の設定をする

セキュリティ対策が実施されていないコンピュータのネットワーク接続を自動的に遮断するために、セキュリティポリシーにセキュリティ設定項目、利用者へのメッセージ通知、およびネットワーク接続制御の設定をします。

2. ネットワーク接続が遮断された機器を確認する

セキュリティポリシーの判定結果に従って、機器のネットワーク接続が自動的に遮断されます。利用者に対策を促すために、遮断された機器を確認します。

3. セキュリティポリシーに違反した機器を対策する

機器の利用者に対して対策を指示します。セキュリティ状況に問題がないと判定されると、自動でネットワーク接続が許可されます。

セキュリティポリシーの判定結果によって、自動で機器のネットワーク接続を許可したり遮断したりできます。

関連リンク

- [1.7.1 セキュリティポリシーを設定する](#)

(1) セキュリティポリシーにネットワーク制御の設定をする

セキュリティ対策が実施されていないコンピュータのネットワーク接続を自動的に遮断したい場合、セキュリティポリシーにネットワーク制御の設定をします。ネットワーク制御の設定には、危険レベルごとにネットワークの接続可否を設定できます。また、数日間連続して違反した場合に遮断するといった条件も設定できます。

例えば、メッセージの自動通知機能を利用して、日々のセキュリティ判定時に対策を促すメッセージを利用者に通知しておき、それでも対策しない利用者はネットワーク接続を遮断するといった運用ができます。このように運用する場合は、セキュリティポリシーを次のように設定します。

- セキュリティ設定項目の設定

違反したらネットワーク接続を遮断する必要がある項目を、セキュリティの判定対象に設定します。また、各項目に判定結果の危険レベルを設定します。

- 利用者へのメッセージ通知の設定

メッセージ通知の対象となる危険レベルとメッセージの本文を設定します。

ポイント

通知されるメッセージに、問題のある状態が続くとネットワーク接続が遮断されることを記入しておきます。

- ネットワーク接続制御の設定

ネットワーク接続を遮断する危険レベルを設定します。また、数日間連続して違反した場合に遮断する場合は、[接続拒否の条件] に許容する日数を設定します。セキュリティ判定後、問題のあるコンピュータのネットワーク接続を即座に遮断したい場合は、接続拒否の条件の設定は不要です。

なお、セキュリティポリシーに違反したコンピュータが、対策後に「安全」と判定されると自動的にネットワーク接続が回復します。

注意事項

手動でネットワーク接続を遮断した場合、対策後に「安全」と判定されても、ネットワーク接続は自動的に回復しません。自動的にネットワーク接続を回復させたい場合は、手動でネットワーク接続を遮断しないでください。

セキュリティポリシーの設定が完了すると、セキュリティの判定結果に応じてコンピュータのネットワーク接続が制御されるようになります。

ポイント

セキュリティ対策のためにコンピュータのネットワーク接続が遮断中でも、特定のサーバには接続できるように設定できます。

関連リンク

- [1.7.1 セキュリティポリシーを設定する](#)

(2) ネットワーク接続が遮断された機器を確認する

セキュリティポリシーにメッセージ通知の設定をしておくと、セキュリティポリシーに違反したコンピュータに対して、セキュリティ対策を実施するよう自動でメッセージを通知できます。また、セキュリティポリシーにネットワーク制御の設定をしておくことで、違反したコンピュータのネットワーク接続が自動的に遮断されるようになります。

セキュリティポリシーに違反しているコンピュータに対しては、日々のセキュリティ判定でメッセージが通知されます。しかし、利用者がメッセージに従わないでセキュリティ対策を実施しない場合、ネットワーク制御の設定に従って、機器のネットワーク接続が自動的に遮断されます。

ネットワーク接続が遮断された機器の利用者から問い合わせがあった場合、管理者はセキュリティ対策を実施するよう利用者に指示する必要があります。このとき、利用者の機器の状態を確認することで、どのようにセキュリティ対策を実施すればよいか、具体的に指示できます。

ネットワーク接続が遮断されたコンピュータを確認するためには、セキュリティ画面の「機器のセキュリティ状態」画面で「接続設定」が  の機器を表示します。このとき、フィルタを利用すると、素早く表示できます。ネットワーク接続が遮断された機器の状態を確認することで、その機器のセキュリティの問題点を把握できます。

ポイント

機器をネットワークから遮断したことを、管理者にメール通知させることもできます。設定画面の「イベント通知の設定」画面で、「警戒」と「セキュリティ」をチェックしてください。ただし、この場合、遮断以外の警戒イベントが発生したときも、メール通知されます。

問題点を把握したら、利用者に対策を依頼します。

関連リンク

- ・ (1) [メールからセキュリティポリシー違反を把握する](#)

(3) セキュリティポリシーに違反した機器を対策する

セキュリティポリシーの違反によってネットワークから遮断された機器の問題点を対策することで、自動的にネットワーク接続を回復できます。

管理者からの依頼やメッセージ通知の内容に基づいて、利用者がセキュリティポリシーに違反している内容をすべて対策すると、コンピュータの危険レベルが「安全」と判定されます。「安全」と判定されたコンピュータは、自動的にネットワーク接続が回復します。

関連リンク

- ・ 9. [セキュリティ状況を管理する](#)
- ・ 1.7.2 [セキュリティポリシー違反を対策する](#)

1.6.4 一時的に機器のネットワーク接続を許可する流れ

新規機器のネットワーク接続を禁止している場合、拠点からの出張者や社内システムの保守員などが組織内のネットワークに接続するときは、ネットワーク制御の設定をそのつど変更する必要があります。このような場合、一時的に接続を許可するコンピュータを設定することで、指定した期間だけネットワークに接続できるようになります。

一時的に機器のネットワーク接続を許可する流れを次に示します。

1.期間を指定して機器のネットワーク接続を許可する

特定の期間だけネットワークに接続できるように、一時的に接続を許可するコンピュータを設定します。

2.一時的なネットワーク接続許可の期間を延長する

ネットワーク接続を許可する期間を変更することで、接続できる期間を延長します。

(1) 期間を指定して機器のネットワーク接続を許可する流れ

拠点からの出張者や社内システムの保守員などが組織内のネットワークに接続する必要がある場合、一時的に接続を許可するコンピュータを設定することで、指定した期間だけネットワークに接続できるようになります。

1.接続するコンピュータの情報を確認する

ネットワーク接続を許可するコンピュータを登録するために、あらかじめ次の内容を確認しておきます。

- 利用者名
- 所属
- 利用開始日/終了日
- MAC アドレス
- 申請理由

2.一時的に接続を許可する

一時的にネットワーク接続を許可するコンピュータは、設定画面の [ネットワーク制御リストの設定] 画面で設定します。

[追加] ボタンをクリックして、事前に確認した情報を登録します。このとき、ネットワーク接続の許可を指定するとともに [利用開始日時] および [利用終了日時] をチェックして、接続を許可する期間を指定します。

設定した期間は、登録したコンピュータがネットワーク接続できるようになります。

設定した期間が過ぎると、自動的にネットワーク接続ができなくなります。

(2) 一時的なネットワーク接続許可の期間を延長する

拠点からの出張者や社内システムの保守員などに対して、一時的に組織内のネットワーク接続を許可している場合、業務の都合によって許可期間を超過してしまうことがあります。このような場合、ネットワーク接続を許可する期間を変更することで、接続できる期間を延長できます。

ネットワーク接続を許可する期間を変更するには、設定画面の〔ネットワーク制御リストの設定〕画面で該当するコンピュータを選択して〔編集〕ボタンをクリックします。表示されるダイアログで、〔利用終了日時〕を変更してください。

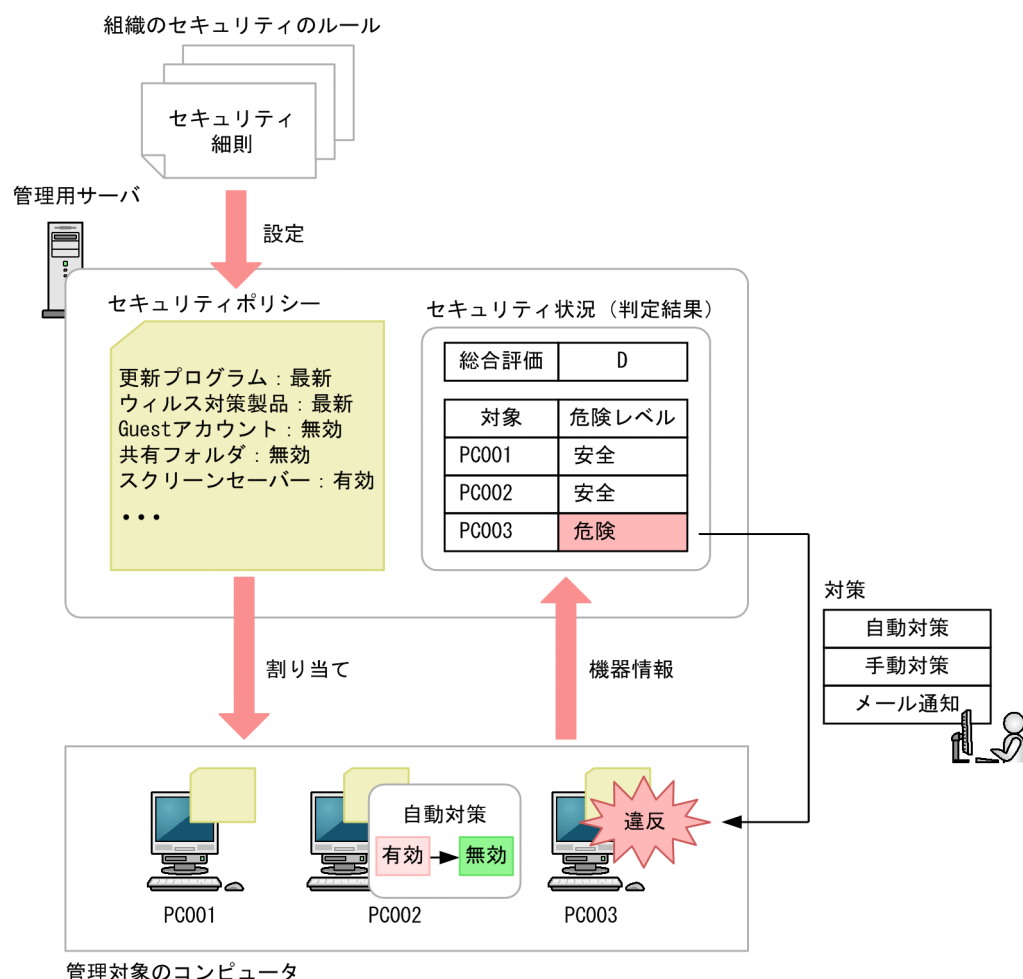
1.7 セキュリティ状況の管理

組織内のコンピュータのセキュリティ状況を管理するためには、セキュリティに関するルールを決め、それを各コンピュータの利用者に遵守させる必要があります。また、セキュリティの現状を把握して、問題点を適宜対策することも必要です。

JP1/IT Desktop Management 2 を利用すると、次に示すような機能を使って効率良くセキュリティを管理できます。

- 組織のセキュリティルールに基づいたセキュリティポリシーを設定し、各コンピュータに適用できる
- 各コンピュータのセキュリティポリシーの遵守状況や問題点を一覧やレポートで把握できる
- セキュリティ上の問題点を自動的に対策できる

セキュリティの管理は、セキュリティ画面で実行します。セキュリティ状況を管理するためには、セキュリティポリシーを設定し、コンピュータの状況を把握して、問題点がある場合は対策します。状況把握と対策のサイクルを繰り返すことで、組織のセキュリティ状況を向上させていきます。セキュリティ状況を管理する流れを次の図に示します。



組織のセキュリティのルールに基づいて、JP1/IT Desktop Management 2 でセキュリティポリシーを設定します。

セキュリティポリシーをコンピュータに割り当てると、一覧やレポートでセキュリティポリシーの遵守状況が確認できます。問題がある場合は対策を実施します。なお、セキュリティポリシーに自動対策を設定している場合は、セキュリティポリシーをコンピュータに割り当てたタイミングで対策が実行されます。

また、セキュリティポリシーの設定によって、ソフトウェアやデバイスの利用を抑止したり、各コンピュータから操作のログを取得して不審な操作を検知したりできます。

ここでは、次に示す業務での JP1/IT Desktop Management 2 の利用方法を説明しています。目的の業務に応じて説明を参照してください。

セキュリティポリシーを設定する

組織のセキュリティに関するルールを基に、JP1/IT Desktop Management 2 でセキュリティポリシーを設定します。設定したセキュリティポリシーをコンピュータに適用することで、セキュリティポリシーの遵守状況（セキュリティ状況）を確認できます。

セキュリティポリシー違反を対策する

セキュリティポリシー違反があった場合、管理者にメールで通知されるように設定し、通知されたメールを基にセキュリティポリシー違反を対策します。対策方法には、自動対策および手動対策があります。

自動で更新プログラムを適用する

日本マイクロソフト社からリリースされた更新プログラムを JP1/IT Desktop Management 2 が取得し、自動的にコンピュータに配布して適用します。更新プログラムのリリースから適用までに一定の期間が必要です。

手動で更新プログラムを適用する

日本マイクロソフト社からリリースされた更新プログラムを管理者が JP1/IT Desktop Management 2 に登録し、コンピュータに配布して適用します。リリースされた更新プログラムを即時にコンピュータに適用できます。

ウィルス感染時に対策状況を確認する

ウィルス対策製品によってウィルスが検知された場合に、コンピュータのウィルス対策状況を確認します。

許可したソフトウェアだけを利用できるようにする

コンピュータにインストールされたソフトウェアを確認し、業務に不要なソフトウェアの場合は使用禁止ソフトウェアとして登録して管理します。

情報漏えいが起きていないか確認する

不審な操作が検出された場合に、情報漏えいが発生していないかどうかを確認します。

デバイスの使用を制限する

許可したデバイスだけで、データの読み書きができるようにします。また、組織内全体で USB デバイスの利用を禁止して、特定のコンピュータだけ USB デバイスの読み書きができるようにすることもできます。

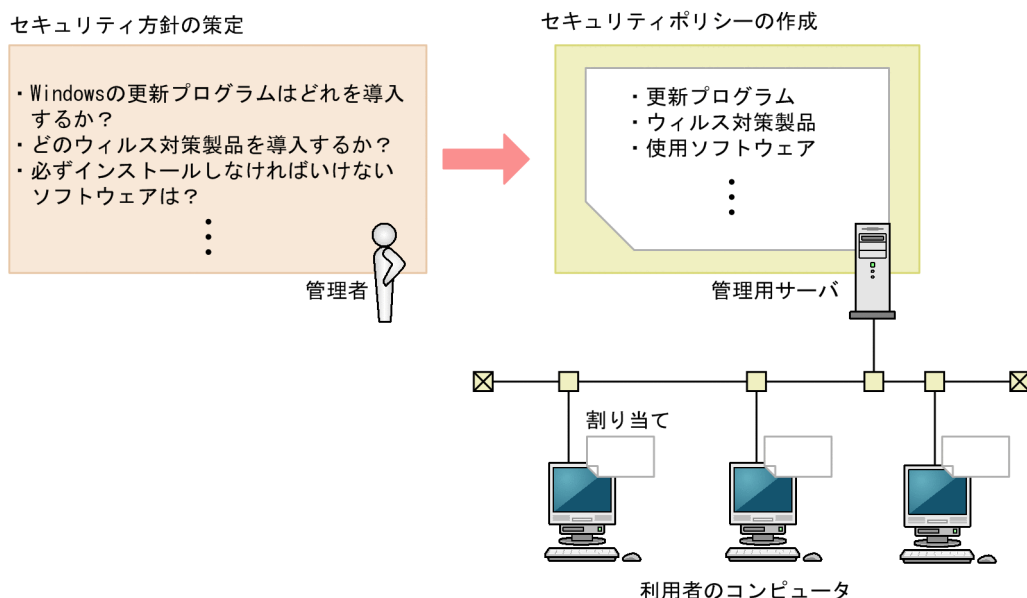
セキュリティの監査に対応する

セキュリティの監査が実施される場合に、セキュリティポリシーに基づいて組織内のセキュリティ状況が適切に管理されている証拠を提示します。

1.7.1 セキュリティポリシーを設定する

組織内のコンピュータのセキュリティ状況を管理するためには、最初に組織のセキュリティ方針を策定する必要があります。組織にセキュリティ方針がない場合、JP1/IT Desktop Management 2 でセキュリティ管理を行う前にセキュリティ方針を策定してください。

策定したセキュリティ方針を基に、JP1/IT Desktop Management 2 でセキュリティポリシーを作成します。作成したセキュリティポリシーをコンピュータに割り当てることで、セキュリティポリシーの遵守状況（セキュリティ状況）を確認できるようになります。最新のセキュリティ対策の傾向（セキュリティトレンド）が変化したり、組織のセキュリティ方針が変更になった場合は、セキュリティポリシーを更新します。



関連リンク

- ・ (1) 組織のセキュリティ方針を策定する
- ・ (2) セキュリティポリシーの管理

(1) 組織のセキュリティ方針を策定する

組織にセキュリティ方針がない場合、JP1/IT Desktop Management 2 でセキュリティ管理をする前にセキュリティ方針を策定します。策定したセキュリティ方針を基に、JP1/IT Desktop Management 2 でセキュリティポリシーを作成します。そのため、セキュリティ方針を策定する前に、セキュリティポリシーの設定項目を確認することをお勧めします。

セキュリティ方針を策定するポイントを次に示します。

- Windows に導入する更新プログラムを決定する
- 組織内で利用するウィルス対策製品を決定する
- 必ずインストールしなければならないソフトウェアや使用を禁止したいソフトウェアがある場合、ソフトウェアのリストを作成する
- 組織内で稼働を禁止したいサービスがある場合、禁止サービスのリストを作成する
- Windows のファイアウォールの設定や共有フォルダの使用有無など、組織内で利用しているコンピュータのセキュリティ設定の方針を決定する
- 印刷、機器の操作、ソフトウェアの起動について抑止したい操作がある場合、抑止操作のリストを作成する
- アクセスを監視したい Web、メール、Web サーバ、および FTP サーバがある場合、リストを作成する

また、セキュリティ方針を策定するためには、新聞記事や雑誌、各ソフトウェア開発会社のホームページなどを確認し、セキュリティトレンドを把握しておく必要があります。組織の運営方針とあわせてセキュリティトレンドを確認することで、強固なセキュリティ管理ができるようになります。

例えば、ウィルス対策製品のウィルス検出率や誤検出の割合について調査しておくことで、組織の運営方針に合致したウィルス対策製品を選択できます。

ポイント

セキュリティトレンドの取得が困難な場合は、ツールベンダーや VAR（付加価値再販業者）、または外部コンサルタントに情報の取得を委託することをお勧めします。

セキュリティ方針を策定したら、それを基にセキュリティポリシーを作成します。

(2) セキュリティポリシーの管理

セキュリティ画面の [セキュリティポリシー] 画面で、セキュリティポリシーを作成して管理します。ここでは、セキュリティポリシーの管理について説明します。

セキュリティポリシーを作成する

組織のセキュリティ方針を基にセキュリティポリシーを作成します。セキュリティポリシーは複数作成できます。部署ごとに異なるセキュリティポリシーを作成したり、特別な管理が必要なコンピュータ用のセキュリティポリシーを作成したりできます。

セキュリティポリシーをコンピュータに割り当てる

コンピュータのセキュリティ状況を把握するためには、作成したセキュリティポリシーをコンピュータまたはグループに割り当てる必要があります。

セキュリティポリシーを編集する

セキュリティトレンドが変化したり、組織のセキュリティ方針が変更になった場合は、セキュリティポリシーを編集します。セキュリティトレンドは、コンピュータやネットワークの環境とともに変化しています。常にセキュリティトレンドを組織内に取り込み続けることで、強固なセキュリティ状況の管理を実現できます。

セキュリティポリシーを削除する

管理体制の変更やセキュリティポリシーの統合に伴って、不要になったセキュリティポリシーがある場合は削除します。

1.7.2 セキュリティポリシー違反を対策する

JP1/IT Desktop Management 2 では、セキュリティポリシー違反が起こった場合に備えてさまざまな設定ができます。セキュリティポリシー違反を自動的に対策したり、違反の発生を自動的にメール通知するように設定したりできます。

また、セキュリティポリシー違反が発生したあと対策するために、違反したコンピュータの設定を強制変更したり、利用者に自動的に対策依頼メッセージを通知したりする機能も備えています。

これらの機能を利用することで、セキュリティポリシー違反が発生したときにスムーズに対策できます。

(1) メールからセキュリティポリシー違反を把握する

セキュリティ状況の判定の結果、セキュリティポリシー違反があった場合に、自動的に管理者へメール通知するようにできます。メール通知を設定しておくことで、セキュリティ状況に問題が発生したことをタイムリーに把握でき、迅速な対応をとれます。

セキュリティポリシー違反があった場合、種別が「セキュリティ管理」のイベントが発生します。このイベントが発生したときに、自動的にメールが通知されるように設定します。通知されたメールを基に、セキュリティ状況を確認し、セキュリティポリシー違反を対策してください。

1.メール通知を設定する

メール通知の契機となるイベントとメールの通知先は、設定画面の [イベント] - [イベント通知の設定] 画面で設定します。

セキュリティポリシー違反をメールで通知するためには、重大度が「緊急」と「警戒」、種類が「セキュリティ」のイベントをメール通知の対象に設定してください。

なお、通知するイベントの重大度とセキュリティ状況の危険レベルは次のように対応します。

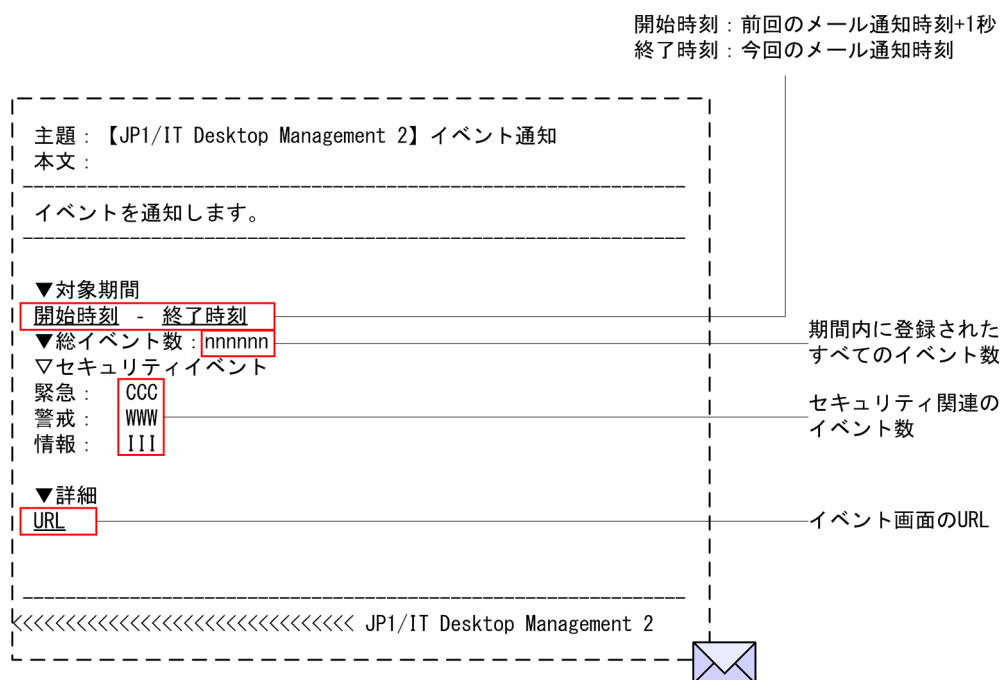
重大度	危険レベル
 (緊急)	 (危険)
 (警戒)	 (警告)

重大度	危険レベル
⚠ (警戒)	⚠ (注意)
✅ (情報)	✅ (安全)

2.通知されたメールを確認する

JP1/IT Desktop Management 2 から通知されるメールでは、セキュリティに関するイベントの発生状況を確認できます。緊急のイベントが発生していた場合は、メールに記載された URL から JP1/IT Desktop Management 2 の操作画面を起動して、セキュリティ状況を確認して対策してください。

メールで通知される内容を次に示します。



3.セキュリティ状況を確認する

JP1/IT Desktop Management 2 の操作画面から、違反の内容や発生個所などの詳細情報を把握できます。ホーム画面やセキュリティ画面から、危険と判定されたコンピュータの状況を確認して対処してください。

なお、メールを通知するためには、メールの送信に利用するメールサーバを設定する必要があります。

関連リンク

- (2) セキュリティポリシー違反を自動的に対策する
- (3) セキュリティポリシー違反を手動に対策する
- 15.7.1 イベント通知の設定をする手順
- 9.1 セキュリティ状況を確認する
- 15.8.1 メールサーバを設定する手順

(2) セキュリティポリシー違反を自動的に対策する

セキュリティポリシーに違反した項目があった場合に、自動的に適正状態に設定変更して自動対策できます。

セキュリティポリシーに自動対策を設定しておくことで、セキュリティポリシーが適用されたタイミングで、自動的に設定が適正状態に変更されます。このため、JP1/IT Desktop Management 2 の管理者やコンピュータの利用者が対策する手間を省けます。組織内のセキュリティ方針や運用に応じて、セキュリティポリシーに自動対策を設定する項目を検討してください。

ポイント

例えば、意図的に Windows ファイアウォールを使用しないようにしている環境では、自動対策によって Windows ファイアウォールが有効になってしまうと、運用に支障をきたすおそれがあります。このような場合は、セキュリティポリシーで自動対策されないように設定してください。

セキュリティポリシーの違反を対策できたかどうかは、セキュリティ画面で該当する項目が安全 () になっているかどうかで確認できます。

関連リンク

- [9.1 セキュリティ状況を確認する](#)
- [\(3\) セキュリティポリシー違反を手動で対策する](#)

(3) セキュリティポリシー違反を手動で対策する

セキュリティ状況を確認した結果、セキュリティポリシーに違反した項目があった場合は手動で対策します。

強制的に対策する

セキュリティの設定項目で自動対策できる項目については、セキュリティポリシー違反が発生した場合に、任意のタイミングで強制対策できます。

利用者に対策してもらう

セキュリティポリシーに違反したコンピュータの利用者に、違反内容と任意のメッセージを自動的に通知できます。自動対策と併用することで、パスワードの安全性やパワーオンパスワードなどの自動対策をしない (できない) 項目の対策を利用者に促せます。メッセージの自動通知は、[セキュリティポリシーの追加] ダイアログまたは [セキュリティポリシーの編集] ダイアログの [アクション項目] で設定できます。

また、任意のタイミングでコンピュータの利用者にメッセージを通知することもできます。

セキュリティポリシーの違反を対策できたかどうかは、セキュリティ画面で該当する項目が安全 () になっているかどうかで確認できます。

関連リンク

- [\(2\) セキュリティポリシー違反を自動的に対策する](#)

- 9.1 セキュリティ状況を確認する
- 9.4 セキュリティポリシー違反を強制対策する手順
- 6.22 利用者にメッセージを通知する手順

(4) オフライン管理のコンピュータのセキュリティポリシー違反を対策する

オフライン管理のコンピュータは、自動対策できません。そのため、セキュリティ状況を確認した結果セキュリティポリシーに違反した項目があった場合は、対象のコンピュータの利用者に、管理者が直接対策の指示をします。

対策を実施したあと、オフライン管理のコンピュータの機器情報を取得し直して、セキュリティ状況を確認します。

セキュリティポリシーの違反を対策できたかどうかは、セキュリティ画面で該当する項目が安全（）になっているかどうかで確認できます。

1.7.3 自動で更新プログラムを配布する流れ

組織内の OS が Windows のコンピュータの場合、不具合を修正したりセキュリティ上の問題を修正したりするために、必要に応じて更新プログラムを適用します。JP1/IT Desktop Management 2 では、日本マイクロソフト社からリリースされた更新プログラムを、セキュリティポリシーに従って自動的にコンピュータに配布、適用できます。

更新プログラムを自動で適用する流れを次に示します。

1.更新プログラムの最新情報を取得する

日本マイクロソフト社からリリースされた最新の更新プログラムの情報は、サポートサービスサイトから自動的に取得できます。追加された更新プログラムの情報を確認して、適用の要否を判断します。

2.コンピュータに自動で更新プログラムを配布する

セキュリティポリシーの判定項目に更新プログラムの適用要否を設定すると、セキュリティポリシーの判定結果に従って自動的に未適用の更新プログラムが配布されます。

3.更新プログラムの適用状況を確認する

更新プログラムの適用状況を確認し、問題があった場合は原因の確認と対策を実施します。

コンピュータに更新プログラムが適用され、適正状態が安全に保たれます。

(1) 更新プログラムの最新情報を取得する方法

コンピュータに最新の更新プログラムを適用するためには、リリースされた更新プログラムの情報を把握する必要があります。

日本マイクロソフト社からリリースされた最新の更新プログラムの情報は、サポートサービスサイトから自動的に取得できます。取得した更新プログラムの情報は、セキュリティ画面の [更新プログラム一覧] 画面で確認できます。

また、更新プログラムが追加されると自動的にメールが通知されるように設定できます。メール通知によって更新プログラムの追加を確認できるだけでなく、メール中の URL から直接ログインして [更新プログラム一覧] 画面を確認することもできます。

注意事項

最新の更新プログラムの情報を取得するためには、サポートサービス契約が必要です。

注意事項

更新プログラムが日本マイクロソフト社からリリースされてから管理用サーバの情報が更新されるまで約 10 営業日掛かります。

ポイント

更新プログラムの情報は、2006 年 1 月 1 日以降にリリースされたものがデフォルトで登録されています。

ポイント

管理用サーバがインターネットに接続できないなどの理由からサポートサービスサイトと接続できない場合、サポートサービスサイトに接続できるコンピュータから更新プログラムの情報とプログラムを手動でダウンロードし、管理用サーバにアップロードすることで、更新プログラムを配布できます。

関連リンク

- [15.8.3 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](#)
- [15.8.1 メールサーバを設定する手順](#)

(2) コンピュータに自動で更新プログラムを配布する方法

セキュリティポリシーの判定項目に更新プログラムの適用可否を設定すると、セキュリティポリシーに違反した場合に、自動的に未適用の更新プログラムを配布して対策できます。

更新プログラムを配布するための設定は、日本マイクロソフト社からリリースされたすべての更新プログラムを適用するか、特定の更新プログラムだけを適用するかの 2 とおりの方法があります。

すべての更新プログラムを適用する場合

サポートサービスサイトから更新プログラムの情報を取得すると、セキュリティポリシーに反映されて判定を実施して、更新プログラムが適用されていない場合は、自動的に更新プログラムが配布されます。適用を除外したい更新プログラムが登録された更新プログラムグループを指定することで、特定の更新プログラムの適用を除外することもできます。

特定の更新プログラムだけを適用する場合

適用しなければならない更新プログラムが登録された更新プログラムグループを選択したあとで、更新プログラムグループに含まれる更新プログラムがセキュリティポリシーの判定結果に従って配布されます。

業務に影響がないようにテストを実施してから配布したい場合は、特定の更新プログラムだけを適用する方法を選択してください。

それぞれの設定方法について説明します。

ポイント

更新プログラムの自動配布は、セキュリティポリシーごとに設定できます。例えば、営業部はすべての更新プログラムを適用するが、開発部は特定の更新プログラムだけを適用する場合、部署ごとのセキュリティポリシーを作成して、更新プログラムの適用方法を設定してください。

すべての更新プログラムを適用する場合

セキュリティ画面の［セキュリティポリシー一覧］画面でセキュリティポリシーを編集します。

セキュリティ設定項目の［更新プログラム］で、［更新プログラム適用］に［すべての更新プログラムが適用済み］を選択します。また、［自動対策］をチェックして［更新プログラムを配布（ITDM 互換配布）］を選択します。

管理用サーバに登録されたすべての更新プログラムの情報を基に各コンピュータの適用状況が判定され、未適用の更新プログラムがあった場合は自動的に配布されます。

ポイント

適用を除外したい更新プログラムがある場合は、セキュリティ画面の［更新プログラム一覧］画面で、あらかじめ更新プログラムグループを作成しておきます。そのあと、作成した更新プログラムグループを［除外する更新プログラムグループ］に指定してください。

特定の更新プログラムだけを適用する場合

1. コンピュータに適用してもよい更新プログラムを選択する

セキュリティ画面の［更新プログラム一覧］画面で、更新プログラムグループを作成します。

運用開始時は、更新プログラムグループに、デフォルトで登録されている更新プログラムのうち、すでにコンピュータに適用している更新プログラムや、これから適用してもよいと判断した更新プログラムを登録します。

ポイント

デフォルトで登録されている更新プログラムは数が多いため、大部分を適用する場合は、全選択したあとで不要な項目のチェックを外すと便利です。

2.セキュリティポリシーを設定する

セキュリティ画面の［セキュリティポリシー一覧］画面でセキュリティポリシーを編集します。

セキュリティ設定項目の［更新プログラム］で、［更新プログラム適用］に［指定した更新プログラムが適用済み］を選択します。このとき、更新プログラムグループには手順 1.で作成したグループを指定します。また、［自動対策］をチェックして［更新プログラムを配布（ITDM 互換配布）］を選択します。この設定によって、更新プログラムグループに登録された更新プログラムだけが、セキュリティポリシーによる判定の対象になります。さらに、未適用と判定された場合は自動的に更新プログラムが配布されます。

3.新規に追加された更新プログラムを確認する

サポートサービスサイトから新規に更新プログラムの情報が取得された場合は、その更新プログラムの適用可否を判断します。

適用してもよいと判断した場合は、その更新プログラムを更新プログラムグループに登録します。これによって、セキュリティポリシーの判定対象の更新プログラムが追加されます。適用できないと判断した更新プログラムは、その理由を［更新プログラム一覧］画面の［ノート］タブに記録しておきます。

ポイント

更新プログラムを適用してもよいかテストをする場合、テスト用の更新プログラムグループとセキュリティポリシーを設定して、テスト用のコンピュータにセキュリティポリシーを割り当てておくると便利です。テストをしたい更新プログラムを更新プログラムグループに登録するだけで、自動的にテスト用のコンピュータに配布されます。

更新プログラムグループに登録された更新プログラムが、セキュリティポリシーの判定結果に従って自動的に配布されます。

(3) 更新プログラムの適用状況を確認する流れ

更新プログラムの適用状況に問題があるかどうかは、セキュリティ画面の［セキュリティポリシー一覧］画面の［更新プログラム］タブで確認できます。

機器のセキュリティ状況を確認した結果、危険レベルが「安全」であれば問題ありませんが、「警告」や「危険」の場合は更新プログラムが適用されていないおそれがあります。次の流れで状況把握および対策を実施します。

1.更新プログラムの適用状況を把握する

「セキュリティポリシー一覧」画面では問題の有無だけを確認できます。このため、どの更新プログラムの適用状況に問題があるかを確認するには、「セキュリティ詳細レポート」の「更新プログラムの適用状況」レポートを表示します。このレポートから、更新プログラムごとに未適用のコンピュータがある項目を確認できます。

2.未適用の原因を確認する

レポートを確認した結果、コンピュータに更新プログラムが適用されていない場合、配布に失敗しているおそれがあります。配布（ITDM 互換）画面の「タスク一覧」画面で、タスク種別が「自動対策で実行されるタスク（更新プログラムの対策）」のタスクを選択し、配布に失敗したコンピュータの状況を確認します。このとき、タスク状態の詳細を確認することで、配布がエラーになった原因を確認できます。

3.更新プログラムの未適用を対策する

未適用のコンピュータに対して、更新プログラムを再配布できます。

セキュリティ画面の「セキュリティポリシー一覧」画面の「更新プログラム」タブで、「操作」の「更新プログラムを配布（ITDM 互換配布）」ボタンをクリックしてください。未適用のコンピュータに、更新プログラムが再配布されます。

ポイント

更新プログラムの再配布は、「機器のセキュリティ状態」画面の「セキュリティ対策を実行」ボタンからも実行できます。

更新プログラムの適用状況の把握および対策が完了します。未適用の更新プログラムが複数ある場合は、この手順を繰り返して対策します。

ポイント

更新プログラムの配布状況は、タスクの実行結果からも確認できます。配布に失敗していた場合は、タスク状態の詳細を確認して原因に対処してください。コンピュータへの適用状況は、セキュリティ画面の「更新プログラム一覧」画面の「未適用コンピュータ」タブから確認してください。

1.7.4 更新プログラムを手動で登録して配布する方法

組織内のコンピュータに即時適用する必要があるような緊急度の高い更新プログラムがリリースされた場合は、更新プログラムを手動で登録してから、配布して適用する必要があります。

ポイント

JP1/IT Desktop Management 2 では、日本マイクロソフト社からリリースされた更新プログラムを、セキュリティポリシーに従って自動的にコンピュータに配布、適用できます。ただし、サポートサービスサイトに更新プログラムの情報が登録され、更新プログラムを自動的に配布できるようになるには、更新プログラムのリリースから約 10 営業日の期間が必要です。

更新プログラムを手動で配布する流れを次に示します。

1. 配布する更新プログラムを準備する

配布する更新プログラムを、日本マイクロソフト社の Web サイトからダウンロードします。そして、更新プログラムの情報を JP1/IT Desktop Management 2 に登録する際に、更新プログラムファイルを作成します。また、特定の更新プログラムだけを適用させる運用にしている場合は、更新プログラムグループに更新プログラムを追加します。

2. 更新プログラムの適用状況を確認する

更新プログラムの適用状況を確認し、問題があった場合は原因の確認および対策を実施します。

(1) 配布する更新プログラムを準備する流れ

配布する更新プログラムの実行ファイルをダウンロードします。また、更新プログラムの情報を JP1/IT Desktop Management 2 に登録して、更新プログラムファイルを登録します。

1. 更新プログラムの実行ファイルをダウンロードする

更新プログラムを手動で登録して配布する場合、配布する更新プログラムの実行ファイルを、あらかじめ日本マイクロソフト社の Web サイトからダウンロードしておきます。

ポイント

更新プログラムの情報を確認するには、日本マイクロソフト社の Web サイトのトップページから、セキュリティのページ（セキュリティホーム）に移動して、目的の更新プログラムのリンクをクリックします。

2. 更新プログラムの情報および更新プログラムファイルを登録する

セキュリティ画面の［更新プログラム一覧］画面から、配布する更新プログラムの情報および更新プログラムファイルを登録します。更新プログラムの情報を登録すると、配布後に適用状況を確認できるようになります。また、更新プログラムファイルを登録すると、利用者のコンピュータに更新プログラムを配布するためのデータを登録できます。

注意事項

更新プログラムの配布時に実行されるコマンドは複数の種類があります。どの更新プログラムにどのコマンドを指定するかは、日本マイクロソフト社の Web サイトで更新プログラムの詳細情報を確認してください。

ポイント

特定の更新プログラムだけを適用させる運用にしている場合は、更新プログラムグループに更新プログラムを追加してください。更新プログラムグループが設定されているセキュリティポリシーの自動対策の設定に従って、対象のコンピュータに更新プログラムが適用されます。

関連リンク

- ・ [9.8.3 更新プログラム一覧へ更新プログラムを手動で追加する手順](#)

(2) 更新プログラムの適用状況を確認する流れ

更新プログラムの適用状況に問題があるかどうかは、セキュリティ画面の [セキュリティポリシー一覧] 画面の [更新プログラム] タブで確認できます。

機器のセキュリティ状況を確認した結果、危険レベルが「安全」であれば問題ありませんが、「警告」や「危険」の場合は更新プログラムが適用されていないおそれがあります。次の流れで状況把握および対策を実施します。

1. 更新プログラムの適用状況を把握する

[セキュリティポリシー一覧] 画面では問題の有無だけを確認できます。このため、どの更新プログラムの適用状況に問題があるかを確認するには、[セキュリティ詳細レポート] の [更新プログラムの適用状況] レポートを表示します。このレポートから、更新プログラムごとに未適用のコンピュータがある項目を確認できます。

2. 未適用の原因を確認する

レポートを確認した結果、コンピュータに更新プログラムが適用されていない場合、配布に失敗しているおそれがあります。配布 (ITDM 互換) 画面の [タスク一覧] 画面で、タスク種別が「自動対策で実行されるタスク (更新プログラムの対策)」のタスクを選択し、配布に失敗したコンピュータの状況を確認します。このとき、タスク状態の詳細を確認することで、配布がエラーになった原因を確認できます。

3. 更新プログラムの未適用を対策する

未適用のコンピュータに対して、更新プログラムを再配布できます。

セキュリティ画面の [セキュリティポリシー一覧] 画面の [更新プログラム] タブで、[操作] の [更新プログラムを配布 (ITDM 互換配布)] ボタンをクリックしてください。未適用のコンピュータに、更新プログラムが再配布されます。

ポイント

更新プログラムの再配布は、[機器のセキュリティ状態] 画面の [セキュリティ対策を実行] ボタンからも実行できます。

更新プログラムの適用状況の把握および対策が完了します。未適用の更新プログラムが複数ある場合は、この手順を繰り返して対策します。

ポイント

更新プログラムの配布状況は、タスクの実行結果からも確認できます。配布に失敗していた場合は、タスク状態の詳細を確認して原因に対処してください。コンピュータへの適用状況は、セキュリティ画面の [更新プログラム一覧] 画面の [未適用コンピュータ] タブから確認してください。

1.7.5 ウィルス感染時に対策状況を確認する

組織内で利用しているコンピュータでウィルス感染が検出された場合、ウィルス対策製品によってウィルスが検疫されたあとに、管理している全コンピュータのウィルス対策状況や利用状況が問題ないかどうかを確認する必要があります。

JP1/IT Desktop Management 2 を利用して、各コンピュータのウィルス対策状況や利用状況を確認できます。

1. ウィルスが発見されたコンピュータに問題がないか確認する

JP1/IT Desktop Management 2 でウィルスが発見されたコンピュータの機器情報を確認します。不正なソフトウェアがインストールされているなどの問題があった場合は、ウィルス感染の原因となっているおそれがあるため、適切な対策を実施します。

2. コンピュータのウィルス対策状況を確認する

組織内のコンピュータのウィルス対策状況を、JP1/IT Desktop Management 2 の [ウィルス対策製品の状況] レポートで確認します。

組織内のウィルス対策状況が確認できます。

関連リンク

- [1.7 セキュリティ状況の管理](#)
- [1.6.2 ウィルス感染時に機器のネットワーク接続を遮断する流れ](#)

(1) ウィルスが発見されたコンピュータに問題がないか確認する

組織内のコンピュータでウィルスが発見された場合、ウィルス対策製品によってウィルスが検疫されます。ウィルスが検疫されたあとは、JP1/IT Desktop Management 2 でウィルスの感染につながるような不審

なソフトウェアが利用されていないか、ウィルス対策状況が最新になっているかなどを確認する必要があります。

1. 利用者からウィルス感染の連絡を受け取る

管理対象のコンピュータの利用者から、ウィルス感染の連絡を受け取ります。感染したウィルスが、ウィルス対策製品によって検疫、駆除されていることを利用者に確認します。

2. 該当するコンピュータの情報を表示する

コンピュータの利用状況を確認するために、機器画面の[機器情報]画面で、ウィルスが発見されたコンピュータを表示します。

ポイント

[OS]、[利用者名]、[部署]、[設置場所]などの条件でフィルタを利用すると、目的のコンピュータを素早く探せます。

3. 不審なソフトウェアがインストールされていないか確認する

ウィルスをコンピュータにダウンロードしてしまうようなソフトウェアがインストールされていると、再度ウィルスの被害が発生するおそれがあります。[機器情報]画面の[インストールソフトウェア情報]タブでコンピュータにインストールされているソフトウェアを確認してください。

不審なソフトウェアがインストールされていた場合は、アンインストールを指示します。

4. ウィルス対策状況が最新かどうかを確認する

ウィルス対策状況が最新になっていないと、再度ウィルスに感染するおそれがあります。[機器情報]画面の[セキュリティ情報]タブで、ウィルス対策製品のエンジンバージョンやウィルス定義バージョンなどが最新になっているかどうかを確認してください。

また、必要に応じて、ウィルス対策製品の Web サイトでウィルスの情報や対処方法を確認します。

ウィルス対策状況に問題があった場合は、対象のコンピュータに適切な対策を行ってください。

5. ウィルススキャンを実施する

ウィルスに感染したファイルがコンピュータ内に残っていないかを確認するために、利用者に対してコンピュータ全体のウィルススキャンをするように指示します。スキャンの結果に問題がなければ、確認は完了です。

ウィルスが発見されたコンピュータに問題がないか確認できます。

関連リンク

- (2) [コンピュータのウィルス対策状況を確認する](#)

(2) コンピュータのウィルス対策状況を確認する

組織内のコンピュータでウィルスが発見された場合、ウィルス対策製品によってウィルスが検疫されます。検疫されたあとは、ウィルスによる被害を防止するため、組織内のコンピュータのウィルス対策状況が最新になっているかどうかを確認する必要があります。

コンピュータのウィルス対策状況は、[ウィルス対策製品の状況] レポートで確認できます。レポートには、「ウィルス対策ソフトウェアがインストールされているか」、「ウィルス定義ファイルが最新になっているか」などの情報が表示されます。

対策状況に問題があった場合は、対象のコンピュータを確認して適切な対策を行ってください。

上長やセキュリティ関連部署などに対策状況を報告する場合、レポートを出力して提出します。[ウィルス対策製品の状況] レポートで [印刷] ボタンをクリックすると、レポートを印刷できます。

1.7.6 許可したソフトウェアだけ利用できるようにする流れ

組織内のコンピュータには、業務で利用するさまざまなソフトウェアがインストールされています。組織内で利用できるソフトウェアを管理していない場合、情報漏えいやコンピュータウィルスの感染につながるおそれがあるソフトウェアがインストールされているおそれがあります。このような状況を防ぐため、組織内のコンピュータにどのようなソフトウェアがインストールされているかを把握して、使用を許可したソフトウェアだけを利用できるようにします。

JP1/IT Desktop Management 2 を利用すると、コンピュータにインストールされているソフトウェアの情報を管理できます。さらに、使用を禁止するソフトウェアを登録して、インストール状況を監視できます。オンライン管理のコンピュータの場合は、使用を禁止するソフトウェアの起動を抑止したり、自動的にアンインストールしたりできます。

ポイント

使用を禁止するソフトウェアだけでなく、使用を必須とするソフトウェアを登録して、インストール状況を監視できます。オンライン管理のコンピュータの場合は、使用を必須とするソフトウェアを自動的にインストールできます。

組織内のコンピュータにインストールされているソフトウェアを確認して、使用を許可したソフトウェアだけを利用できるように、ソフトウェアを管理する流れを次に示します。

1.最近インストールされたソフトウェアを確認する

JP1/IT Desktop Management 2 で、最近コンピュータに新しくインストールされたソフトウェアがないか確認します。新しくインストールされたソフトウェアがある場合は、業務に必要なソフトウェアか調査します。

2.ソフトウェアの利用を制限する

業務に不要なソフトウェアの場合は、JP1/IT Desktop Management 2 に使用禁止ソフトウェアとして登録して、利用を制限します。

また、今後使用禁止ソフトウェアがインストールされた場合は、自動的にアンインストールするように設定します。

使用を許可したソフトウェアだけが利用されている状況になります。

関連リンク

- 1.7 セキュリティ状況の管理

(1) 最近インストールされたソフトウェアを確認する流れ

組織内のコンピュータに、セキュリティ上問題のあるファイル共有ソフトウェアや、業務に関係のないソフトウェアがインストールされていないかを確認します。これらのソフトウェアがインストールされていると、情報漏えいにつながったり、コンピュータウィルスに感染したりするおそれがあります。そのため、コンピュータに新しくインストールされたソフトウェアがないか定期的に確認して、組織内にインストールされているソフトウェアを把握します。

コンピュータに新しくインストールされたソフトウェアがある場合は、ソフトウェアの情報を調査して、利用者に使用目的を確認します。

1. 新しくインストールされたソフトウェアを確認する

機器画面の【サマリ】－【ダッシュボード】画面に表示される【新規発見ソフトウェア】パネルで、最近コンピュータに新しくインストールされたソフトウェアがないか確認してください。新しくインストールされたソフトウェアがある場合は、業務に必要なソフトウェアか調査します。

2. ソフトウェアの情報を調査する

機器画面の【サマリ】－【ダッシュボード】画面に表示される【新規発見ソフトウェア】パネルに、最近コンピュータに新しくインストールされたソフトウェアが表示されます。ソフトウェア名のリンクをクリックすると、機器画面の【ソフトウェア情報】画面に移動します。【ソフトウェア情報】画面でソフトウェアの情報やソフトウェアをインストールしているコンピュータを確認してください。

また、インターネットなどを利用して、業務に必要なソフトウェアかどうかを調査します。業務に不要なソフトウェアだった場合は、利用者に使用目的を確認します。

3. 利用者に使用目的を確認する

機器画面の【ソフトウェア情報】画面で、【インストール済みコンピュータ】タブを選択してください。表示されたコンピュータの利用者に、業務に不要なソフトウェアがインストールされていることを連絡して、使用目的を確認します。

正当な理由と認められない場合は、ソフトウェアをアンインストールするように指示するか、配布機能を利用してソフトウェアをアンインストールします。また、使用を許可していないソフトウェアを今後インストールしないように利用者に注意します。

業務に不要なソフトウェアの場合は、使用禁止ソフトウェアとして登録して利用を制限します。

ポイント

操作ログを取得するように設定している場合は、セキュリティ画面の【操作ログ】画面でソフトウェアの利用形跡（プログラムの起動のログ）を調査できます。

関連リンク

- [12.3 コンピュータからソフトウェアをアンインストールする手順](#)
- [10.2 操作ログを確認する手順](#)

(2) ソフトウェアの利用を制限する流れ

コンピュータに新しくインストールされたソフトウェアが業務に不要なソフトウェアだった場合は、使用禁止ソフトウェアとして登録してソフトウェアの利用を制限します。

1.使用禁止ソフトウェアとして登録する

ソフトウェアの利用を制限するため、機器画面の［ソフトウェア情報］画面で、セキュリティポリシーに使用禁止ソフトウェアとして登録します。

ポイント

使用禁止ソフトウェアはセキュリティポリシー設定時に登録することもできます。

使用禁止ソフトウェアとして登録すると、レポート画面の［セキュリティ詳細レポート］画面－［使用禁止ソフトウェアのインストール状況］レポートでインストール状況を確認できるようになります。また、オンライン管理のコンピュータの場合は、使用禁止ソフトウェアの起動を抑止したり、自動的にアンインストールしたりできます。

2.使用禁止ソフトウェアのインストール状況を確認する

レポート画面の［セキュリティ詳細レポート］画面で、［使用禁止ソフトウェアのインストール状況］レポートを確認します。使用禁止ソフトウェアの利用傾向や対策状況について確認し、問題がある場合は対処してください。

ポイント

使用ソフトウェアのポリシーには使用必須ソフトウェアも登録できます。使用必須ソフトウェアを登録すると、［使用必須ソフトウェアのインストール状況］レポートでインストール状況を確認できるようになります。また、オンライン管理のコンピュータの場合は、使用必須ソフトウェアを自動的にインストールできます。

使用を許可したソフトウェアだけが利用されている状況になります。

関連リンク

- [6.20 使用禁止ソフトウェアを設定する手順](#)
- [9.3.1 セキュリティポリシーを追加する手順](#)

1.7.7 USB デバイスの使用を制限する

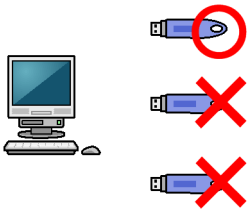
組織内のコンピュータには、顧客データ、売上データ、開発データなど、さまざまなデータがあります。これらの機密情報が外部に漏れると、多大な損失が生じ、組織の社会的信用も失墜します。そのため、データの持ち出しやデータの紛失などから機密情報を守るために、セキュリティ対策を実施する必要があります。

JP1/IT Desktop Management 2 を利用すると、デバイスの使用を抑止できます。これによって持ち出しによる情報漏えいを防げます。

ここでは、USB デバイスの使用を制限する方法について説明します。USB デバイスの使用を制限する方法には、次の 2 つがあります。

- 登録した USB デバイスだけ使用を許可する
- 特定のコンピュータだけ USB デバイスの使用を許可する

登録したUSBデバイスだけ使用を許可する



特定のコンピュータだけUSBデバイスの使用を許可する



ここでは、USB デバイスを貸し出し制にして、個人が所有している USB デバイスは使用できないようにする場合の流れについて説明します。

1.使用を許可する USB デバイスを登録する

貸し出し用の USB デバイスを準備して、JP1/IT Desktop Management 2 に使用を許可する USB デバイスとして登録します。

2.許可した USB デバイス以外の使用を抑止する

JP1/IT Desktop Management 2 で USB デバイスの読み取り・書き込みを抑止します。このとき、手順 1.で登録した USB デバイスだけは使用を許可するようにします。

3.USB デバイスを貸し出す

USB デバイスの使用を希望する利用者から申請書を提出してもらい、内容を確認して USB デバイスを貸し出します。

USB デバイスの貸し出し、返却のタイミングで、JP1/IT Desktop Management 2 で USB デバイスの資産状態を変更します。

4.USB デバイスの使用履歴を確認する

申請された内容どおりに USB デバイスが使用されたか確認します。

USB デバイスの使用状況が適切に管理され、不要なデータの持ち出しがなくなります。

関連リンク

- (5) 特定のコンピュータだけデータの持ち出しを許可する
- 1.7 セキュリティ状況の管理
- (6) USB デバイスの紛失に対応する

(1) 使用を許可する USB デバイスを登録する

持ち出しによる情報漏えいを防ぐために、特定の USB デバイスだけ使用を許可し、それ以外の USB デバイスを利用できないようにします。例えば、組織で所有する USB デバイスだけを利用できるようにし、個人が所有している USB デバイスは使用できないように抑止できます。

特定の USB デバイスだけ使用を許可するためには、まず使用を許可する USB デバイスを登録する必要があります。

1.USB デバイスを登録する

貸し出し用の USB デバイスを準備して、使用を許可する USB デバイスとして登録します。登録時には、誰が USB デバイスを登録したかわかるように、登録者の利用者情報を設定します。

USB デバイスを登録すると、資産画面の [ハードウェア資産] 画面に、USB デバイスのハードウェア資産情報が登録されます。

ポイント

利用者に USB デバイスを登録してもらいたい場合は、あらかじめエージェント設定に USB デバイス登録用の認証情報を設定し、そのエージェント設定をコンピュータに割り当てておきます。管理者は、必要に応じて利用者に認証情報と登録方法を連絡して、USB デバイスを登録してもらいます。

2.ハードウェア資産情報を編集する

登録された USB デバイスのハードウェア資産情報は、[資産状態] が「未確認」になっています。また、USB デバイスから収集できた情報および登録時に設定した利用者情報だけが登録されています。このため、自動的に収集されない [資産管理番号]、[資産状態] (在庫) などを手動で登録します。[資産状態] を「未確認」および「滅却」以外にすると、使用を許可する USB デバイスとして登録されます。

使用を許可する USB デバイスが登録されます。

関連リンク

- 9.7 USB デバイスを登録する手順

- [11.1.2 ハードウェア資産情報を編集する手順](#)
- (2) 許可した USB デバイス以外の使用を抑止する

(2) 許可した USB デバイス以外の使用を抑止する

持ち出しによる情報漏えいを防ぐために、特定の USB デバイスだけ使用を許可し、それ以外の USB デバイスを利用できないようにします。例えば、組織で所有する USB デバイスだけを利用できるようにし、個人が所有している USB デバイスは使用できないように抑止できます。

使用を許可する USB デバイスを登録したあとは、それ以外の USB デバイスの使用を抑止する必要があります。

禁止操作のポリシーを設定する

許可した USB デバイス以外の使用を抑止するため、禁止操作のポリシーを設定します。このとき、登録した USB デバイスだけは使用を許可するようにします。

使用を許可する USB デバイス以外は、使用が抑止されます。

関連リンク

- [9.6 デバイスの使用を抑止する手順](#)
- (1) 使用を許可する USB デバイスを登録する

(3) USB デバイスを利用者に貸し出す

組織で所有する USB デバイス（JP1/IT Desktop Management 2 に登録済みの USB デバイス）だけを利用できるようにしている場合、利用者が USB デバイスを利用するときは貸し出す必要があります。この場合、利用者から利用申請を提出してもらい、使用目的が妥当な場合は USB デバイスを貸し出します。

1. 利用申請を提出してもらう

USB デバイスの貸し出しを管理するために、次に示すような情報を入手してください。

- 使用日
- 返却日
- 使用目的
- 部署
- 利用者名
- メールアドレス
- 電話番号
- USB デバイスを使用するコンピュータの資産管理番号
- USB デバイスに書き込むデータのファイル名

2.USB デバイスを利用者に貸し出す

使用目的が妥当な場合は、USB デバイスを利用者に貸し出します。

USB デバイスの貸出先を管理するためには、資産情報を編集して、利用者情報を貸出先の利用者のものにします。USB デバイスの利用者情報を変更したくない場合は、貸出先を管理するための管理項目を追加したり、[ノート] タブに貸し出し日と貸し出し先などの履歴を保存したりしてください。

USB デバイスを貸し出したあとは、その USB デバイスが貸し出し中であることがわかるように、ハードウェア資産情報の [資産状態] に「貸出中」などの状態を新規追加して、[資産状態] を変更します。また、返却予定を把握するため、[予定資産状態] と [変更予定日] を設定します。1 週間後に返却される予定の場合は、[予定資産状態] に「在庫」を、[変更予定日] に 1 週間後の日付を設定します。

ポイント

[予定資産状態] を設定すると、ダイジェストレポートの [ハードウェア資産の予定] で、返却予定の USB デバイスを確認できるようになります。

USB デバイスの使用が終わったら、利用者から USB デバイスを返却してもらいます。

返却時は、ハードウェア資産情報の [資産状態] を「貸出中」から「在庫」に変更して、いつでも貸し出せる状態に戻します。

関連リンク

- [11.1.6 資産状態を変更する手順](#)
- [11.1.7 予定資産状態を変更する手順](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [15.4.1 資産管理項目を追加する手順](#)

(4) USB デバイスの使用履歴を確認する

USB デバイスが使用された履歴は、操作ログで確認できます。

ポイント

操作ログを取得するには、セットアップ時に操作ログの設定をする必要があります。また、操作ログのポリシーを有効にしている必要があります。

1.利用者の操作ログを表示する

操作ログは、セキュリティ画面の [操作ログ] 画面から確認できます。USB デバイスの履歴を確認するためには、フィルタを利用して [操作種別] が「デバイス操作」の操作ログを確認してください。特定の USB デバイスの使用履歴を確認する場合は、[発生元] や [ユーザー名]などで操作ログをフィルタリングしてください。

2.操作ログの詳細情報を確認する

USB デバイスが適正に使用されたかどうかを確認するためには、操作ログの詳細情報を確認します。次の情報を確認してください。

- USB デバイスを操作したコンピュータの情報
- USB デバイスを操作したユーザーの情報
- USB デバイスにコピーしたファイルの情報

USB デバイスが適切に利用されたかどうかを確認できます。使用状況に問題があった場合は、利用者に状況を確認して対処してください。

関連リンク

- [10.4 不審操作のログを確認する手順](#)

(5) 特定のコンピュータだけデータの持ち出しを許可する

不要なデータの持ち出しによる情報漏えいを防ぐため、USB デバイスの使用を制限できます。

USB デバイスの使用を制限する方法の一つとして、特定のコンピュータだけデータの持ち出しを許可する方法があります。例えば、共有コンピュータだけ USB デバイスの使用を許可し、個人のコンピュータでは USB デバイスを使用できないように運用できます。

ここでは、特定のコンピュータだけ USB デバイスの使用を許可する方法について説明します。

1.すべてのコンピュータに USB デバイスの使用を抑止するポリシーを割り当てる

USB デバイスの使用を抑止するセキュリティポリシーをすべてのコンピュータに適用します。

禁止操作のポリシーで USB デバイスの抑止を有効にしたセキュリティポリシーを作成して、すべてのコンピュータに割り当ててください。

2.USB デバイスの使用を許可するコンピュータに専用のポリシーを割り当てる

USB デバイスの使用を許可するコンピュータ専用のセキュリティポリシーを適用します。

禁止操作のポリシーで USB デバイスの抑止を無効にしたセキュリティポリシーを作成して、USB デバイスの使用を許可するコンピュータに割り当ててください。

特定のコンピュータだけ USB デバイスが使用できるようになります。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [1.7.7 USB デバイスの使用を制限する](#)
- [\(6\) USB デバイスの紛失に対応する](#)

(6) USB デバイスの紛失に対応する

万が一、組織で利用している USB デバイスを紛失してしまった場合、USB デバイスに顧客データ、売上データ、開発データなどの機密情報が格納されていると、情報漏えいにつながるおそれがあります。このため、USB デバイスを紛失してしまった場合は早急に対策が必要です。

禁止操作のポリシーで次の設定をしている場合は、USB デバイスに格納されていたファイルの情報を確認できます。

- USB デバイスの使用抑止設定が有効
- [登録済みの USB デバイスは使用を許可する] を選択
- [許可された USB デバイスに格納されているファイル一覧を取得する] にチェック

紛失した USB デバイスに、機密情報を含むファイルが格納されていなかったか確認してください。

USB デバイスの格納ファイルを確認する

資産画面の [ハードウェア資産] 画面に表示される [格納ファイル一覧] タブで、USB デバイスに格納されていたファイルの情報を確認できます。なお、[格納ファイル一覧] タブは対象の USB デバイスが登録されていて [機器種別] が「USB デバイス」の場合だけ表示されます。[ファイルパス] や [更新日時] から格納されていたファイルを特定して、ファイルの詳細な内容を調査してください。

ポイント

[格納ファイル一覧] タブに表示される情報は、最後に USB デバイスをコンピュータに接続したときに、USB デバイスに格納されていたファイルの情報です。それ以降に外部のコンピュータから USB デバイスに格納したファイルがある場合は、紛失者にファイルの内容を確認してください。

また、USB デバイスの紛失が発生した事実を残すため、USB デバイスのハードウェア資産情報に紛失に関する情報を登録します。

紛失に関する情報を登録する

紛失した USB デバイスを使用できないようにするために、資産画面の [ハードウェア資産] 画面で、紛失した USB デバイスの [資産状態] を「滅却」に変更します。すると、その USB デバイスは未登録として扱われ、禁止操作のセキュリティポリシーが適用されたコンピュータで読み取りと書き込みができなくなります。

また、[ノート] タブに紛失日時、紛失者、紛失経緯などの情報を保存します。

ポイント

情報漏えいにつながるような問題が発生した場合は、全従業員に事例を展開して、セキュリティ対策を徹底するように通知しましょう。

関連リンク

- [11.1.6 資産状態を変更する手順](#)

1.7.8 セキュリティ監査に対応する流れ

組織のセキュリティ監査を実施する場合、組織内の環境がセキュリティのルールに従っているかどうか、セキュリティ管理に関する問題が発生していないか、問題が発生した場合は対処済みかどうかなどを確認する必要があります。

JP1/IT Desktop Management 2 を利用してセキュリティを管理している場合、次に示す情報を出力して、セキュリティ管理が正しく行われていることを確認できます。

セキュリティポリシーの判定結果

セキュリティポリシーの遵守状況を確認できます。

セキュリティ管理に関するイベント

セキュリティ管理に関して発生した問題を確認できます。セキュリティポリシーの遵守状況に問題がなければ、これらの問題は対処済みであることを確認できます。

禁止操作の抑止状況

セキュリティポリシーに基づいて禁止操作が抑止されていることを確認できます。

ネットワークに接続しているコンピュータの一覧

管理対象のコンピュータの一覧を作成することで、セキュリティ管理の対象となるコンピュータを確認できます。

セキュリティ監査に対応する流れを次に示します。

1. セキュリティポリシーの判定結果を出力する

JP1/IT Desktop Management 2 で、セキュリティ詳細レポートの [危険レベルの状況] レポートを出力します。

2. セキュリティ管理に関するイベントを出力する

JP1/IT Desktop Management 2 で、セキュリティ管理に関するイベントを出力します。

3. 禁止操作の抑止状況を出力する

JP1/IT Desktop Management 2 で、セキュリティ詳細レポートの [禁止操作の状況] レポートを出力します。

4. 管理対象のコンピュータの一覧を出力する

JP1/IT Desktop Management 2 で、管理対象のコンピュータの一覧を出力します。

セキュリティ監査時に、出力した情報を提出します。

関連リンク

- [1.7 セキュリティ状況の管理](#)

(1) セキュリティポリシーの判定結果を出力する流れ

セキュリティ監査や上長への状況報告などで、セキュリティポリシーの遵守状況を提示するためには、セキュリティ詳細レポートの「危険レベルの状況」レポートを確認して印刷します。

1. 「危険レベルの状況」レポートを確認する

セキュリティポリシーの遵守状況を確認するため、レポート画面の「セキュリティ詳細レポート」で「危険レベルの状況」レポートを表示します。

すべての機器の危険レベルが「安全」であるか確認してください。「安全」以外の機器がある場合は、「内訳」に表示されている台数のリンクをクリックして、該当する機器の状況を確認したあと必要に応じて対策します。

2. 「危険レベルの状況」レポートを印刷する

「危険レベルの状況」レポートの「印刷」ボタンをクリックして、レポートを出力します。

必要に応じて、印刷したレポートを提出します。

関連リンク

- [1.7.2 セキュリティポリシー違反を対策する](#)
- [9.3.1 セキュリティポリシーを追加する手順](#)

(2) セキュリティ管理に関するイベントを出力する流れ

セキュリティ監査や上長への状況報告などで、セキュリティ管理に関する問題の発生状況と対処状況を提示するためには、セキュリティ管理に関するイベントを確認して印刷します。セキュリティポリシーの遵守状況に問題がなければ、イベントで確認できる問題は対処済みになっています。

1. セキュリティ管理のイベントを確認する

セキュリティ管理に関する問題が発生していないか、問題が発生した場合は対処済みかをイベント画面で確認します。

フィルタを利用して、「種類」が「セキュリティ」のイベントを確認してください。「重大度」が「緊急」または「警戒」のイベントで、「確認状態」が「未確認」のイベントがある場合は、エラーの内容から原因を特定して対処します。対処が完了したら、「確認状態」を「確認済」に切り替えます。

ポイント

この場合、問題に対処したらイベントの状態を「確認済」に変更するように運用している必要があります。

2. セキュリティ管理のイベント情報を印刷する

セキュリティ管理のイベント情報をエクスポートして、出力された CSV ファイルを印刷します。

必要に応じて、印刷したイベント情報を提出します。

関連リンク

- [13.2 イベント情報をエクスポートする手順](#)
- [13.1 イベントの詳細を確認する手順](#)

(3) 禁止操作の抑止状況を出力する流れ

セキュリティ監査や上長への状況報告などで、セキュリティポリシーに基づいて禁止操作が行われていないことを提示するためには、セキュリティ詳細レポートの「禁止操作の状況」レポートで、セキュリティポリシーに基づいて禁止操作が抑止されていることを確認して印刷します。

ポイント

禁止操作を抑止するためには、事前にセキュリティポリシーで抑止する操作を設定しておく必要があります。

1. 「禁止操作の状況」レポートを確認する

禁止操作の抑止状況を確認するため、レポート画面から「セキュリティ詳細レポート」－「禁止操作の状況」レポートを表示します。

「禁止操作の状況」レポートでは、印刷の抑止状況、ソフトウェアの起動抑止状況、および機器の使用抑止状況を確認できます。

不自然に抑止回数が多い場合は、利用者に事情を確認するなどして、セキュリティ上の問題がないか調査します。

2. 「禁止操作の状況」レポートを印刷する

「禁止操作の状況」レポートの「印刷」ボタンをクリックして、レポートを印刷します。

必要に応じて、印刷したレポートを提出します。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)

(4) 管理対象のコンピュータの一覧を出力する

セキュリティ監査や上長への状況報告などで、セキュリティ管理の対象となっているコンピュータを提示するためには、管理対象のコンピュータの一覧を出力します。

ポイント

管理対象のコンピュータには、特定のセキュリティポリシーを割り当てていなくても、デフォルトポリシーが自動的に割り当てられます。このため、管理対象のコンピュータの一覧を出力することで、セキュリティ管理の対象となるコンピュータの一覧を提示できます。

機器画面の［機器情報］画面で、コンピュータだけをフィルタで表示して機器情報をエクスポートします。その後、エクスポートした CSV ファイルを印刷します。

必要に応じて、印刷したコンピュータの一覧を提出します。

関連リンク

- [6.17 機器情報をエクスポートする手順](#)
- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.5 セキュリティポリシーを割り当てる手順](#)

1.8 情報漏えい起きていないか確認する

情報漏えいが発生した場合、組織の重要データが外部に漏れるだけでなく、組織の社会的信頼の失墜につながりかねません。

情報漏えいにつながるような不審な操作があった場合は、早急に調査をして問題の有無を把握する必要があります。JP1/IT Desktop Management 2 では、不審操作の発生を検知して、自動的に管理者にメール通知できます。これによって、発生した不審操作をタイムリーに調査できます。

また、情報漏えいは外部からの侵入者による情報持ち出しによっても発生するおそれがあります。もし、そのような事態が発生した場合は、コンピュータから情報が持ち出された形跡を調査して、問題の有無を早急に確認する必要があります。JP1/IT Desktop Management 2 では、各コンピュータから収集した操作のログを調査できるほか、外部から持ち込まれたコンピュータがネットワークに接続された形跡を確認したり、各コンピュータの不正アクセスに関するセキュリティ設定の状況を確認したりできます。

関連リンク

- [1.8.1 検知された不審操作を調査する流れ](#)
- [1.8.2 情報が持ち出された形跡を調査する流れ](#)
- [1.7 セキュリティ状況の管理](#)

1.8.1 検知された不審操作を調査する流れ

情報漏えいにつながるような操作をタイムリーに調査するためには、不審な操作があったことを管理者が即座に把握して、状況を素早く調査できる必要があります。

JP1/IT Desktop Management 2 を利用して、不審操作が検知されたら自動的に管理者にメール通知されるようにしておくことで、不審操作の発生を即座に把握できます。また、各コンピュータから収集された操作ログを基に、持ち出したデータの出所や最初に持ち出した利用者などを確認できます。

検知された不審操作を調査する流れを次に示します。

1.不審操作の自動通知を設定する

不審操作が検知された場合に、管理者へ自動的にメール通知されるように設定します。

2.不審操作を調査する

不審操作が検知されたら検知内容を確認し、問題がある場合は操作ログも確認します。

検知された不審操作の内容を調査して、問題の有無を確認できます。

なお、不審操作を検知するためには、操作ログを収集してセキュリティポリシーに検知の条件を設定している必要があります。

- 10.4 不審操作のログを確認する手順

不審操作が検知された場合に、管理者へ自動的にメール通知されるように設定します。

不審操作の自動通知を設定するには：

- メールで通知される内容を次に示します。



イベントの発生を確認したら、メールに記載された URL から JP1/IT Desktop Management 2 の操作画面を起動して、セキュリティ状況を確認して対策してください。

関連リンク

- ・ [9.1 セキュリティ状況を確認する](#)

(2) 不審操作を調査する流れ

不審操作が検知されたら検知内容を確認し、問題がある場合は操作ログも確認します。

ファイル持ち出しによる不審操作の場合は、次の流れで不審操作を調査してください。印刷による不審操作の場合は、操作ログで調査してください。操作ログでの調査については、「[\(1\) 操作ログを確認する](#)」を参照してください。

1. 検知内容を確認する

不審操作が検知されると、[種類] が「不審操作」のイベントが発生します。このイベントの発生状況は、ホーム画面の [イベントの状況] パネルに表示される [不審操作] の件数から確認できます。

[イベントの状況] パネルで括弧内の件数のリンクをクリックすると、イベント画面に移動して、[種類] が「不審操作」で [確認状態] が「未確認」のイベントを確認できます。

イベントの一覧で [内容] 欄のリンクをクリックすると、表示されるダイアログで検知された操作ログの内容を確認できます。ここで表示される内容から、情報漏えいの調査が必要かどうかを判断してください。調査が必要と判断した場合は、イベントの一覧で [発生元] 欄のリンクをクリックしてください。セキュリティ画面の [操作ログ] 画面に移動して、関連する操作ログを確認できます。

2. 操作ログを追跡調査する

セキュリティ画面の [操作ログ] 画面で操作ログを追跡調査できます。

操作ログを追跡調査するには、追跡調査したい操作の [追跡] ボタンをクリックして、表示される [操作の追跡] ダイアログの情報を確認してください。なお、[追跡] ボタンが非活性の操作ログは、追跡調査の対象外のログです。

[操作の追跡] ダイアログでは、選択した操作ログが含まれる一連の操作の流れに対して、最初に行われた操作と最後に行われた操作を確認できます。例えば、USB デバイスへのファイルコピーが検知された場合は、どこに格納されていたデータを持ち出したか（最初の操作）、最終的に USB デバイスへコピーしたか（最後の操作）がわかります。これによって、重要データが持ち出されたかどうかを確認できます。

不審操作の追跡調査が完了します。

調査の結果、情報漏えいが発生したおそれがある場合は、操作した利用者に状況を確認して対策を検討します。

1.8.2 情報が持ち出された形跡を調査する流れ

情報が持ち出されたおそれがある場合は、形跡を調査して問題の有無を早急に確認する必要があります。

JP1/IT Desktop Management 2 を利用することで、各コンピュータが操作された形跡がないか、不明な機器がネットワークに接続されていないか、各コンピュータに不正アクセスに関するセキュリティ設定がされているかを調査できます。

情報が持ち出された形跡を調査する流れを次に示します。

1. 操作ログを確認する

各コンピュータから収集された操作ログを確認することで、各コンピュータの操作状況を確認できます。第三者によるログインの形跡や不審な持ち出し操作があった場合は、操作ログから持ち出されたデータを確認して対処を検討する必要があります。

2. 新規に接続された機器を確認する

不明な機器が組織内のネットワークに接続されている場合、その機器から情報が漏えいするおそれがあります。ネットワークを探索することで、組織内のネットワークに新規に接続された機器がないかどうかを確認できます。

3. コンピュータのセキュリティ設定を確認する

コンピュータに不正アクセスできるようになっていると、第三者にコンピュータを操作されて情報漏えいが発生するおそれがあります。管理対象のコンピュータのセキュリティ設定を確認して、問題があった場合は対策します。

情報が持ち出された形跡がないかどうかを確認できます。

(1) 操作ログを確認する

各コンピュータから収集された操作ログを確認することで、各コンピュータの操作状況を確認できます。第三者によるログインの形跡や不審な持ち出し操作があった場合は、操作ログから持ち出されたデータを確認して対処を検討する必要があります。

操作ログは、セキュリティ画面の [操作ログ] - [操作ログ一覧] 画面で確認できます。

データベースに存在しない操作ログは、管理用サーバに過去の操作ログを取り込んで確認します。すべての操作ログを取り込むと時間が掛かるため、持ち出されたデータの中から持ち出したコンピュータを絞り込んでから、取り込んでください。

収集された操作ログは、一つ一つ追跡調査する必要があります。このため、調査の際は幾つかの観点で対象の操作ログを絞り込むことをお勧めします。例えば、情報持ち出しが発生したおそれがある場合に操作ログを調査するときは、次のような観点で操作ログを確認します。

操作された時間帯のログを確認する

持ち出しに関する操作が発生した時間帯がわかっている場合は、はじめに時間帯で操作ログを絞り込んでおくと、効率良く操作ログを確認できます。操作ログの一覧で、フィルタの条件に [操作時刻] と時間帯を指定することで、確認したい操作ログを時間軸で絞り込めます。

操作の種類を限定してログを確認する

持ち出しに関連する操作だけに絞り込むことで、効率良く操作ログを確認できます。操作ログの一覧のフィルタで、例えば次のような条件を指定します。

- [操作種別] が [ファイル操作]、[印刷操作]、[デバイス操作]
- [操作種別 (詳細)] が [ログオン]、[ファイルコピー]、[ファイルアップロード]、[ファイル送信]、[デバイス区分]

また、[発生元]、[部署]、[設置場所]、[ユーザー名] などの条件でフィルタを利用して、持ち出したコンピュータを絞り込んでください。

持ち出されたコンピュータを基に確認する

重要データが保管されているサーバや NAS など、特定のコンピュータから持ち出されていないかどうかを確認できます。操作ログの一覧で、フィルタの条件に [発生元] とコンピュータ名を指定することで、特定のコンピュータから情報が持ち出されていないかどうかを確認できます。

確認の結果、持ち出しが発生したおそれがある場合は、操作ログが取得されたコンピュータの利用者に状況を確認して対策を検討します。

関連リンク

- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [10.7.2 コンピュータを選択して操作ログを取り込む手順](#)

(2) 新規に接続された機器を確認する

不明な機器が組織内のネットワークに接続されている場合、その機器から情報が漏えいするおそれがあります。ネットワークを探索することで、組織内のネットワークに新規に接続された機器がないかどうかを確認できます。

探索結果は、設定画面の [機器の探索] - [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。

[ネットワークの探索] 画面に表示された機器に、不明な機器がないかどうかを確認してください。[探索履歴の確認] の一覧で、[今回新規発見] のフィルタを利用すると、新規接続された機器を素早く確認できます。

不明な機器があった場合は、ネットワークアドレスを基に機器を確認します。

関連リンク

- [6.4 ネットワークに接続されている機器を探索する手順](#)

(3) コンピュータのセキュリティ設定を確認する

コンピュータに不正アクセスできるようになっていると、情報漏えいが発生するおそれがあります。管理対象のコンピュータのセキュリティ設定を確認して、問題があった場合は対策してください。

コンピュータのセキュリティ設定の状況は、セキュリティ画面の[機器のセキュリティ状態]－[機器一覧]画面で確認します。危険レベルが「危険」、「警告」、または「注意」の場合、そのコンピュータはセキュリティ設定に問題があるおそれがあります。[機器一覧]画面で確認したい機器を選択して、[OSのセキュリティ設定]タブまたは[ユーザー定義のセキュリティ設定]タブを選択すると、セキュリティ設定項目ごとに安全な状態かどうかを確認できます。

安全ではないセキュリティ設定があった場合は、強制的に設定を変更して対策できます。[セキュリティ対策を実行]ボタンをクリックして、表示されるダイアログで対策したい項目を選択して[OK]ボタンをクリックしてください。

ポイント

セキュリティ設定の状況は、セキュリティ詳細レポートからも確認できます。セキュリティ設定に関するセキュリティ詳細レポートを表示するには、レポート画面の[セキュリティ詳細レポート]－[セキュリティ設定の状況]を選択してください。

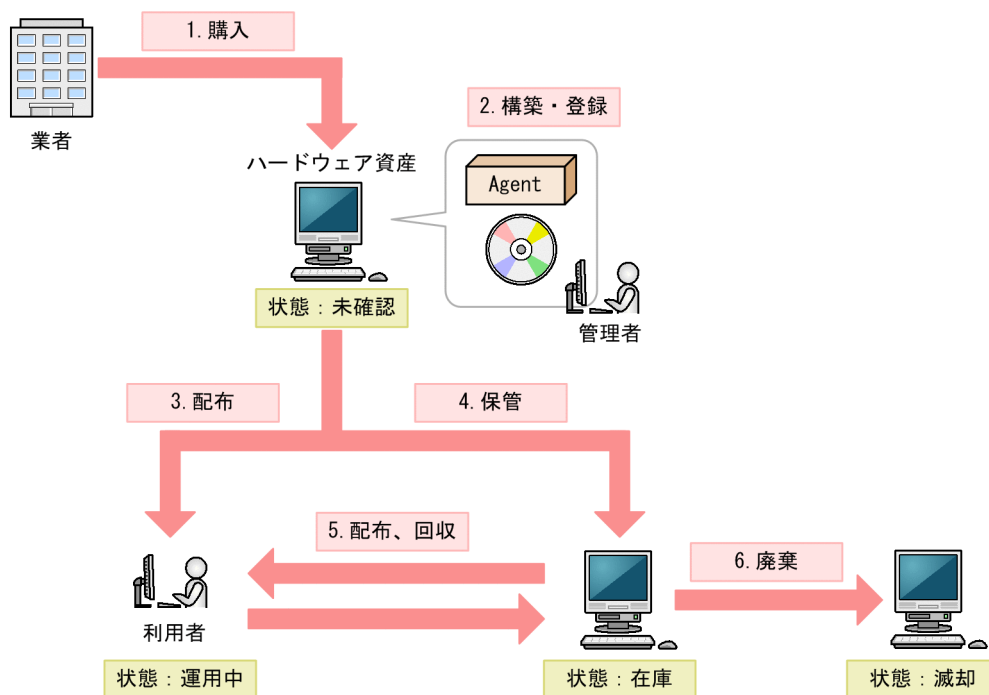
1.9 ハードウェア資産を管理する

組織内には、コンピュータ、サーバ、スマートデバイス、プリンタ、ネットワーク装置、USB デバイスなど、業務で利用するさまざまなハードウェア資産があります。組織の運用に応じた定期的な機器の入れ替えや突発的なトラブルに対応するためには、ハードウェア資産の状況把握が必要です。

JP1/IT Desktop Management 2 を利用すると、次に示すような機能を使って効率良くハードウェア資産を管理できます。

- 所有している資産を台帳のように一覧で把握できる
- パネルやレポートなどのグラフィカルな画面から、資産の状況を簡単に把握できる
- フィルタを活用して、作業対象のハードウェア資産の情報を素早く把握できる

ハードウェア資産の管理は、資産画面の［ハードウェア資産］画面で実行します。ハードウェア資産を管理するためには、ハードウェア資産情報を登録し、ハードウェア資産を管理する流れに沿って情報をメンテナンスしていきます。ハードウェア資産を管理する流れを次の図に示します。



（凡例）

Agent：エージェント

ハードウェア資産を購入したら、ハードウェア資産の環境を構築し、ハードウェア資産情報を登録します。その後、ハードウェア資産を利用者に配布します。ハードウェア資産を利用しない場合は在庫として保管しておきます。リプレースや代替機貸し出しなどの運用に応じて、使用中のハードウェア資産を回収したり、在庫のハードウェア資産を配布したりします。ハードウェア資産が不要になった場合は、滅却処理をして廃棄します。

ここでは、次に示す業務での JP1/IT Desktop Management 2 の利用方法を説明しています。

機器を購入する

従業員の増加や設備の追加などに伴って組織内に新しい機器を購入します。購入した機器の情報を JP1/IT Desktop Management 2 に登録して、資産管理できるようにします。

機器をリプレースする

従業員の異動や機器の入れ替えなどに伴って組織内の機器をリプレースします。

機器を棚卸する

組織内の機器を棚卸します。

利用されていない機器を確認する

組織内の余剰資産を確認します。

機器を滅却する

古い機器を職場から回収して滅却します。

機器の障害に対応する

組織内の機器に障害が発生した場合に、保守サービスに修理を依頼したり、代替機を貸し出したりします。

関連リンク

- [1.9.3 機器を購入する流れ](#)
- [1.9.4 機器をリプレースする流れ](#)
- [1.9.5 機器を棚卸する流れ](#)
- [1.9.6 利用されていない機器を確認する流れ](#)
- [1.9.7 機器を滅却する流れ](#)
- [1.9.8 機器の障害に対応する流れ](#)

1.9.1 手持ちの管理台帳の情報を登録する

手持ちの管理台帳をインポートして、ハードウェア資産情報を一括登録できます。

1.インポートする CSV ファイルを用意する

資産情報をインポートするために、管理台帳のデータをあらかじめ CSV ファイルに変換しておきます。

2.管理台帳をインポートする

管理台帳をインポートすることで、管理台帳上の情報をハードウェア資産情報に登録できます。資産情報をインポートする方法については、「[11.4.1 ハードウェア資産情報をインポートする手順](#)」を参照してください。

資産情報をインポートするときには、管理台帳上の項目と JP1/IT Desktop Management 2 の資産管理項目の対応づけを設定します。これによって、管理台帳上のすべての情報を JP1/IT Desktop Management 2 の資産管理項目にインポートできます。

ポイント

管理台帳上の項目の並び順や項目名を変更することなく対応づけを設定できます。また、対応する項目がない場合は、インポート時に資産管理項目を新規に作成して対応づけできます。

事前に、JP1/IT Desktop Management 2 の管理対象にした機器がある場合は、機器情報が収集され、機器に対応したハードウェア資産情報が自動的に登録されます。

インポートするときは、インポートする情報と登録されているハードウェア資産情報を対応づけるための [マッピングキー] を指定します。インポートを実行すると、管理台帳と JP1/IT Desktop Management 2 のハードウェア資産情報でマッピングキーが一致したものは、資産情報が更新されます。管理台帳にマッピングキーが一致しない情報があつた場合は、新規のハードウェア資産情報として登録されます。

マッピングキーは次の項目から選択できます。ハードウェア資産を一意に特定できる項目を指定してください。

- 資産管理番号
- シリアルナンバー※
- IP アドレス
- MAC アドレス
- ホスト名
- IMEI
- 契約電話番号

注※ BIOS 情報のシリアルナンバーです。

注意事項

マッピングキーに指定する項目は、JP1/IT Desktop Management 2 とインポートする管理台帳の両方に値が存在する項目にしてください。例えば、管理台帳に [シリアルナンバー] が掲載されていても、ハードウェア資産情報に [シリアルナンバー] の値が登録されていない場合は、インポートしても正しく情報が対応づけられません。この場合、管理台帳上のハードウェア資産がすべて新規のハードウェア資産情報として登録されてしまいます。

3.インポート結果を確認する

インポート後は、資産画面の [ハードウェア資産] 画面で、管理台帳の情報がハードウェア資産情報に正しく登録されているかどうかを確認してください。

登録済みのハードウェア資産情報を更新する場合に、インポート実行後に [資産状態] が「未確認」のハードウェア資産情報があるときは、その資産は管理台帳に情報が登録されていなかったか、マッピングキーが一致しなかったおそれがあります。

管理台帳に情報が登録されていなかった資産は、手動で資産情報を登録してください。マッピングキーが一致していなかった場合は、別のハードウェア資産として新規登録されているので、ハードウェア資産情報と機器の対応づけを確認、変更して不要な方の情報を削除してください。

インポートが完了し、管理台帳の情報がハードウェア資産情報に登録されます。

ハードウェア資産情報の登録が完了したら、運用に応じて資産情報をメンテナンスしていきます。なお、ハードウェア資産情報が機器情報と関連づいている場合、ハードウェア資産情報のうちの「機器情報」は、収集された機器情報で自動的に更新されます。

関連リンク

- [11.1.14 ハードウェア資産情報に対応する機器情報を変更する手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)

1.9.2 ハードウェア資産情報をメンテナンスする方法

ハードウェア資産情報は、運用に応じてメンテナンスして最新状態に保つようにします。ハードウェア資産情報をメンテナンスするには、次の3つの方法があります。

ポイント

ハードウェア資産情報が機器情報と関連づいている場合、ハードウェア資産情報のうちの「機器情報」は、収集された機器情報で自動的に更新されます。

インポートを利用して一括編集する

ハードウェア資産情報の CSV ファイルをインポートして、ハードウェア資産情報を一括で更新できます。

ハードウェア資産情報の CSV ファイルは、ハードウェア資産情報をエクスポートすることで作成できます。出力された CSV ファイルを編集しインポートすることで、ハードウェア資産情報を更新できます。

ハードウェア資産情報をエクスポートする方法については、「[11.5 資産情報をエクスポートする手順](#)」を参照してください。ハードウェア資産情報をインポートする方法については、「[11.4.1 ハードウェア資産情報をインポートする手順](#)」を参照してください。

注意事項

ハードウェア資産情報をエクスポートするときは、インポート時にハードウェア資産情報を一意に判別できる項目（マッピングキーになる項目）を1つ以上エクスポートしておく必要があります。マッピングキーになる項目は、[資産管理番号]、[シリアルナンバー]、[IP アドレス]、[MAC アドレス]、[ホスト名]、[IMEI]、[契約電話番号] です。

手動で編集する

ハードウェア資産情報を手動で登録する場合、資産画面の[ハードウェア資産]画面で、情報を登録したい資産を選択して[編集]ボタンをクリックします。表示されたダイアログで、資産情報を登録できます。複数の資産を選択して、一括で登録することもできます。

ハードウェア資産情報を手動で編集する方法については、「[11.1.2 ハードウェア資産情報を編集する手順](#)」を参照してください。

利用者情報を収集して自動更新する

オンライン管理のコンピュータの場合で、ハードウェア資産情報が管理対象のコンピュータの機器情報と関連づいているときは、[利用者情報の入力]画面をコンピュータに表示させて、利用者が入力した情報を収集できます。オフライン管理のコンピュータの場合は、`getinv.vbs` コマンドを実行して機器情報を収集するときに、[利用者情報の入力]画面を対象のコンピュータに表示できます。なお、[利用者情報の入力]画面を表示するためには、対象のコンピュータにエージェントをインストールする必要があります。

収集できる情報を次に示します。

- 部署
- 設置場所
- 利用者名
- アカウント
- メールアドレス
- 電話番号
- 任意に追加した管理項目

利用者が入力した情報を収集することで、管理者が資産情報をメンテナンスする手間を省けます。例えば、定期的に利用者側で最新情報を入力してもらうように運用しておくと、大人数の部署異動があっても、管理者側で情報をメンテナンスすることなく異動後の利用者情報を把握できます。

なお、管理が不要になったハードウェア資産情報は削除することもできます。ハードウェア資産情報を削除する方法については、「[11.1.3 ハードウェア資産情報を削除する手順](#)」を参照してください。

関連リンク

- [11.1.4 資産画面で\[利用者情報の入力\]画面の表示間隔を設定する手順](#)
- [11.1.6 資産状態を変更する手順](#)

1.9.3 機器を購入する流れ

従業員の増加や設備の追加などに伴い組織内に新しい機器を導入したら、機器を登録して資産管理を始めます。

新規にコンピュータを購入して JP1/IT Desktop Management 2 で資産管理を始めるまでの流れを次に示します。

1. 新規機器を購入する

購入するコンピュータのスペックや価格などを調査し、購入数を検討します。また、コンピュータの利用者情報（部署、設置場所、利用者名など）を入手します。

2. 機器の資産情報を登録する

コンピュータを購入したら、利用者にコンピュータを配布する前にエージェントをインストールして、JP1/IT Desktop Management 2 の管理対象にします。

エージェントをインストールしたコンピュータをネットワークに接続すると、機器情報が自動で登録されます。

機器情報と同時にハードウェア資産情報も登録されるので、事前に入手しておいたコンピュータの利用者情報を手動で登録します。

3. 機器を配布する

JP1/IT Desktop Management 2 でコンピュータの配布先の情報を出力します。出力した情報を基に、コンピュータを配布します。

コンピュータを配布したら、JP1/IT Desktop Management 2 で資産管理を始めます。

(1) 新規機器を購入する

従業員の増加や設備の追加などに伴って、組織内に新しいコンピュータを導入する場合、事前に購入計画を立てます。また、コンピュータの利用者を把握するため利用者情報を入手します。

購入計画を立てる

コンピュータを購入する前に購入計画を立てます。例えば、次のような項目を検討します。

- 契約種別（購入、レンタル、リースなど）
- 用途（一般 OA 用、開発用、特殊用途用など）
- スペック
- 価格
- 台数

ポイント

資産画面の【サマリ】－【ダッシュボード】画面に表示される【観点ごとのハードウェア資産台数】パネルで、【半年以内に登録した資産】のリンクをクリックすると、最近購入したコンピュータのスペックを確認できます。コンピュータを購入する際の参考にしてください。

利用者情報を入手する

コンピュータの登録時に必要な利用者情報を、事前に入手しておきます。次の情報を入手してください。

- 部署
- 設置場所
- 利用者名
- メールアドレス
- 電話番号

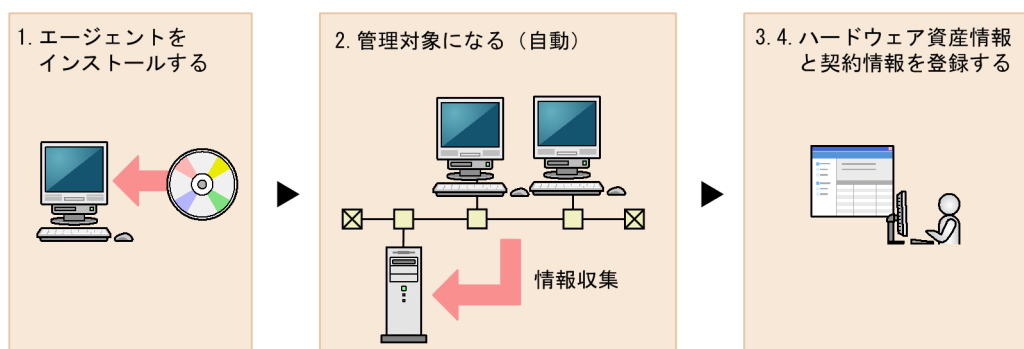
入手した利用者情報は、コンピュータを購入したあとで JP1/IT Desktop Management 2 に登録します。

購入するコンピュータが決まったら業者に発注します。

(2) 機器の資産情報を登録する流れ

新しいコンピュータを購入したら、利用者にコンピュータを配布する前に、エージェントをインストールして JP1/IT Desktop Management 2 の管理対象にします。コンピュータを管理対象にしたら、ハードウェア資産情報と契約情報を登録します。

作業の流れを次の図に示します。なお、ここで説明する作業は、システム管理用のネットワークを利用して実施してください。



1. エージェントをインストールする

JP1/IT Desktop Management 2 の管理対象にするため、コンピュータにエージェントをインストールします。

ポイント

あらかじめ環境を作成したモデルマシンにエージェントをインストールして、ほかのコンピュータにディスクコピーすると、コンピュータごとに環境を構築する手間を省けます。

2. JP1/IT Desktop Management 2 の管理対象にする

エージェントをインストールしたコンピュータをネットワークに接続すると、自動的に管理対象になり、コンピュータから収集された情報が機器画面の [機器情報] 画面に表示されます。さらに、コンピュータの情報は資産画面の [ハードウェア資産] 画面にも、新規のハードウェア資産情報として自動的に登録されます。

3.ハードウェア資産情報を登録する

自動的に登録されたハードウェア資産情報は、[資産状態] が「未確認」となっています。また、コンピュータから収集できた情報だけが登録されています。このため、コンピュータから自動的に収集されない [資産管理番号]、[資産状態]（運用中、在庫など）、利用者情報などを手動で登録します。

ポイント

利用者情報は、利用者情報の入力画面から利用者に入力してもらうこともできます。

4.契約情報を登録する

契約を結んでいるハードウェア資産の場合は、資産画面の [契約] 画面で契約情報を登録します。

契約情報を登録するときに、契約対象のハードウェア資産を設定すると、ハードウェア資産の費用や契約期限を管理できるようになります。

ポイント

バーコードリーダーを利用している場合は、バーコードリーダー用の資産管理番号シールを作成してコンピュータに貼ります。コンピュータを棚卸するときにバーコードリーダーでシールを読み込むと、効率良く現品確認できるようになります。

ポイント

事前にハードウェア資産情報だけ手動で登録しておき、あとからコンピュータをネットワークに接続して機器情報を登録することもできます。例えば、シリアルナンバーを含むハードウェア資産情報の一覧をインポートして、事前にハードウェア資産情報だけ登録しておきます。配布後にコンピュータをネットワークに接続すると、収集された機器情報のうち同じシリアルナンバーの機器情報が対応づけられて、ハードウェア資産情報に登録されます。

これで、必要な情報の登録が完了します。情報の登録が完了したら、利用者コンピュータを配布します。在庫として保管するコンピュータがある場合は、保管場所にコンピュータを移動します。

関連リンク

- [1.1 エージェントの導入](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [6.14 利用者情報を取得する手順](#)
- [11.3.1 契約情報を追加する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)

(3) 機器を利用者に配布する流れ

購入したコンピュータの情報を JP1/IT Desktop Management 2 に登録したら、利用者にコンピュータを配布します。配布する前にコンピュータの一覧を作成し、一覧を基にコンピュータを配布します。

1. 配布するコンピュータの一覧を作成する

コンピュータを配布するため、配布するコンピュータの一覧を作成します。配布するコンピュータのハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、配布時に必要な情報をエクスポートします。例えば、配布するコンピュータを識別するために [資産管理番号] を、設置場所を確認するために [部署]、[設置場所] を、利用者と連絡を取るために [利用者名]、[メールアドレス]、[電話番号] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く配布するために、[部署] や [設置場所]などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. コンピュータを配布する

エクスポートした一覧の情報を基に、コンピュータを配布します。配送業者にコンピュータの配布を依頼する場合は、一覧を渡して作業してもらいます。利用者に受理したことを示すサインを一覧に記入してもらえると、配布が完了したことを確認できます。

コンピュータを配布したら、JP1/IT Desktop Management 2 で資産管理を始めます。発生する業務に応じて情報をメンテナンスし、常に最新の状態でハードウェア資産情報を管理してください。

ポイント

ハードウェア資産情報が機器情報と関連づいている場合、ハードウェア資産情報のうちの [機器情報] は、収集された機器情報で自動的に更新されます。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)

1.9.4 機器をリプレースする流れ

従業員の異動や機器の入れ替えなどに伴って組織内の機器をリプレースする場合、JP1/IT Desktop Management 2 でリプレース対象の機器を調査して、機器を配布・回収します。

機器をリプレースする流れを次に示します。

1. リプレースの計画を立てる

JP1/IT Desktop Management 2 でリプレースが必要な機器を調査して、回収する機器を決定します。回収する機器を決定したら、代わりに配布する機器を準備します。

2. 新しい機器を配布する

JP1/IT Desktop Management 2 で配布する機器の設置場所の情報を出力します。出力した情報を基に、機器を配布します。

機器を配布したら、利用者に古い機器のデータを新しい機器に移行するよう指示します。

3. 機器を回収する

古い機器のデータを新しい機器に移行したら、古い機器を回収します。

JP1/IT Desktop Management 2 で回収する機器の設置場所の情報を出力します。出力した情報を基に、機器を回収します。

機器のリプレースが完了します。

(1) スマートデバイスのリプレースの計画を立てる流れ

従業員の異動や機器の入れ替えなどに伴って組織内の機器をリプレースする場合、リプレースが必要な機器を調査して、リプレースする機器を決定します。リプレースする機器が決定したら、代わりに配布する機器を準備します。また、事前に利用者にリプレースについて通知します。

1. リプレースする機器を決定する

資産画面の [ハードウェア資産] 画面で、リプレースが必要な機器がないか調査します。例えば、3 年以上使用した機器をリプレースする方針の場合は、フィルタを利用して [登録日時] が 3 年以上前の機器がないか確認します。

ポイント

よく業務で使用するフィルタ条件を保存しておくことで、毎回条件を指定する手間が省けます。保存したフィルタ条件は、メニューエリアで選択することで一覧に適用できます。

リプレースが必要な機器が見つかった場合は、回収予定の機器として把握できるように、資産画面の [ハードウェア資産] 画面で [予定資産状態] に「在庫」、[変更予定日] に回収日を設定します。

2. 配布する機器を準備する

回収する機器の代わりに新しく配布する機器を準備します。

• 在庫の機器を利用する場合

資産画面の [ハードウェア資産] 画面で、[資産状態] が「在庫」の機器を確認します。フィルタを利用すると、表示する情報を絞り込めます。スペックなどを確認して問題がなければ、配布予定の機器として把握できるように、[予定資産状態] に「運用中」を、[変更予定日] に配布日を設定します。

• 新しく機器を購入する場合

新しく機器を購入したら、JP1/IT Desktop Management 2 の管理対象にして、ハードウェア資産情報と契約情報を登録します。そのあと、配布予定の機器として把握できるように、[予定資産状態] に「運用中」を、[変更予定日] に配布日を設定します。

3.利用者にリプレースを通知する

スムーズにリプレースできるように、リプレースする機器の利用者に、リプレースする理由とリプレース予定日を連絡します。

リプレースの準備が完了します。

関連リンク

- [11.1.7 予定資産状態を変更する手順](#)
- [1.9.3 機器を購入する流れ](#)

(2) 新しい機器を配布する流れ

リプレースの準備ができたなら、配布する機器の一覧を作成して、一覧を基に機器を配布します。機器を配布したらハードウェア資産情報を最新の状態にメンテナンスします。

1.配布する機器の一覧を作成する

機器を配布するため、配布する機器の一覧を作成します。[予定資産状態] が「運用中」のハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、配布時に必要な情報をエクスポートします。例えば、配布する機器を識別するために [資産管理番号] を、設置場所を確認するために [部署]、[設置場所] を、利用者と連絡を取るために [利用者名]、[メールアドレス]、[電話番号] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く配布するために、[部署] や [設置場所]などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2.機器を配布する

エクスポートした一覧の情報を基に、機器を配布します。配送業者に機器の配布を依頼する場合は、一覧を渡して作業してもらいます。利用者に受理したことを示すサインを一覧に記入してもらうと、配布が完了したことを確認できます。

3.ハードウェア資産情報をメンテナンスする

配布が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の [ハードウェア資産] 画面で、配布した機器の [資産状態] を「在庫」から「運用中」に変更します。また、[部署]、[設置場所]、利用者情報を最新の情報に変更します。

機器の配布が完了します。利用者に、古い機器のデータを新しい機器に移行するよう指示します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [11.1.6 資産状態を変更する手順](#)

(3) 利用しなくなった機器を回収する流れ

利用しなくなった機器を在庫に戻す場合、回収予定日になったら機器を回収します。回収前に機器の一覧を作成し、一覧を基に機器を回収してください。機器を回収したらハードウェア資産情報を最新の状態にメンテナンスします。また、移管して問題ないソフトウェアライセンスであれば、回収した機器に割り当てられていたソフトウェアライセンスを、別の機器に移管します。

ポイント

ダイジェストレポートの [ハードウェア資産の予定] で、回収予定 ([予定資産状態] が「在庫」) の機器の台数を確認することもできます。また、ダイジェストレポートをメールで送付することもできます。

ポイント

スムーズに回収するため、回収する機器の利用者に、機器を回収する理由や回収予定日を事前に通知しておくことをお勧めします。

1. 回収する機器の一覧を作成する

機器を回収するため、回収する機器の一覧を作成します。[予定資産状態] が「在庫」のハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、回収時に必要な情報をエクスポートします。例えば、回収する機器を識別するために [資産管理番号] を、設置場所を確認するために [部署]、[設置場所] を、利用者と連絡を取るために [利用者名]、[メールアドレス]、[電話番号] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く回収するために、[部署] や [設置場所]などを基準に並べ替えておく と 便利 です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. 機器を回収する

エクスポートした一覧を基に機器を回収します。配送業者に機器の回収を依頼する場合は、一覧を渡して作業してもらいます。

機器を回収したら、エクスポートした一覧の情報と照らし合わせて、回収結果が正しいか確認します。

3.ハードウェア資産情報をメンテナンスする

回収が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の[ハードウェア資産]画面で、回収した機器の[資産状態]を「運用中」から「在庫」に変更します。また、[設置場所]に機器の保管場所を指定して、[部署]や利用者情報をシステム管理者の情報に変更します。

4.ソフトウェアライセンスを別の機器に移管する

回収した機器に割り当てられていたソフトウェアライセンスを有効利用するため、別の機器にソフトウェアライセンスを移管します。

ポイント

ソフトウェアライセンスを移管しない場合は、ソフトウェアライセンスの割り当てを解除します。

回収した機器は在庫として管理します。

関連リンク

- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)
- [11.2.13 ソフトウェアライセンスを移管する手順](#)
- [11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順](#)

1.9.5 機器を棚卸する流れ

組織で利用している資産を管理するためには、定期的に棚卸を実施して、現状を正しく把握しておく必要があります。JP1/IT Desktop Management 2 に現品確認の結果を登録することで、現品確認できなかった機器の情報を簡単に抽出できるようになります。

機器を棚卸する流れを次に示します。

1.現品確認を実施する

ハードウェア資産情報の一覧を作成し、組織内のすべての機器の現品を確認します。

2.現品確認の結果を反映する

JP1/IT Desktop Management 2 で機器の棚卸状況を管理するために、現品確認の結果を反映します。

3.現品確認できなかった機器を調査する

現品確認できなかった機器の利用状況を調査します。確認できた機器は JP1/IT Desktop Management 2 に現品確認の結果を反映します。

機器の現品確認の結果が JP1/IT Desktop Management 2 に反映されます。

ポイント

機器の棚卸にバーコードリーダーを使用している場合は、機器の現品確認および結果の反映をより簡単に行えます。

関連リンク

- [11.1.11 バーコードリーダーを使用して棚卸する](#)

(1) 現品確認を実施する流れ

機器を現品確認するには、ハードウェア資産情報の一覧を出力して、現品と突き合わせて確認します。

1. ハードウェア資産情報の一覧をエクスポートする

現品を確認するために、ハードウェア資産情報の一覧を作成します。資産画面の [ハードウェア資産] 画面でハードウェア資産情報を CSV ファイルにエクスポートしてください。機器を識別するために、[資産管理番号]、[棚卸日]、[部署]、[設置場所]、[利用者名] などの項目をエクスポートしてください。なお、ここでエクスポートした CSV ファイルは、現品確認の結果を反映するときにも使用します。[資産管理番号] および [棚卸日] の項目は、必ずエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、確認しやすくするために、「部署」や「設置場所」などを基準に並べ替えておくと便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. ハードウェア資産情報の一覧を基に現品確認する

エクスポートした一覧を基に、現品確認します。現品確認できた場合は、一覧の該当機器に、現品確認できたことを示す印を付けます。ここで印を付けた機器の棚卸日を、JP1/IT Desktop Management 2 で更新します。

現品確認が完了し、確認結果が記入された機器の一覧が完成します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)

(2) 現品確認の結果を反映する流れ

JP1/IT Desktop Management 2 で機器の棚卸状況を管理するために、現品確認の結果を反映します。現品確認の結果を反映すると、資産画面の [ハードウェア資産] 画面でハードウェア資産情報の [棚卸日] が更新されます。

1. 棚卸日を更新した CSV ファイルを作成する

棚卸日を一括更新するために、棚卸日を更新したハードウェア資産情報の CSV ファイルを作成します。機器を現品確認したときに使用した CSV ファイルを編集して、現品確認できた機器の [棚卸日] を更新してください。

ポイント

現品確認をしたときに、[部署]、[設置場所]、[利用者名] などのハードウェア資産情報が変更されていた場合は、CSV ファイルを編集して、[棚卸日] と同時に更新してください。

2. 棚卸日を更新する

CSV ファイルを作成したら、ハードウェア資産情報の CSV ファイルをインポートして、一括で棚卸日を更新します。

現品確認できた機器は、ハードウェア資産情報の [棚卸日] が更新されます。

ポイント

手もとにあるハードウェア資産を個別に確認したい場合は、手動で 1 件ずつ棚卸日を更新してください。

ポイント

機器の「最終接続確認日時」、または利用者による [利用者情報の入力] 画面の入力が完了した日を [棚卸日] として自動更新できます。

関連リンク

- [11.1.8 手動で棚卸日を更新する手順](#)
- [11.1.10 棚卸日の自動更新を設定する手順](#)

(3) 現品確認できなかった機器を調査する流れ

現品確認できなかった機器は、利用状況を調査して、再度現品確認する必要があります。

1. 現品確認できなかった機器を確認する

資産画面の [ハードウェア資産] 画面で、[棚卸日] が更新されていないハードウェア資産情報を確認します。フィルタを利用して、[棚卸日] が最新の棚卸日より古いハードウェア資産情報を表示します。

2. ハードウェア資産情報の一覧をエクスポートする

現品を調査するために、ハードウェア資産情報の一覧を作成します。棚卸日が更新されていないハードウェア資産情報を CSV ファイルにエクスポートしてください。機器を識別するために、[資産管理番号]、[部署]、[設置場所]、[利用者名] などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、確認しやすくするために、「部署」や「設置場所」などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

3. 該当機器の利用者に状況を確認する

ハードウェア資産情報の一覧を作成したら、現品がどこにあるか機器の利用者に確認します。

機器が見つかった場合

機器の現品確認ができたことを一覧に記載します。ハードウェア資産情報に修正があれば、同時に記載します。

機器が見つからなかった場合

機器が紛失したおそれがあります。利用者に状況を確認してください。紛失していた場合は、該当資産の「資産状態」を「滅却」にします。また、紛失理由や紛失日時などを「ノート」タブにメモしておきます。

4. 現品確認の結果を反映する

現品確認できた機器について、現品確認の結果を反映します。

機器の棚卸が完了します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [\(2\) 現品確認の結果を反映する流れ](#)
- [1.9.7 機器を滅却する流れ](#)

1.9.6 利用されていない機器を確認する流れ

効率的に資産を運用するために、機器の利用状況を確認して、利用されていない機器を回収します。

利用されていない機器を回収する流れを次に示します。

1. 機器の利用状況を調査する

利用されていない機器を発見するために、JP1/IT Desktop Management 2 で管理している機器を更新日で絞り込み、一定期間情報が更新されていない機器を確認します。情報が更新されていない機器の利用者に、機器の必要性や利用状況を確認します。

2. 機器を回収する

利用状況を調査した機器について、必要性が低いものを回収します。

回収予定を計画し、機器の利用者に機器の回収について通知します。回収予定日になったら、機器を回収します。

回収した機器が在庫になります。必要に応じて回収した機器を配布し、効率的に資産を運用してください。

(1) 機器の利用状況を調査する流れ

利用されていない機器を発見するために、機器情報の更新日時を確認します。長期間更新されていない機器は、利用者に機器の利用状況を確認して、機器を回収するかどうかを判断します。

1. 利用されていない機器を確認する

機器画面の[機器情報]画面で、[更新日時]を条件に機器情報を絞り込みます。例えば、機器情報の[更新日時]が31日以上前の機器を表示するフィルタを作成して、長期間利用されていない機器を把握します。

機器の利用者に、機器が利用されていないことを通知し、機器の必要性や利用状況を確認します。

ポイント

機器画面の[サマリ] - [ダッシュボード]画面に表示される[観点ごとの機器台数]パネルでは、作成したフィルタおよびカスタムグループごとに管理対象の機器の台数を確認できます。素早く機器情報を把握したい場合は、このパネルを利用することをお勧めします。

2. 機器を回収するかどうかを判断する

利用状況を確認した結果、機器の必要性が低いとわかった場合は、機器の回収を計画します。また、エラーによって機器情報が更新されていない場合は、エラーの原因を調査して対処します。

3. 機器の回収予定日を設定する

資産画面で、利用されていないと判断した機器の回収予定日を設定します。[予定資産状態]を「在庫」にして、[変更予定日]に機器を回収する予定日を入力します。

ポイント

機器の回収予定日を設定するときは、資産の一覧を設置場所または部署で並べ替えることをお勧めします。同じ場所にある機器の回収予定日を同日に設定することで、効率的に回収を行います。

利用されていない機器が確認でき、回収対象の機器を特定できます。

ポイント

機器情報の更新間隔は、機器に適用したエージェント設定によって変更できます。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]画面で作成できます。

関連リンク

- 11.1.7 予定資産状態を変更する手順

(2) 利用しなくなった機器を回収する流れ

利用しなくなった機器を在庫に戻す場合、回収予定日になったら機器を回収します。回収前に機器の一覧を作成し、一覧を基に機器を回収してください。機器を回収したらハードウェア資産情報を最新の状態にメンテナンスします。また、移管して問題ないソフトウェアライセンスであれば、回収した機器に割り当てられていたソフトウェアライセンスを、別の機器に移管します。

ポイント

ダイジェストレポートの「ハードウェア資産の予定」で、回収予定（「予定資産状態」が「在庫」）の機器の台数を確認することもできます。また、ダイジェストレポートをメールで送付することもできます。

ポイント

スムーズに回収するため、回収する機器の利用者に、機器を回収する理由や回収予定日を事前に通知しておくことをお勧めします。

1. 回収する機器の一覧を作成する

機器を回収するため、回収する機器の一覧を作成します。「予定資産状態」が「在庫」のハードウェア資産情報を CSV ファイルにエクスポートしてください。ハードウェア資産情報のうち、回収時に必要な情報をエクスポートします。例えば、回収する機器を識別するために「資産管理番号」を、設置場所を確認するために「部署」、「設置場所」を、利用者と連絡を取るために「利用者名」、「メールアドレス」、「電話番号」などの項目をエクスポートしてください。

ポイント

ハードウェア資産情報をエクスポートするときは、効率良く回収するために、「部署」や「設置場所」などを基準に並べ替えておくとう便利です。ハードウェア資産情報は、操作画面上の項目名をクリックすると並べ替えができます。

2. 機器を回収する

エクスポートした一覧を基に機器を回収します。配送業者に機器の回収を依頼する場合は、一覧を渡して作業してもらいます。

機器を回収したら、エクスポートした一覧の情報と照らし合わせて、回収結果が正しいか確認します。

3. ハードウェア資産情報をメンテナンスする

回収が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の「ハードウェア資産」画面で、回収した機器の「資産状態」を「運用中」から「在庫」に変更します。また、「設置場所」に機器の保管場所を指定して、「部署」や利用者情報をシステム管理者の情報に変更します。

4.ソフトウェアライセンスを別の機器に移管する

回収した機器に割り当てられていたソフトウェアライセンスを有効利用するため、別の機器にソフトウェアライセンスを移管します。

ポイント

ソフトウェアライセンスを移管しない場合は、ソフトウェアライセンスの割り当てを解除します。

回収した機器は在庫として管理します。

関連リンク

- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [11.5 資産情報をエクスポートする手順](#)
- [1.9.2 ハードウェア資産情報をメンテナンスする方法](#)
- [11.1.6 資産状態を変更する手順](#)
- [11.2.13 ソフトウェアライセンスを移管する手順](#)
- [11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順](#)

1.9.7 機器を滅却する流れ

リプレースや修理などに伴って機器を回収した場合に、古くなったり壊れたりして今後使用しない機器があるときは、機器を滅却します。

機器を滅却する流れを次に示します。

1.滅却対象の機器を決定する

回収した機器のうち、今後使用しない機器があるときは滅却対象にします。滅却対象の機器は、情報漏えいを防ぐためディスクの内容を完全に消去します。

2.機器を廃棄する

滅却予定日になったら機器を廃棄します。

不要になった機器が廃棄され、滅却が完了します。

関連リンク

- [1.9.4 機器をリプレースする流れ](#)

(1) 滅却対象の機器を決定する流れ

リプレースや修理などに伴って機器を回収した場合に、古くなったり壊れたりして今後使用しない機器があるときは、滅却対象にします。今後も使用することがある機器は在庫として保管します。

1. 今後使用しない機器がないか確認する

回収した機器の中に、今後使用しない機器がないかを確認します。

例えば、利用年数が5年以上経過している機器を減却する方針の場合は、資産画面の[ハードウェア資産]画面で、回収した機器の[登録日時]または[契約日]から、機器の利用年数を確認します。フィルタを利用すると、表示する情報を絞り込めます。

表示項目に[登録日時]または[契約日]が表示されていない場合は、一覧の項目名を右クリックして[表示項目の選択]を選択してください。表示されるダイアログで[登録日時]または[契約日]をチェックして[OK] ボタンをクリックすると、表示項目に[登録日時]または[契約日]が表示されます。なお、ハードウェア資産の契約情報が登録されていない場合は、[契約日]には「-」が表示されます。

2. 減却対象にする

今後使用しない機器がある場合は、減却予定の機器として把握できるように、[予定資産状態]を「減却」にして、[変更予定日]に減却予定日を設定します。

3. ハードディスクに格納されているデータを完全に消去する

減却対象の機器は、情報漏えいを防ぐため、専用のツールを使用してハードディスクに格納されているデータを完全に消去します。

スマートデバイスを減却する場合は、[ハードウェア資産]画面で[機器一覧へ] ボタンをクリックして機器画面に移動したあと、[操作メニュー]の[初期化する(スマートデバイス)]を選択してスマートデバイスを初期化します。

在庫として残す機器は、必要なときにすぐに利用できるようにディスクコピーします。

減却対象の機器は、いつでも廃棄できる状態になります。

関連リンク

- [11.1.7 予定資産状態を変更する手順](#)
- [1.11 資産に関する契約を管理する流れ](#)

(2) 機器を廃棄する流れ

今後使用しない機器は、減却予定日になったら廃棄します。廃棄前に機器の一覧を作成して、一覧を基に機器を廃棄します。機器を廃棄したらハードウェア資産情報を最新の状態にメンテナンスします。

1. 廃棄する機器の一覧を作成する

機器を廃棄するため、廃棄する機器の一覧を作成します。[予定資産状態]が「減却」のハードウェア資産情報をCSVファイルにエクスポートしてください。ハードウェア資産情報のうち、廃棄時に必要な情報をエクスポートします。例えば、廃棄する機器を識別するために[資産管理番号]などの項目をエクスポートしてください。

2. 機器を廃棄する

エクスポートした一覧を基に機器を廃棄します。廃棄業者に廃棄を依頼する場合は、一覧を渡して作業してもらいます。

3.ハードウェア資産情報をメンテナンスする

廃棄が完了したら、ハードウェア資産情報を最新の状態にメンテナンスします。資産画面の「ハードウェア資産」画面で、廃棄した機器の「資産状態」を「在庫」から「滅却」に変更します。

ポイント

ハードウェア資産の「資産状態」を「滅却」にすると、対応する機器情報は削除されます。

ポイント

ネットワークモニタを有効にしている場合、ハードウェア資産の「資産状態」を「滅却」にすると、対応する機器の情報がネットワーク制御リストから削除されます。ただし、対応する機器にエージェントが導入されていて、ネットワークに接続している場合、自動的に、機器が再び管理対象になってネットワーク制御リストに再登録されます。

機器の廃棄が完了します。なお、廃棄した機器のハードウェア資産情報は、「資産状態」が「滅却」の機器として残ります。

また、滅却した機器に関する契約は、必要に応じて解約します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [11.1.6 資産状態を変更する手順](#)

1.9.8 機器の障害に対応する流れ

組織内で利用している機器に障害が発生した場合、システム管理者は現場からの問い合わせを基に障害内容を把握し、必要に応じて保守サービス契約を結んでいる契約会社に修理を依頼します。機器を修理に出したら、利用者に代替機を貸し出します。また、障害対応の内容を記録しておきます。

JP1/IT Desktop Management 2 で管理している情報を利用して、機器の障害に対応する流れを次に示します。

1.障害内容を確認する

利用者からの問い合わせを基に、機器を確認して障害内容を把握します。

2.保守サービスを利用する

障害が発生した機器に対して、保守サービスを利用するために契約会社へ連絡を取ります。

3.代替機を利用者に貸し出す

障害が発生した機器を修理に出した場合、在庫の機器を代替機として利用者に一時的に貸し出します。

4.修理後の機器を利用者に返却する

機器の修理が完了したら、利用者に機器を返却して、貸し出していた代替機を回収します。

5.障害履歴を記録する

障害の内容や発生日時、対処の内容などを JP1/IT Desktop Management 2 に記録します。

機器の修理が完了し、障害履歴が JP1/IT Desktop Management 2 に記録されます。

(1) 障害内容を確認する

組織内で利用している機器に障害が発生した場合、管理者は障害内容を把握する必要があります。

電話やメールでの問い合わせだけでは障害内容が不明確な場合は、障害発生現場へ詳細を確認しに行きます。このため、利用者から電話やメールで問い合わせを受けたときには、機器の利用者名や部署、電話番号など、障害が発生した機器を特定できる情報を確認しておきます。

ポイント

リモートコントロール機能を利用すると、障害が発生した機器を直接操作して、障害内容を確認できます。離れた場所にある機器で障害が発生しても、現場に行かないで早急に対応できます。

障害が発生した機器を確認する

資産画面の [ハードウェア資産] 画面で、該当するハードウェア資産情報を表示します。このとき、問い合わせ時に確認した情報（利用者名や部署、電話番号など）を基にフィルタを利用すると素早く確認できます。

関連リンク

- [1.5 機器のリモートコントロール](#)
- [\(5\) 障害履歴を記録する](#)

(2) 保守サービスを利用する流れ

機器に障害が発生した場合、保守サービスを利用するために契約会社へ連絡を取ります。

契約会社の連絡先を確認するためには、障害が発生した機器の契約情報を確認します。

1. 資産画面の [ハードウェア資産] 画面で、障害が発生した機器を選択する

このとき、問い合わせ時に確認した情報（利用者名や部署、電話番号など）を基にフィルタを利用すると機器を素早く表示できます。

2. [契約情報] タブで、該当する契約情報の [契約会社名] のリンクをクリックする

表示されるダイアログで契約会社の連絡先や担当者を確認できます。

なお、契約会社の情報を表示するためには、あらかじめ次の情報を登録しておく必要があります。

契約会社情報

設定画面の「資産管理」－「契約会社リストの設定」画面で契約会社の電話番号や担当者を登録できます。

保守サービスの契約情報

「契約」画面から契約情報を登録できます。契約情報を登録するときに、該当する契約会社情報を指定してください。また、契約対象のハードウェア資産も指定してください。

関連リンク

- [15.4.8 契約会社情報の管理](#)
- [\(5\) 障害履歴を記録する](#)

(3) 代替機を利用者に貸し出す

障害が発生した機器を修理に出した場合、利用者には在庫の機器を代替機として一時的に貸し出します。このとき、障害が発生した機器と貸し出した機器の資産管理番号を確認しておいてください。

障害が発生した機器は、修理中で利用されていないことがわかるように、ハードウェア資産情報の「資産状態」を「在庫」に変更します。また、貸し出した機器は、利用中であることがわかるように、ハードウェア資産情報の「資産状態」を「運用中」に変更します。資産画面の「ハードウェア資産」画面で、該当するハードウェア資産情報を表示します。このとき、資産管理番号を基にフィルタを利用します。

また、一時的な貸し出しのため、後日回収する予定をハードウェア資産情報に登録します。1週間後に修理が完了して、貸し出した機器を回収して在庫に戻す場合は、「予定資産状態」に「在庫」を、「変更予定日」に1週間後の日付を設定します。

ポイント

「予定資産状態」を設定すると、ダイジェストレポートの「ハードウェア資産の予定」で、回収予定の機器を確認できるようになります。また、ダイジェストレポートをメールで送付することもできます。

関連リンク

- [11.1.6 資産状態を変更する手順](#)
- [11.1.7 予定資産状態を変更する手順](#)
- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)

(4) 修理後の機器を利用者に返却する流れ

障害が発生した機器の修理が完了したら、利用者に機器を返却して、貸し出していた代替機を回収します。機器を回収したらハードウェア資産情報を最新の状態にメンテナンスします。

1.修理が完了した機器を返却する

修理が完了した機器を利用者に返却します。

2.代替機を回収する

機器を返却した際に、一時的に貸し出していた機器を回収します。

3.ハードウェア資産情報をメンテナンスする

返却した機器は、利用中になるため〔資産状態〕を「在庫」から「運用中」に変更します。また、回収した機器は在庫に戻るため、ハードウェア資産情報の〔資産状態〕を「運用中」から「在庫」に変更します。

資産画面の〔ハードウェア資産〕画面で、該当するハードウェア資産情報を表示するときは、資産管理番号を基にフィルタを利用します。

MAC アドレスが変更になった場合

ネットワークモニタ機能で新規機器の接続を拒否している場合、ネットワークカードの交換などによって MAC アドレスが変更されると、異なる機器として識別されてネットワーク接続できなくなることがあります。

エージェント導入済みのコンピュータ、または Windows の管理共有で認証済みのエージェントレスのコンピュータの場合は、そのままネットワーク接続できます。MAC アドレスが変更になっても同一の機器として認識され、ネットワーク制御リストに登録された MAC アドレスが自動的に更新されます。

SNMP で認証済み、または ICMP で生存確認をしているエージェントレスの機器の場合、MAC アドレスが変更になると異なる機器として認識され、ネットワーク接続が拒否されます。ネットワーク接続を許可するためには、ネットワーク制御リストに登録されている MAC アドレスを手動で変更する必要があります。

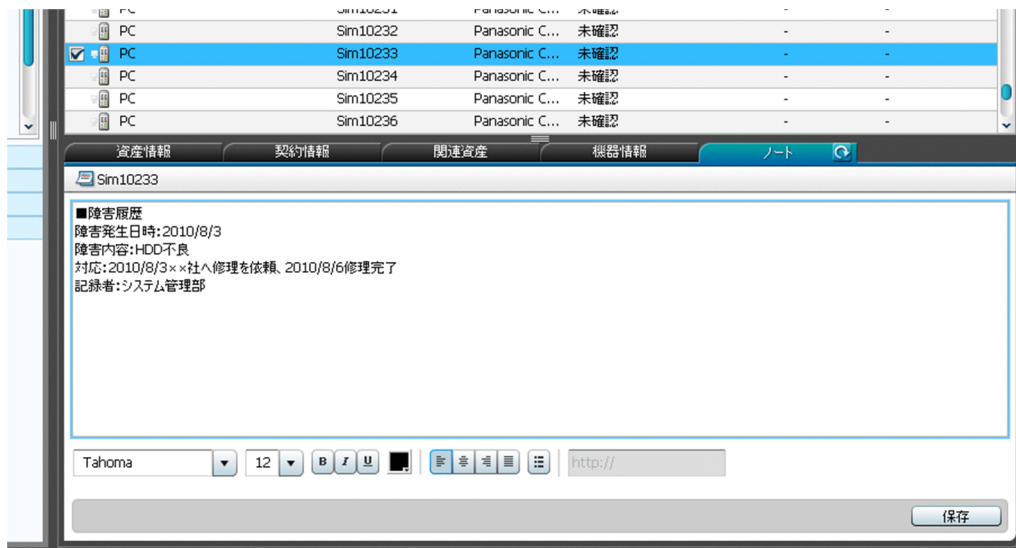
なお、更新された MAC アドレスの情報は、機器画面の〔機器情報〕画面および設定画面の〔ネットワーク制御〕－〔ネットワーク制御リストの設定〕画面で確認できます。

関連リンク

- [\(3\) 利用しなくなった機器を回収する流れ](#)
- [11.1.6 資産状態を変更する手順](#)
- [8. 機器のネットワーク接続を管理する](#)

(5) 障害履歴を記録する

障害の内容や、障害発生日時、対応者などの障害履歴は、資産画面の〔ノート〕タブにメモとして保存しておけます。



障害が発生したときや修理から戻ってきたタイミングなどで、該当するハードウェア資産情報の [ノート] タブに障害履歴を記録しておくことをお勧めします。

[ノート] タブにメモを残すには、記録したい内容を入力し [保存] ボタンをクリックしてください。

1.9.9 機器情報の不審な変更を調査する流れ

組織内では、利用者が勝手にコンピュータにメモリを抜き差ししたり、ソフトウェアをインストール、アンインストールしたりするなど、コンピュータの構成を変更する場合があります。このような機器情報の変更の問題がないかを判断するために、JP1/IT Desktop Management 2 で取得した機器情報の変更履歴を確認して、機器情報の不審な変更を調査する流れを次に示します。

1. JP1/IT Desktop Management 2 の操作画面で機器情報の変更履歴を確認する

機器画面の [変更履歴] 画面で、定期的に機器情報の変更内容を確認します。

2. 変更履歴の中に不審な変更がないかを判断する

例えば、次のような確認をして不審な変更かどうかを判断します。

- ハードウェアの部品が変更されている場合：その変更が記載された帳票を確認する。
- インストールソフトウェアの追加や削除があった場合：JP1/IT Desktop Management 2 の配布 (ITDM 互換) 画面でタスクを表示させて、そのソフトウェアのインストールやアンインストールが実施されたかを確認する。

3. 不審な変更がある場合は、機器の管理責任者に調査を依頼する

不審な変更がある場合は、機器の管理責任者とその上長に連絡します。管理責任者には、対象の機器の特定や実物の確認などの調査を依頼します。

4. 機器の管理責任者の調査結果を基に、対策を実施する

機器の管理責任者の調査結果を基に、変更内容に問題があると判断した場合は、問題に応じた対策を実施します。

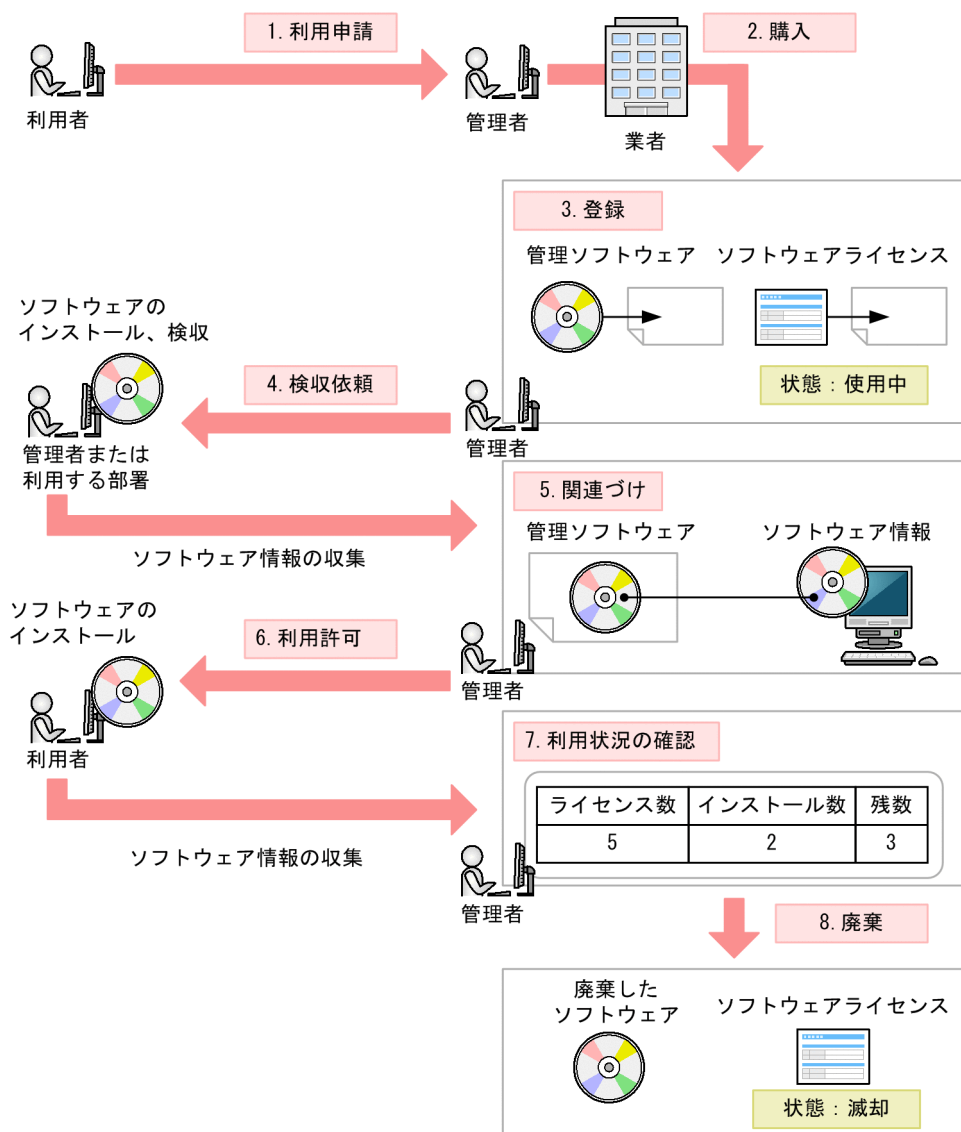
1.10 ソフトウェアライセンスを管理する

組織内のコンピュータには、業務で利用するさまざまなソフトウェアがインストールされています。ソフトウェアを使用する場合はソフトウェアライセンスを必要とすることが多く、ソフトウェアライセンスの超過利用を防いだり、効率良くソフトウェアライセンスを利用したりするためには、ソフトウェアライセンスを管理して利用状況を把握する必要があります。

JP1/IT Desktop Management 2 を利用すると、次に示すような機能を利用して効率良くソフトウェアライセンスを管理できます。

- 所有しているソフトウェアライセンスを台帳のように一覧で把握できる
- パネルやレポートなどのグラフィカルな画面から、ソフトウェアライセンスの利用状況を簡単に把握できる
- ソフトウェアライセンスをコンピュータに割り当てて、許可したとおりに利用されているかどうかを把握できる

ソフトウェアライセンスの管理は、資産画面の「管理ソフトウェア」画面および「ソフトウェアライセンス」画面で実行します。ソフトウェアライセンスを管理するためには、管理ソフトウェア情報とソフトウェアライセンス情報を JP1/IT Desktop Management 2 に登録し、ソフトウェアライセンスを管理する流れに沿ってソフトウェアライセンスの利用状況を把握します。ソフトウェアライセンスを管理する流れを次の図に示します。



利用者からソフトウェアの利用申請があったら、申請を確認してソフトウェアを購入します。購入後、管理するソフトウェア名（管理ソフトウェア）を決めてソフトウェアライセンス情報を JP1/IT Desktop Management 2 に登録します。このとき、管理ソフトウェア情報も登録します。（図中：1～3）

ソフトウェアは、利用者に提供する前に、利用する部署に依頼して検収します。検収時にソフトウェアを管理対象のコンピュータにインストールすると、管理用サーバにソフトウェア情報が収集されます。収集されたソフトウェア情報と管理ソフトウェア情報を関連づけます。これによって管理ソフトウェアのインストール状況が把握できるようになります。（図中：4～5）

その後、利用者からの申請を確認し、ソフトウェアの利用を許可します。利用者のコンピュータにソフトウェアがインストールされると、管理用サーバにソフトウェア情報が収集されてソフトウェアライセンスの利用状況を把握できるようになります。ソフトウェアが不要になった場合は、減却処理をして廃棄します。（図中：6～8）

ここでは、次に示す業務での JP1/IT Desktop Management 2 の利用方法を説明しています。

ソフトウェアを購入する

従業員の増加や新しいソフトウェアの導入などに伴ってソフトウェアを購入します。購入したソフトウェアの情報を JP1/IT Desktop Management 2 に登録して、ソフトウェアライセンスの利用状況を把握できるようにします。

余剰ライセンスを有効利用する

組織内の余剰ライセンスをチェックして、余っていたら必要としているコンピュータに割り当てて有効利用します。

許可なく利用されているライセンスを対処する

許可なく利用されているソフトウェアライセンスをチェックして対処します。

ソフトウェアライセンスを棚卸する

組織内のソフトウェアライセンスを棚卸します。

ソフトウェアライセンスを滅却する

使用しなくなったソフトウェアを職場から回収し、古いソフトウェアを滅却します。

関連リンク

- [1.10.1 ソフトウェアを購入する流れ](#)
- [1.10.2 余剰ライセンスを有効利用する流れ](#)
- [\(3\) 許可なく利用されているソフトウェアライセンスを対処する流れ](#)
- [1.10.3 ソフトウェアライセンスを棚卸する流れ](#)
- [1.10.4 ソフトウェアライセンスを滅却する流れ](#)

1.10.1 ソフトウェアを購入する流れ

従業員の増加や新しいソフトウェアの導入などに伴ってソフトウェアを購入したら、JP1/IT Desktop Management 2 に情報を登録して、ソフトウェアライセンスの管理を始めます。

新規にソフトウェアを購入して、ソフトウェアライセンスの管理を始めるまでの流れを次に示します。

1. ソフトウェアを購入する

利用者からソフトウェアの利用申請を提出してもらい、購入するかどうかを検討します。ソフトウェアの購入が決まったら、業者に発注します。

2. ソフトウェアの情報を登録する

ソフトウェアを入手したら、ソフトウェアライセンス情報と管理ソフトウェア情報を登録します。

3. ソフトウェアを検収する

エージェントをインストールしているテスト用のコンピュータに入手したソフトウェアをインストールして動作チェックを実施します。

ソフトウェアをインストールすると、ソフトウェア情報が収集されます。

4.インストール状況を管理できるように設定する

収集されたソフトウェア情報を、管理ソフトウェア情報のインストールソフトウェアとして設定します。インストールソフトウェアを設定すると、ソフトウェアのインストール状況が確認できるようになります。

5.ソフトウェアの媒体を貸し出す

ソフトウェアが問題なく動作することを確認したら、利用者にソフトウェアの媒体を貸し出して、インストールしてもらいます。

6.ソフトウェアライセンスの利用状況を確認する

JP1/IT Desktop Management 2 で、ソフトウェアライセンスの利用状況を確認します。

JP1/IT Desktop Management 2 で、ソフトウェアライセンスの管理を始めます。

関連リンク

- [1.10 ソフトウェアライセンスを管理する](#)
- [1.10.2 余剰ライセンスを有効利用する流れ](#)

(1) ソフトウェアを購入する流れ

新しくソフトウェアが必要になった場合は、利用者からソフトウェアの利用申請を提出してもらいます。提出してもらった情報から利用目的が妥当かどうか確認して、ソフトウェアを購入するかどうか検討してください。

1.利用申請を提出してもらう

利用申請時には、ソフトウェアの情報と利用者情報を提出してもらいます。次に示すような情報を入手してください。

- ソフトウェア名
- バージョン
- ライセンス数
- 利用目的
- 部署
- 利用者名
- メールアドレス
- 電話番号
- ソフトウェアを使用するコンピュータの資産管理番号

2.購入するかどうか検討する

利用申請の情報を基に、ソフトウェアを購入するかどうか検討します。例えば、次のような項目を検討します。

- ソフトウェアの利用目的は妥当か

- ソフトウェアライセンスは幾つ必要か
- 予算内で購入できるか

ポイント

以前購入したソフトウェアを追加購入する場合は、ソフトウェアライセンスの利用状況を確認します。もし、ソフトウェアライセンスが余っている場合は、余剰分を引いた本数だけソフトウェアを追加購入します。

ソフトウェアの購入が決まったら、業者に発注します。

関連リンク

- (6) [ソフトウェアライセンスの利用状況を確認する](#)

(2) ソフトウェアの情報を登録する流れ

ソフトウェアを購入したら、ソフトウェアライセンスの管理を始めるため、JP1/IT Desktop Management 2 に管理ソフトウェア情報とソフトウェアライセンス情報を登録します。管理ソフトウェア情報とソフトウェアライセンス情報を登録することで、ソフトウェアライセンスの利用状況を把握できるようになります。

契約を結んでいるソフトウェアの場合は、ソフトウェアライセンス情報に対応する契約情報を登録します。ソフトウェアライセンスに対応する契約を登録することで、どのソフトウェアライセンスに対してどの契約を結んでいるのかを把握できるようになります。

1. ソフトウェアライセンス情報を登録する

ソフトウェアを購入したら、資産画面の［ソフトウェアライセンス］画面で、ライセンス証書などを基にソフトウェアライセンス情報を登録します。

ポイント

コンピュータにソフトウェアライセンスを割り当てると、未許可でソフトウェアをインストールしているコンピュータや、利用許可しているのに利用されていないソフトウェアライセンスを把握できるようになります。

2. 管理ソフトウェア情報を登録する

ソフトウェアライセンス情報を登録するときに、あわせて管理ソフトウェア情報を登録します。

［ソフトウェアライセンスの追加］ダイアログで、［管理ソフトウェア名］を指定するときに〔(新規追加)〕を選択すると、管理ソフトウェア情報を登録できます。このとき、［管理ソフトウェア名］だけを設定します。管理ソフトウェア情報に対応するインストールソフトウェアは、あとから設定します。

3. 契約情報を登録する

契約を結んでいるソフトウェアの場合は、資産画面の［契約］画面で、ソフトウェアライセンスの契約情報（購入やサポート契約などの情報）を登録します。

これで、必要な情報の登録が完了します。情報の登録が完了したら、ソフトウェアが正しく使用できるか検収します。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.3.1 契約情報を追加する手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.4.4 契約情報をインポートする手順](#)

(3) ソフトウェアを検収する

ソフトウェアの情報を登録したら、ソフトウェアが正しく使用できるか確認するため、エージェントをインストールしているテスト用のコンピュータにソフトウェアをインストールします。

ソフトウェアをインストールしたら、動作に問題がないかをチェックします。

ポイント

ソフトウェアをインストールすると、ソフトウェア情報が収集されて、機器画面の［ソフトウェア情報］画面に表示されます。

(4) インストール状況を管理できるように設定する

管理ソフトウェア情報のインストールソフトウェアを設定すると、ソフトウェアのインストール状況を確認できるようになります。

資産画面の［管理ソフトウェア］画面で、対応する管理ソフトウェア情報を編集して、インストールソフトウェアの検収時に収集されたソフトウェア情報を設定してください。

関連リンク

- [11.2.2 管理ソフトウェア情報を編集する手順](#)

(5) ソフトウェアの媒体を利用者に貸し出す

ソフトウェアの登録が終わり、ソフトウェアが問題なく動作することを確認したら、利用者にソフトウェアの媒体を貸し出して、インストールしてもらいます。

ポイント

配布機能を利用して、利用者のコンピュータにソフトウェアをインストールすることもできます。

関連リンク

- [1.13.1 ソフトウェアをインストールする流れ](#)

(6) ソフトウェアライセンスの利用状況を確認する

ソフトウェアライセンス情報と管理ソフトウェア情報を登録していると、ソフトウェアライセンスの利用状況を確認できます。ソフトウェアライセンスの利用状況を確認することで、ソフトウェアライセンスに過不足がないかを把握できます。

ソフトウェアライセンスの利用状況は、資産画面の「ソフトウェアライセンス状況」画面で確認できます。「ソフトウェアライセンス状況」画面には、管理ソフトウェアごとのライセンスの保有数や残数が集計されて表示されます。

【残数】がプラスの場合は、ソフトウェアライセンスが余っている状況です。

マイナスの場合は、ソフトウェアライセンスが超過している状況です。この場合、ソフトウェアライセンスを追加購入するなどの対策を検討してください。

1.10.2 余剰ライセンスを有効利用する流れ

保有しているソフトウェアを追加購入する場合、購入前に余剰ライセンスがないかソフトウェアライセンスの利用状況を確認します。

余剰ライセンスがある場合は、ソフトウェアを必要としている利用者のコンピュータにソフトウェアライセンスを割り当てて、余剰ライセンスを有効利用できます。

ポイント

ソフトウェアライセンスの利用状況を確認するには、資産画面でソフトウェアライセンス情報と管理ソフトウェア情報を登録する必要があります。

ソフトウェアライセンスが余っている場合に、ソフトウェアライセンスを有効利用する流れを次に示します。

1. ソフトウェアライセンスの利用状況を確認する

JP1/IT Desktop Management 2 で、余剰ライセンスがないかソフトウェアライセンスの利用状況を確認します。

2. 余剰ライセンスを割り当てる

余剰ライセンスがあることを確認できたら、ソフトウェアを必要としている利用者のコンピュータにソフトウェアライセンスを割り当てます。

また、利用者にソフトウェアをインストールするように連絡します。

ソフトウェアライセンスを割り当てたコンピュータにソフトウェアがインストールされて、余剰ライセンスが有効利用されます。

関連リンク

- [1.10 ソフトウェアライセンスを管理する](#)

(1) ソフトウェアライセンスの利用状況を確認する

ソフトウェアライセンス情報と管理ソフトウェア情報を登録していると、ソフトウェアライセンスの利用状況を確認できます。ソフトウェアライセンスの利用状況を確認することで、ソフトウェアライセンスに過不足がないかを把握できます。

ソフトウェアライセンスの利用状況は、資産画面の「管理ソフトウェア」画面で確認できます。「管理ソフトウェア」画面には、管理ソフトウェアごとのライセンスの保有数や残数が集計されて表示されます。

「残数」がプラスの場合は、ソフトウェアライセンスが余っている状況です。

マイナスの場合は、ソフトウェアライセンスが超過している状況です。この場合、ソフトウェアライセンスを追加購入するなどの対策を検討してください。

(2) 余剰ライセンスを割り当てる流れ

ソフトウェアライセンスの利用状況を確認して余剰ライセンスがあることを確認できたら、余剰ライセンスを有効利用するため、ソフトウェアを必要としている利用者のコンピュータにソフトウェアライセンスを割り当てます。

また、利用者にソフトウェアをインストールするように連絡して、ソフトウェアがインストールされたか確認します。

1. ソフトウェアライセンスをコンピュータに割り当てる

余剰ライセンスを有効利用するため、ソフトウェアを必要としている利用者のコンピュータにソフトウェアライセンスを割り当てます。

2. ソフトウェアをインストールするように指示する

ソフトウェアライセンスを割り当てたら、利用者にソフトウェアをインストールするように連絡します。

3. ソフトウェアがインストールされたか確認する

ソフトウェアがインストールされたかチェックするため、資産画面の「ソフトウェアライセンス状況」画面で、「インストール済みコンピュータ」タブを確認します。

「インストール済みコンピュータ」タブには、ソフトウェアをインストールしているコンピュータが表示されます。ソフトウェアライセンスを割り当てたコンピュータにソフトウェアがインストールされたか確認してください。

ソフトウェアライセンスを割り当てたコンピュータにソフトウェアがインストールされて、余剰ライセンスが有効利用されます。

関連リンク

- (3) 許可なく利用されているソフトウェアライセンスを対処する流れ
- 11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順

(3) 許可なく利用されているソフトウェアライセンスを対処する流れ

ソフトウェアライセンス数に制限がある場合は、ソフトウェアの使用を許可したコンピュータだけにソフトウェアがインストールされている必要があります。そのため、許可したコンピュータ以外でソフトウェアが不正にインストールされていないか、JP1/IT Desktop Management 2 で日々確認してください。許可なく利用されているソフトウェアライセンスがある場合は、利用者に使用目的を確認して対処します。

ポイント

ダイジェストレポートの [超過しているソフトウェアライセンス] で、超過ライセンスのソフトウェア数を確認できます。また、ダイジェストレポートをメールで送付することもできます。

許可なく利用されているソフトウェアライセンスを対処する流れを次に示します。

1. コンピュータにソフトウェアライセンスを割り当てる

JP1/IT Desktop Management 2 で、ソフトウェアの使用を許可するコンピュータにソフトウェアライセンスを割り当てます。

2. 割り当てたソフトウェアライセンスの利用状況を確認する

JP1/IT Desktop Management 2 で、ソフトウェアの使用を許可するコンピュータ以外でソフトウェアが不正にインストールされていないか確認します。

3. ソフトウェアライセンスの利用違反に対処する

許可していないコンピュータにソフトウェアがインストールされている場合は、利用者に使用目的を確認します。正当な理由でソフトウェアを使用している場合は、ソフトウェアライセンスを割り当てて、ソフトウェアの使用を許可します。

ソフトウェアライセンスが適切に利用されている状態になります。

関連リンク

- 1.10 ソフトウェアライセンスを管理する
- 15.6.2 ダイジェストレポートの送付先を設定する手順

(4) コンピュータにソフトウェアライセンスを割り当てる

許可したコンピュータにだけソフトウェアがインストールされているかを確認できるようにするため、資産画面の [ソフトウェアライセンス] 画面で、ソフトウェアの使用を許可するコンピュータにソフトウェアライセンスを割り当てます。

関連リンク

- 11.2.4 ソフトウェアライセンス情報を追加する手順
- 11.2.1 管理ソフトウェア情報を追加する手順
- 11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順

(5) 割り当てたソフトウェアライセンスの利用状況を確認する

コンピュータにソフトウェアライセンスを割り当てたあとは、ソフトウェアが正しく利用されているか、次の点を定期的に確認します。

ソフトウェアライセンスの余剰や超過がないか確認する

資産画面の「ソフトウェアライセンス状況」画面で、管理ソフトウェアの「保有数」、「ライセンス消費数」、および「残数」から、ソフトウェアライセンスの利用状況を確認します。

「保有数」には、管理ソフトウェアに対応するソフトウェアライセンスの保有ライセンス数が表示されます。「ライセンス消費数」には、管理ソフトウェアの利用数が表示されます。「残数」には、「保有数」から「ライセンス消費数」を引いた値が表示されます。

ポイント

「残数」がプラスの場合は、ソフトウェアライセンスが余っている状況です。マイナスの場合は、ソフトウェアライセンスが不足している状況です。

ソフトウェアライセンスを割り当てているコンピュータにだけソフトウェアがインストールされているか確認する

割り当てたソフトウェアライセンスの利用状況を確認します。

資産画面の「ソフトウェアライセンス状況」画面で、管理ソフトウェアの「ライセンス消費数」と「割り当てライセンス数」の値が同じか確認します。「ライセンス消費数」と「割り当てライセンス数」の値が異なるときは、ソフトウェアライセンスの利用状況を確認してください。

表示項目に「割り当てライセンス数」が表示されていない場合は、一覧の項目名を右クリックして「表示項目の選択」を選択してください。表示されるダイアログで「割り当てライセンス数」をチェックして「OK」ボタンをクリックすると、表示項目に「割り当てライセンス数」が表示されます。

保有数	ライセンス消費数	残数	割り当てライセンス数
10	11	-1	11

- 「ライセンス消費数」 > 「割り当てライセンス数」 の場合

ソフトウェアを許可なくインストールしているコンピュータがあるおそれがあります。「インストール済みコンピュータ」タブを選択して、「未割り当てコンピュータだけを表示する」をチェックしてください。ソフトウェアライセンスが割り当てられていないのに、ソフトウェアをインストールしているコンピュータを確認できます。

- 「ライセンス消費数」 < 「割り当てライセンス数」 の場合

ソフトウェアライセンスが有効に利用されていないおそれがあります。[割り当て済みコンピュータ] タブを選択して、[未インストールのコンピュータだけを表示する] をチェックしてください。ソフトウェアライセンスが割り当てられているのに、ソフトウェアをインストールしていないコンピュータを確認できます。

ポイント

[ソフトウェアライセンス] タブに複数のソフトウェアライセンスがある場合は、有効に利用されていないソフトウェアライセンスがどれかを調査します。[残数] 欄を確認し、残数の多いソフトウェアライセンスが、有効に利用されていないソフトウェアライセンスです。

(6) ソフトウェアライセンスの利用違反に対処する流れ

ソフトウェアライセンスの利用状況を確認して、許可していないコンピュータにソフトウェアがインストールされていた場合は、利用者に使用目的を確認します。正当な理由でソフトウェアを使用している場合はソフトウェアライセンスを割り当てて、ソフトウェアの使用を許可します。

1. 利用者に使用目的を確認する

資産画面の [ソフトウェアライセンス状況] 画面で、[インストール済みコンピュータ] タブを選択して、[未割り当てコンピュータだけを表示する] をチェックしてください。表示されたコンピュータの利用者に、許可なくソフトウェアがインストールされていることを連絡して、使用目的を確認します。

2. コンピュータにソフトウェアライセンスを割り当てる

正当な理由でソフトウェアを使用している場合は、コンピュータにソフトウェアライセンスを割り当てて、ソフトウェアの使用を許可します。

正当な理由と認められない場合は、ソフトウェアをアンインストールするように指示するか、配布機能を利用してソフトウェアをアンインストールします。また、使用を許可していないソフトウェアを今後インストールしないように利用者に注意します。

3. ソフトウェアライセンスの利用状況を確認する

資産画面の [ソフトウェアライセンス状況] 画面で、[ライセンス消費数] と [割り当てライセンス数] の値が同じか確認します。また、[残数] をチェックしてソフトウェアライセンスの超過が発生していないか確認します。

[ライセンス消費数] と [割り当てライセンス数] の値が同じで、かつ、ソフトウェアライセンスの超過が発生していないことを確認できたら、ソフトウェアライセンスが適切に利用されている状態になります。

なお、ソフトウェアライセンスが適切に利用されていることを確認できても、定期的にソフトウェアライセンスの利用状況を確認してください。

関連リンク

- [11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順](#)
- [12.3 コンピュータからソフトウェアをアンインストールする手順](#)

1.10.3 ソフトウェアライセンスを棚卸する流れ

組織で利用しているソフトウェアライセンスを管理するためには、定期的に棚卸を実施して、現状を正しく把握しておく必要があります。JP1/IT Desktop Management 2 に現品確認の結果を登録することで、現品確認できなかったソフトウェアライセンスの情報を簡単に抽出できるようになります。

ソフトウェアライセンスを棚卸する流れを次に示します。

1. 現品確認を実施する

ソフトウェアライセンス情報の一覧を作成し、組織内のすべてのソフトウェアライセンスを現品確認します。

2. 現品確認の結果を反映する

ソフトウェアライセンスの棚卸状況を管理するため、JP1/IT Desktop Management 2 に現品確認の結果を反映します。

3. 現品確認できなかったソフトウェアライセンスを調査する

現品確認できなかったソフトウェアライセンスの利用状況を調査します。確認できたソフトウェアライセンスは JP1/IT Desktop Management 2 に現品確認の結果を反映します。

ソフトウェアライセンスの棚卸結果が JP1/IT Desktop Management 2 に反映されます。

関連リンク

- [1.10 ソフトウェアライセンスを管理する](#)

(1) 現品確認を実施する流れ

ソフトウェアライセンスを現品確認するには、ソフトウェアライセンス情報の一覧を出力して、現品と突き合わせて確認します。

1. ソフトウェアライセンス情報の一覧をエクスポートする

現品を確認するために、ソフトウェアライセンス情報の一覧を作成します。資産画面の [ソフトウェアライセンス] 画面でソフトウェアライセンス情報を CSV ファイルにエクスポートしてください。ソフトウェアライセンスを識別するために、[ライセンス管理番号]、[棚卸日]、[ライセンス名]、[ライセンス数]、[ライセンス種類] などの項目をエクスポートしてください。なお、ここでエクスポートした CSV ファイルは、現品確認の結果を反映するときにも使用します。[ライセンス管理番号] および [棚卸日] の項目は、必ずエクスポートしてください。

2. ソフトウェアライセンス情報の一覧を基に現品確認する

ソフトウェアライセンス情報の一覧を作成したら、現品確認します。

確認が必要なものを次に示します。

- 媒体
- ライセンス証書（売買契約書）

ソフトウェアライセンス情報の一覧とライセンス証書および媒体を突き合わせて、対象のソフトウェアライセンスがあるかどうかを確認します。現品確認できた場合は、一覧の該当ソフトウェアライセンスに、現品確認できたことを示す印を付けます。ここで印を付けたソフトウェアライセンスの棚卸日を、JP1/IT Desktop Management 2 で更新します。

現品確認が完了し、確認結果が記入されたソフトウェアライセンスの一覧が完成します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- (2) 現品確認の結果を反映する流れ

(2) 現品確認の結果を反映する流れ

ソフトウェアライセンスの棚卸状況を管理するため、JP1/IT Desktop Management 2 に現品確認の結果を反映します。現品確認の結果を反映すると、資産画面の [ソフトウェアライセンス] 画面でソフトウェアライセンス情報の [棚卸日] が更新されます。

1. 棚卸日を更新した CSV ファイルを作成する

棚卸日を一括更新するために、棚卸日を更新したソフトウェアライセンス情報の CSV ファイルを作成します。現品確認したときに使用した CSV ファイルを編集して、現品確認できたソフトウェアライセンスの [棚卸日] を更新してください。

ポイント

現品確認をしたときに、[ライセンス数]、[ライセンス状態] などのソフトウェアライセンス情報が変更されていた場合は、CSV ファイルを編集して、[棚卸日] と同時に更新してください。

2. 棚卸日を更新する

CSV ファイルを作成したら、ソフトウェアライセンス情報の CSV ファイルをインポートして、一括で棚卸日を更新します。

現品確認できたソフトウェアライセンスは、ソフトウェアライセンス情報の [棚卸日] が更新されます。

ポイント

手もとにあるソフトウェアライセンスを個別に確認したい場合は、手動で 1 件ずつ棚卸日を更新してください。

関連リンク

- [11.1.8 手動で棚卸日を更新する手順](#)

(3) 現品確認できなかったソフトウェアライセンスを調査する流れ

現品確認できなかったソフトウェアライセンスは、利用状況を調査して、再度現品確認する必要があります。

1. 現品確認できなかったソフトウェアライセンスを確認する

資産画面の「ソフトウェアライセンス」画面で、「棚卸日」が更新されていないソフトウェアライセンス情報を確認します。フィルタを利用して、「棚卸日」が最新の棚卸日より古いソフトウェアライセンス情報を表示します。

2. ソフトウェアライセンス情報の一覧をエクスポートする

現品を調査するために、ソフトウェアライセンス情報の一覧を作成します。棚卸日が更新されていないソフトウェアライセンス情報を CSV ファイルにエクスポートしてください。ソフトウェアライセンスを識別するために、「ライセンス管理番号」、「ライセンス名」、「ライセンス数」、「ライセンス種類」などの項目をエクスポートしてください。

3. ソフトウェアライセンスを調査する

ソフトウェアライセンス情報の一覧を作成したら、現品（ライセンス証書、媒体）がどこにあるか探します。

ソフトウェアライセンスが見つかった場合

ライセンス証書や媒体が見つかった場合は、ソフトウェアライセンスの現品確認ができたことを一覧に記載します。ソフトウェアライセンス情報に修正があれば、同時に記載します。

ソフトウェアライセンスが見つからなかった場合

ライセンス証書や媒体が紛失したおそれがあります。管理者に状況を確認してください。紛失していた場合は、資産画面の「ソフトウェアライセンス」画面で該当ソフトウェアライセンスの「ライセンス状態」を「滅却」にします。また、紛失理由や紛失日時などを「ノート」タブにメモしておきます。

4. 現品確認の結果を反映する

現品確認できたソフトウェアライセンスについて、現品確認の結果を反映します。

ソフトウェアライセンスの棚卸が完了します。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [\(2\) 現品確認の結果を反映する流れ](#)
- [1.10.4 ソフトウェアライセンスを滅却する流れ](#)

1.10.4 ソフトウェアライセンスを滅却する流れ

バージョンが古くなるなどして利用しなくなったソフトウェアは、ソフトウェアライセンスを滅却します。

ソフトウェアライセンスを滅却する流れを次に示します。

1.ソフトウェアライセンスが必要かどうかを判断する

ソフトウェアの利用中止を申請されたら、該当するソフトウェアライセンスが必要かどうかを判断してください。減価償却が完了していたら、ほかにソフトウェアを利用したい人がいないことを確認して、減却を決定します。

2.ソフトウェアライセンスを減却して反映する

減却することを決定したら、ソフトウェアの媒体を処分して、コンピュータからアンインストールされていることを確認します。減却したソフトウェアライセンスは、JP1/IT Desktop Management 2 でソフトウェアライセンス情報をメンテナンスします。

減却したソフトウェアライセンスとして、JP1/IT Desktop Management 2 で管理されます。

関連リンク

- [1.10 ソフトウェアライセンスを管理する](#)

(1) ソフトウェアライセンスが必要かどうかを判断する流れ

ソフトウェアの利用者から利用中止の申請を受けたら、該当するソフトウェアライセンスを減却してもよいかどうかを判断する必要があります。利用状況や減価償却状況などを確認して、不要なソフトウェアライセンスの減却を決定します。

1.ソフトウェアのインストール数を確認する

減却対象のソフトウェアライセンスを利用している人がいないことを確認します。資産画面の［ソフトウェアライセンス状況］画面で、該当するソフトウェアの［ライセンス消費数］を確認してください。消費数が「0」以外の場合は、ほかにソフトウェアの利用者がいるため、ソフトウェアライセンスの減却を中止します。なお、利用中止の申請をした利用者のコンピュータからは、対象のソフトウェアがアンインストールされているものとします。

2.減価償却が完了していることを確認する

減却対象のソフトウェアライセンスの減価償却が完了していることを確認します。資産画面の［ソフトウェアライセンス］画面の［契約情報］タブを選択して、ソフトウェアライセンスに対応する契約を表示します。契約の［総額］と［契約日］などを参考に、減価償却が完了していることを確認してください。

3.ほかにソフトウェアを利用したい人がいないことを確認する

利用者にソフトウェアライセンスの減却予定をメールで通知し、ほかにソフトウェアを利用したい人がいないことを確認します。利用希望者がいた場合は、ソフトウェアライセンスを希望者のコンピュータに割り当てます。

すべての確認が完了したら、不要と判断したソフトウェアライセンスだけを減却します。

関連リンク

- [\(2\) ソフトウェアライセンスを減却して反映する流れ](#)

(2) ソフトウェアライセンスを滅却して反映する流れ

ソフトウェアライセンスを必要ないと判断した場合、ソフトウェアライセンスを滅却します。媒体を処分したあと、該当ソフトウェアがインストールされているコンピュータが残っていないかどうかを確認します。確認が完了したらソフトウェアライセンス情報を最新の状態にメンテナンスします。

1. ソフトウェアの媒体を処分する

ソフトウェアの再利用を防ぐため、媒体を処分します。CD/DVD であれば表面に傷を付けたり、専用の装置で粉碎したりして内容を読み込めないようにしてください。

2. ソフトウェアのアンインストールを確認する

媒体を処分したら、滅却を決定したあとにインストールされたソフトウェアがないことを確認します。資産画面の [ソフトウェアライセンス状況] 画面の [インストール済みコンピュータ] タブで、該当ソフトウェアをインストールしているコンピュータがないことを確認してください。インストールしているコンピュータがあった場合、コンピュータの利用者に該当ソフトウェアをアンインストールするように指示します。

3. ソフトウェアライセンス状態をメンテナンスする

ソフトウェアのアンインストールを確認したら、ソフトウェアライセンス情報を最新の状態にメンテナンスします。資産画面の [ソフトウェアライセンス] 画面で、該当するソフトウェアライセンスの [ライセンス状態] を「使用中」から「滅却」に変更します。

ソフトウェアライセンスの滅却と JP1/IT Desktop Management 2 への反映が完了します。

関連リンク

- [11.2.8 ライセンス状態を変更する手順](#)

1.11 資産に関する契約を管理する流れ

JP1/IT Desktop Management 2 で契約情報を管理すると、次に示すような便利な機能を利用して効率良く契約の状況を把握できます。

- ・ 契約対象のハードウェア資産やソフトウェアライセンスを簡単に把握できる
- ・ 契約満了が近づいている契約情報を素早く把握でき、今後の運用計画に役立てられる
- ・ ハードウェア資産やソフトウェアライセンスに掛かっているコストを把握できる

契約情報の管理は、資産画面の〔契約〕画面で実行します。契約情報の管理を始めるためには、まず契約情報を登録する必要があります。契約情報を登録したあとは、契約対象の機器の追加、契約の満了や更新などのイベントに応じて契約情報をメンテナンスしてください。

資産に関する契約を管理する流れを次に示します。

1. 契約情報を管理する

契約情報を登録します。また、必要に応じて契約情報を編集したり、削除したりすることで、契約情報を最新の状態に保つようにします。

2. 満了となる契約情報を把握する

JP1/IT Desktop Management 2 から自動的に通知されるメールを確認して、契約期間の満了が近づいていることを把握します。今後も契約を継続する場合は更改し、継続利用の必要がない場合は契約を終了します。

3. 契約を更改する

今後も継続したい契約を更改します。契約会社の担当者から更改情報を入手して、満了分と継続分の2つに分けて契約情報を管理します。

4. 契約を終了する

継続して利用しない契約を終了します。JP1/IT Desktop Management 2 で契約状態を変更したら、契約対象の資産を業者へ返却したり、滅却したりします。

1.11.1 満了となる契約情報を把握する

JP1/IT Desktop Management 2 から、契約の期限についての情報が、メールで通知されるように設定できます。メールは自動的に通知されるため、期限の切れそうな契約について JP1/IT Desktop Management 2 の操作画面を開かなくても定期的に把握できます。

メール本文には、契約満了が迫っている契約や期限切れとなっている契約など、ダイジェストレポートに表示される内容が記載されます。なお、メール本文の契約数のリンクをクリックすると、JP1/IT Desktop Management 2 の操作画面が起動して、資産画面の〔契約〕画面で該当する契約情報の一覧が表示されます。契約情報の詳細を知りたい場合は、リンクをクリックしてください。

1. 満了となる契約情報を通知するように設定する

設定画面の [ダイジェストレポートの設定] 画面で、ダイジェストレポートの送信先を設定できます。送信先が1つも設定されていない場合は、ダイジェストレポートは送信されません。なお、メールの送信機能を利用するためには、メールサーバの設定が必要です。

2. 満了となる契約情報を把握する

JP1/IT Desktop Management 2 から送信されたメールを確認して、契約満了が迫っている契約や期限切れとなっている契約を確認します。契約満了が迫っている契約は、更改するか終了するかを判断します。また、期限切れとなっている契約は、契約対象のハードウェア資産やソフトウェアライセンスを確認して、契約の更改や終了を行ってください。

関連リンク

- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [15.8.1 メールサーバを設定する手順](#)
- [11.3.1 契約情報を追加する手順](#)
- [1.11.2 契約を更改する](#)
- [1.11.3 契約を終了する](#)

1.11.2 契約を更改する

満了となる契約情報を把握したら、契約を継続するものについて、契約を更改します。

ポイント

契約を継続する場合は、過去の契約情報も引き続き参照できるように、満了分と継続分の2つに分けて契約情報を管理します。

1. 担当者から更改情報を入手する

契約会社の担当者に、更改情報の送付を依頼します。

2. 継続分の契約情報を登録する

更改情報を入手したら、満了分の契約情報をコピーして継続分の契約情報を登録します。資産画面の [契約] 画面で、該当の契約情報を選択して [編集] ボタンをクリックし、表示されたダイアログで [別の契約として保存] ボタンをクリックします。

新規に保存された契約情報を編集し、[契約期間]、[契約日]、[契約状態] などの変更が必要な項目を更新してください。

3. 満了分の契約情報の契約状態を変更する

満了日になったら、満了分の契約情報の [契約状態] を変更します。資産画面の [契約] 画面で [状態を変更] ボタンをクリックします。表示されるダイアログで、[満了] を選択してください。

4.対象となる資産を更新する

契約の対象となるソフトウェアライセンスまたはハードウェア資産が変更されている場合は、対象となる資産情報への関連づけを更新します。資産画面の「契約」画面で「ソフトウェアライセンス」タブまたは「ハードウェア資産」タブを選択して、関連する資産情報を編集してください。

関連リンク

- [11.3.2 契約情報を編集する手順](#)
- [1.11.3 契約を終了する](#)

1.11.3 契約を終了する

満了となる契約情報を把握したら、継続して利用しない資産について、契約を終了します。

契約を満了するためには、資産画面の「契約」画面で「状態を変更」ボタンをクリックします。表示されるダイアログで、「満了」を選択してください。

また、ハードウェア資産の「契約種別」が「リース」および「レンタル」の場合は、資産を返却します。資産を業者に返却したあとで、対象のハードウェア資産情報を削除するか、「資産状態」を「滅却」にします。

ソフトウェアライセンスの契約を終了する場合は、資産の返却は必要ありません。

■ 注意事項

「ハードウェア資産の費用」レポートおよび「ソフトウェアライセンスの費用」レポートで集計される契約費用は、契約情報の「契約期間」に設定した契約終了日までで算出されます。そのため、契約を途中解約した場合は、契約情報の「契約期間」を編集して、契約終了日を変更してください。

関連リンク

- [11.3.2 契約情報を編集する手順](#)
- [1.11.2 契約を更改する](#)

1.12 資産のコスト削減を検討する流れ

JP1/IT Desktop Management 2 では、ハードウェア資産やソフトウェアライセンスの運用に掛かっているコストを把握できます。また、利用されていない資産をほかの利用者に割り当てたり、余剰が多いライセンスの契約を解約したりなどのコスト削減に関する作業を支援します。

ハードウェア資産やソフトウェアライセンスに掛かるコストを把握して、効率的に資産を運用する流れを次に示します。

1. 毎月の資産に掛かるコストを確認する

コストの推移に関するレポートを確認して、コストが掛かっているハードウェア資産およびソフトウェアライセンスの中で不要なものは解約します。なお、コストの推移に関するレポートを確認するためには、契約情報に費用を設定する必要があります。

2. 利用されていない資産を確認する

利用されていないハードウェア資産やソフトウェアがないかを確認します。利用されていない資産がある場合は、不要な契約を解除することでコストを削減できます。

3. 余剰ライセンスを確認する

余剰ライセンスがあるのに新規にソフトウェアライセンスを購入していないかどうかを確認します。余計にソフトウェアライセンスを購入しないように、利用状況の確認を徹底します。

関連リンク

- [1.12.1 毎月の資産に掛かるコストを確認する](#)
- [1.12.2 利用されていない資産を確認する](#)
- [1.12.3 余剰ライセンスを確認する](#)

1.12.1 毎月の資産に掛かるコストを確認する

ハードウェア資産やソフトウェアライセンスに毎月掛かっているコストを確認します。不要な契約は解約して、コスト削減を図ります。

1. コストに関するレポートを確認する

レポート画面で、[ハードウェア資産の費用] レポートおよび [ソフトウェアライセンスの費用] レポートを確認します。前月の契約費用が大きいと判断したハードウェア資産およびソフトウェアライセンスの契約種別を資産画面で調査します。

2. 契約情報の詳細を確認する

資産画面の [契約] 画面を参照して、メニューエリアで [ハードウェア資産] または [ソフトウェアライセンス] のフィルタを選択します。また、インフォメーションエリアのフィルタで [契約状態] および [契約種別] を選択すると、一覧の情報が絞り込まれます。[契約状態] は「契約中」を選択します。

【契約種別】は、レポートを確認して契約費用が大きいと判断した【契約種別】を選択してください。一覧の情報を絞り込んだら、【契約情報】タブでそれぞれの詳細を確認します。

3. 不要な契約を解約する

画面下部のタブで詳細を確認し、不要な契約がないかどうか判断します。例えば、現在ソフトウェアライセンスが利用されていない、および今後も利用しないと判断した場合は、契約会社に連絡して解約します。

4. 【契約状態】を「途中解約」に変更する

契約を解約したら、【契約状態】を「契約中」から「途中解約」に変更します。

注意事項

【ハードウェア資産の費用】レポートおよび【ソフトウェアライセンスの費用】レポートで集計される契約費用は、契約情報の【契約期間】に設定した契約終了日までで算出されます。そのため、契約を途中解約した場合は、契約情報の【契約期間】を編集して、契約終了日を変更してください。

関連リンク

- [11.3.5 契約状態を変更する手順](#)

1.12.2 利用されていない資産を確認する

利用されていないハードウェア資産やソフトウェアがないかを確認します。利用されていない資産がある場合は、不要な契約を解除することでコストを削減できます。ここでは、利用されていないソフトウェアを確認する方法について説明します。

高額なソフトウェアライセンスの中で、利用されていないものを調査します。利用されていないと判断したソフトウェアライセンスの契約を解約したり、ほかの利用者に割り当てたりすることで、効率的に資産を運用します。

1. 高額なソフトウェアを一覧で確認する

資産画面の【契約】画面を参照して、メニューエリアで【ソフトウェアライセンス】のフィルタを選択します。

ソフトウェアライセンスの契約情報を表示した状態で、表示項目の【総額】をクリックしてください。【総額】を基準に契約情報が並べ替えられます。

表示項目に【総額】が表示されていない場合は、一覧の項目名を右クリックして【表示項目の選択】を選択してください。表示されるダイアログで【総額】をチェックして【OK】ボタンをクリックすると、表示項目に【総額】が表示されます。

ポイント

あらかじめ一定の金額以上の管理ソフトウェアを表示するフィルタを作成しておく、簡単に高額な管理ソフトウェアを把握できます。

2.ソフトウェアライセンスの利用状況を確認する

高額なソフトウェアライセンスを選択し、[ソフトウェアライセンス] タブで[残数]を確認します。数値が0だった場合は、ライセンスの余剰はないため、問題ありません。数値が1以上だった場合は、ソフトウェアライセンスが余っていて有効に利用されていないおそれがあります。利用者を募集して、希望者のコンピュータにソフトウェアライセンスを割り当ててください。

3.利用者に管理ソフトウェアの利用状況を確認する

ソフトウェアライセンスの残数がない場合は、特に高額なソフトウェアライセンスについて、利用者に利用状況を確認します。

4.管理ソフトウェアのアンインストールを指示する

利用者から、該当する管理ソフトウェアを利用していないという連絡をもらった場合は、管理ソフトウェアのアンインストールを指示します。

関連リンク

- [1.9.6 利用されていない機器を確認する流れ](#)
- [11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順](#)

1.12.3 余剰ライセンスを確認する

ソフトウェアライセンスの利用状況を確認します。余剰ライセンスが多い管理ソフトウェアは、追加購入していないかどうかを確認して、効率的にソフトウェアライセンスを運用します。

1.余剰ライセンスが多いソフトウェアを確認する

資産画面の[ソフトウェアライセンス状況] 画面を表示します。インフォメーションエリアの表示項目で[残数]を選択すると、管理ソフトウェアのライセンスの残数の順番に並べ替えられます。残数が多いものは、ソフトウェアライセンスが有効に利用されていないおそれがあります。

2.余剰ライセンスがあるのに追加購入していないかどうか確認する

余剰ライセンスが多いソフトウェアを確認したら、その中で最近ソフトウェアを追加購入しているものがないかどうかを確認します。[ソフトウェアライセンス] タブで[登録日時] が新しいものを調査してください。

表示項目に[登録日時]が表示されていない場合は、一覧の項目名を右クリックして[表示項目の選択]を選択してください。表示されるダイアログで[登録日時]をチェックして[OK] ボタンをクリックすると、表示項目に[登録日時]が表示されます。

余剰ライセンスがあるのにソフトウェアライセンスを新規購入していた場合は、該当ソフトウェアライセンスを購入した管理者に余剰ライセンスを確認してから購入するように注意を促します。

関連リンク

- [11.2.1 管理ソフトウェア情報を追加する手順](#)
- [11.2.2 管理ソフトウェア情報を編集する手順](#)
- [11.3.3 契約情報を削除する手順](#)
- [\(2\) 余剰ライセンスを割り当てる流れ](#)

1.13 ソフトウェアやファイルの配布

配布機能を利用すると、組織内のコンピュータに必要なソフトウェアをインストールしたり、不要なソフトウェアをアンインストールしたりできます。また、ソフトウェアだけではなく、ファイルも配布できます。

コンピュータの利用者が個別にソフトウェアをインストールまたはアンインストールする必要がなくなり、ソフトウェアの導入や管理に掛かる手間を省けます。また、最新バージョンのソフトウェアを一括でインストールできるなど、ソフトウェアの保守が簡単になります。

注意事項

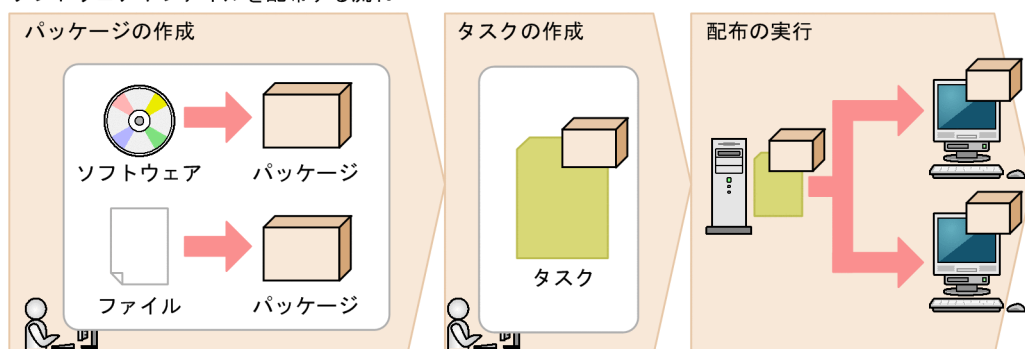
配布機能を利用できるのは、オンライン管理のコンピュータだけです。

配布機能を利用すると、次に示すような便利な機能を利用して効率良くソフトウェアのインストールやアンインストール、ファイルの配布ができます。

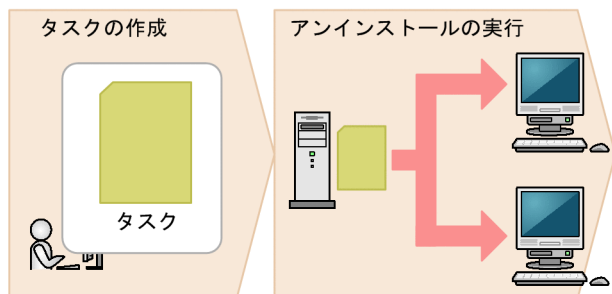
- ・ 利用者が操作することなく、ソフトウェアのインストールやアンインストールができる
- ・ スケジュールやインストールタイミングを設定して、業務都合に応じて配布できる
- ・ パネルやレポートなどのグラフィカルな画面から、配布の実行状況を簡単に把握できる

配布機能の流れを次の図に示します。

ソフトウェアやファイルを配布する流れ



ソフトウェアをアンインストールする流れ



最初に、インストールするソフトウェアまたは配布するファイルをパッケージとして管理用サーバに登録します。次に、パッケージの配布を開始するスケジュールや、配布先のコンピュータでの動作を指定した

タスクを作成します。タスクを作成すると、指定したスケジュールに従ってパッケージが配布されます。ソフトウェアをアンインストールする場合は、アンインストール用のタスクを作成します。アンインストールの場合、パッケージの作成は不要です。

ここでは、次に示す業務での JP1/IT Desktop Management 2 の利用方法を説明しています。目的の業務に応じて説明を参照してください。

ソフトウェアをインストールする

ソフトウェアの新規導入やバージョンアップなどに伴って、組織内のコンピュータにソフトウェア（インストーラーがあるソフトウェア）をインストールする場合について説明します。

ファイルを配布する

各コンピュータに格納されている設定ファイルの更新や、インストール不要の自社ソフトウェアの展開などに伴って、組織内のコンピュータにファイルを配布する場合について説明します。

ソフトウェアをアンインストールする

組織内のコンピュータから、業務に不要なソフトウェアや使用を禁止しているソフトウェアをアンインストールする場合について説明します。

1.13.1 ソフトウェアをインストールする流れ

ソフトウェアの新規導入やバージョンアップなどに伴って、組織内のコンピュータにソフトウェアをインストールする場合は、配布機能を利用できます。

組織内のコンピュータにソフトウェアを配布してインストールする流れを次に示します。

1. ソフトウェアのインストール状況を確認する

ソフトウェアをバージョンアップしたりライセンスを追加したりする場合は、ソフトウェアのインストール状況を確認して必要な本数を把握します。その後、確認結果に応じて必要な本数だけソフトウェアを購入します。

2. ソフトウェアの配布計画を立てる

ソフトウェアを配布する前に配布計画を立てます。また、配布計画は事前に利用者に通知しておきます。

3. コンピュータにソフトウェアをインストールする

ソフトウェアをインストールするには、インストールするソフトウェアを登録したパッケージと、パッケージを配布するタスクを作成します。タスクに指定したスケジュールに従って、パッケージが配布されます。

4. タスクの実行結果を確認する

配布の実行状況を確認します。配布またはインストールに失敗したコンピュータがある場合は、原因を確認して対処したあと、タスクを再実行します。

指定したすべてのコンピュータにソフトウェアがインストールされます。

関連リンク

- 1.13 ソフトウェアやファイルの配布

(1) ソフトウェアのインストール状況を確認する

ソフトウェアをバージョンアップしたりライセンスを追加したりする場合、配布が必要な本数を把握するために事前にソフトウェアのインストール状況を確認します。その後、確認結果に応じて必要な本数だけソフトウェアを購入します。

ソフトウェアのインストール状況とライセンスの利用状況は、資産画面の「管理ソフトウェア」画面で確認できます。

The screenshot shows the 'IT Desktop Management 2' application. The left sidebar contains a navigation menu with options like 'サマリー', 'ハードウェア資産', 'ソフトウェアライセンス', and '管理ソフトウェア'. The main area is titled '管理ソフトウェア一覧' and shows a list of 5 software items. Below this, a detailed view for 'Software1' is expanded, showing fields like '管理ソフトウェア名', '説明', 'ライセンス種類', '保有数', 'ライセンス消費数', '残数', '割り当てライセンス数', 'メーカー', '登録日時', and '更新日時'.

管理ソフトウェア名	メーカー	ライセンス種類	保有数	ライセンス消費数	残数
Software1		インストールライ...	10	0	10
Software10		インストールライ...	100	0	100
Software3		インストールライ...	100	0	100
Software4		インストールライ...	200	0	200
Software5		インストールライ...	30	0	30

項目	値
管理ソフトウェア名	Software1
説明	
ライセンス種類	インストールライセンス
保有数	10
ライセンス消費数	0
残数	10
割り当てライセンス数	0
メーカー	
登録日時	2014/08/04 15:49:45
更新日時	2014/08/04 15:49:45

ソフトウェアをバージョンアップする場合、バージョンアップ対象となる古いバージョンのソフトウェアがインストールされているコンピュータ台数を確認してください。ソフトウェアライセンスを追加する場合は、インストール先となるコンピュータの台数を確認してください。

ポイント

ソフトウェアライセンスを追加する場合、余剰ライセンスがあるかどうかを確認することをお勧めします。余っているソフトウェアライセンスを使用して、不足分だけを購入すると余剰ライセンスを活用できます。

ソフトウェアの購入数が決まったら、業者に発注します。購入したソフトウェアは、JP1/IT Desktop Management 2 に資産情報（ソフトウェアライセンス情報と管理ソフトウェア情報）を登録して、ソフトウェアライセンスの利用状況を把握できるようにします。

関連リンク

- [1.10.2 余剰ライセンスを有効利用する流れ](#)
- [1.10.1 ソフトウェアを購入する流れ](#)

(2) ソフトウェアの配布計画を立てる

ソフトウェアを配布する前に配布計画を立てます。また、配布計画は事前に利用者に通知しておきます。

1. ソフトウェアの配布計画を立てる

ソフトウェアの配布計画として、次のような項目を検討します。

- ソフトウェアを配布するコンピュータ
- ソフトウェアを配布する日時

ソフトウェアを配布する日時は、ネットワークの負荷を考慮して検討してください。例えば、業務に支障がないように夜間に配布する、コンピュータの台数が多いので複数日に分けて配布するなどの計画を立てます。

なお、配布機能を実行するには事前に必要な準備があります。

ポイント

ソフトウェアを配布する前に、テスト用のコンピュータを使用して、ソフトウェアが正常に配布されてインストールされるか確認することをお勧めします。

2. 利用者にソフトウェアの配布計画を通知する

インストールが計画どおりに実行されるように、また、インストールに伴う問い合わせが発生しないように、ソフトウェアの配布計画を事前にコンピュータの利用者に通知しておきます。例えば、次のような情報を通知します。

- ソフトウェア名
- バージョン
- 配布理由
- 配布日時
- 注意事項

コンピュータにソフトウェアを配布するための準備が整います。

関連リンク

- [12.1 コンピュータにソフトウェアをインストールする手順](#)

(3) コンピュータにソフトウェアをインストールする手順

【ソフトウェアをインストールしましょう】ウィザードを使って、利用者のコンピュータにソフトウェアを配布してインストールできます。

【ソフトウェアをインストールしましょう】ウィザードでは、インストールするソフトウェアを登録したパッケージと、パッケージの配布を実行するタスクを作成します。ウィザードを完了すると、タスクに指定したスケジュールに従って、パッケージが配布されます。

コンピュータにソフトウェアをインストールするには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで【パッケージ】－【パッケージ一覧】を選択します。
3. インフォメーションエリアで【操作メニュー】から【インストールウィザードを起動する】を選択してウィザードを起動します。
4. 【はじめに...】画面でウィザードの流れを確認して、【次へ】ボタンをクリックします。
5. 【ソフトウェアを指定する】画面で【新しいパッケージを作成する】を選択して、パッケージに登録するファイルを指定し、【次へ】ボタンをクリックします。
事前にパッケージを作成している場合は、作成済みのパッケージを選択することもできます。
6. 【パッケージを設定する】画面でパッケージ情報を設定して、【次へ】ボタンをクリックします。
7. 【パッケージ配布タスクを作成する】画面で、配布を実行するスケジュールなどを設定して、【次へ】ボタンをクリックします。
【対象のコンピュータでの動作】をクリックすると、インストールを実行するタイミングや、利用者に通知するメッセージなどを設定できます。
8. 【対象のコンピュータを選択する】画面で、【変更】ボタンをクリックします。
9. 【対象のコンピュータの変更】ダイアログで、ソフトウェアをインストールするコンピュータを指定して、【OK】ボタンをクリックします。
10. 【次へ】ボタンをクリックします。
11. 【設定内容を確認する】画面で、設定内容を確認して【完了】ボタンをクリックします。
12. 【完了！】画面で、【閉じる】ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータにソフトウェアが配布されてインストールされます。タスクの実行状況は、配布（ITDM 互換）画面の【タスク】画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でソフトウェアのインストールを延期できます。

関連リンク

- 12.6 利用者側でダウンロードやインストールを延期する
- 12.5.5 タスクを中止する手順

(4) タスクの実行結果を確認する流れ

配布（ITDM 互換）画面の「タスク」画面で、タスクの実行状況を確認できます。

The screenshot shows the 'IT Desktop Management 2' application. The left sidebar contains navigation options like 'ダッシュボード', 'パッケージ', 'タスク', and 'フィルタ'. The main area is titled 'タスク一覧' (Task List) and shows a table of tasks. The table has columns: 'タスク種別' (Task Type), 'タスク名' (Task Name), '操作種別' (Operation Type), 'タスク状態' (Task Status), '開始日時' (Start Date/Time), '経過時間' (Elapsed Time), '失敗コンピ...' (Failed Computers), '状況(%)' (Status (%)), and '操作' (Action). The tasks listed are all 'TestTask...' with a status of '予約中' (On Hold). Below the table, the 'タスク情報' (Task Information) tab is active, showing details for 'TestTask0001'. This tab is divided into two sections: 'タスク情報の詳細' (Task Information Details) and 'タスク状態の詳細' (Task Status Details). The first section shows the task name, description, and schedule. The second section shows the current status, start time, completion time, and progress for different components.

タスク種別	タスク名	操作種別	タスク状態	開始日時	経過時間	失敗コンピ...	状況(%)	操作
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー

タスク情報の詳細		タスク状態の詳細	
タスク種別	管理者が実行するタスク	タスク状態	予約中
タスク名	TestTask0001	開始日時	(2099/12/31 00:00:00 実行予定)
説明		完了日時(経過時間)	-
操作種別	パッケージ配布	進捗状況(完了/対象)	0%(0/10,000 台)
実行スケジュール	2099/12/31 00:00:00	失敗	0%(0 台)
対象のコンピュータでの動作		成功	0%(0 台)
実行タイミング	すぐに実行	キャンセル	0%(0 台)
自動起動	しない	実行中	100%(10,000 台)
上書き禁止	しない		
実行前メッセージの表示	しない		
実行後メッセージの表示	しない		

タスクの実行状況は、完了するまで定期的に確認することをお勧めします。タスクの実行に失敗したコンピュータがある場合は、タスクが失敗した原因を確認して対処したあと、タスクを再実行してください。

ポイント

配布管理のイベント（タスク完了、タスク失敗など）が発生したときに自動的にメールで通知するように設定できます。

1.タスクの実行状況を確認する

配布（ITDM 互換）画面の [タスク] 画面で、実行状況を確認したいタスクを選択します。タスクを選択すると、下部のタブにタスクの情報が表示されます。[タスク情報] タブで [タスク状態の詳細] – [進捗状況（完了／対象）] を確認して、タスクが問題なく完了しているか確認します。

2.失敗したタスクの原因を確認して対処する

タスクの実行に失敗したコンピュータがある場合は、[タスク情報] タブの [失敗] のリンクをクリックしてください。[タスク状態] タブに移動して、タスクの実行に失敗したコンピュータの一覧が表示されます。

[タスク状態] のリンクをクリックすると、表示されるダイアログでタスク状態の詳細が確認できます。タスクが失敗した原因を確認して対処してください。

3.タスクを再実行する

タスクが失敗した原因を取り除いたら、タスクを再実行します。

タスクの設定を変えないで、すぐにタスクを再実行する場合

同じ設定でタスクをすぐに実行する場合は、タスクを再実行します。

タスクの設定を変えて再実行する場合

実行スケジュールや対象コンピュータを変更する場合は、タスクを編集またはコピーしてからタスクを実行します。

指定したコンピュータに対して、タスクが再実行されます。

関連リンク

- [15.7.1 イベント通知の設定をする手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.5 タスクを中止する手順](#)

1.13.2 ファイルを配布する流れ

各コンピュータに格納されている設定ファイルの更新や、インストール不要の自社ソフトウェアの展開などに伴って、組織内のコンピュータにファイルを配布する場合に配布機能を利用できます。

組織内のコンピュータにファイルを配布する流れを次に示します。

1.ファイルの配布計画を立てる

ファイルを配布する前に配布計画を立てます。また、配布計画は事前に利用者に通知しておきます。

2. コンピュータにファイルを配布する

ファイルを配布するには、配布するファイルを登録したパッケージと、パッケージを配布するタスクを作成します。タスクに指定したスケジュールに従って、パッケージが配布されます。

3. タスクの実行結果を確認する

タスクの実行状況を確認します。配布に失敗したコンピュータがある場合は、原因を確認して対処したあと、タスクを再実行します。

指定したすべてのコンピュータにファイルが配布されます。

関連リンク

- [1.13 ソフトウェアやファイルの配布](#)

(1) ファイルの配布計画を立てる

ファイルを配布する前に配布計画を立てます。また、配布計画は事前に利用者に通知しておきます。

1. ファイルの配布計画を立てる

ファイルの配布計画として、次のような項目を検討します。

- ファイルを配布するコンピュータ
- ファイルを配布する日時

ファイルを配布する日時は、ネットワークの負荷を考慮して検討してください。例えば、業務に支障がないように夜間に配布する、コンピュータの台数が多いので複数日に分けて配布するなどの計画を立てます。

なお、配布機能を実行するには事前に必要な準備があります。

ポイント

ファイルを配布する前に、テスト用のコンピュータを使用して、ファイルが正常に配布されるか確認することをお勧めします。

2. 利用者にファイルの配布計画を通知する

配布が計画どおりに実行されるように、また、配布に伴う問い合わせが発生しないように、ファイルの配布計画を事前にコンピュータの利用者に通知しておきます。例えば、次のような情報を通知します。

- ファイル名
- 配布先フォルダ
- 配布理由
- 配布日時
- 注意事項

コンピュータにファイルを配布するための準備が整います。

関連リンク

- [12.2 コンピュータにファイルを配布する手順](#)

(2) コンピュータにファイルを配布する手順

[ファイルを配布しましょう] ウィザードを使って、利用者のコンピュータにファイルを配布できます。

[ファイルを配布しましょう] ウィザードでは、配布するファイルを登録したパッケージと、パッケージの配布を実行するタスクを作成します。ウィザードを完了すると、タスクに指定したスケジュールに従って、パッケージが配布されます。

コンピュータにファイルを配布するには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [操作メニュー] から [ファイル配布ウィザードを起動する] を選択してウィザードを起動します。
4. [はじめに...] 画面でウィザードの流れを確認して、[次へ] ボタンをクリックします。
5. [ファイルを指定する] 画面で [新しいパッケージを作成する] を選択して、パッケージに登録するファイルを指定し、[次へ] ボタンをクリックします。
事前にパッケージを作成している場合は、作成済みのパッケージを選択することもできます。
6. [パッケージを設定する] 画面でパッケージ情報を設定して、[次へ] ボタンをクリックします。
7. [パッケージ配布タスクを作成する] 画面で、配布を実行するスケジュールなどを設定して、[次へ] ボタンをクリックします。
[対象のコンピュータでの動作] をクリックすると、パッケージ配布後にファイルを配布するタイミングや、利用者に通知するメッセージなどを設定できます。
8. [対象のコンピュータを選択する] 画面で、[変更] ボタンをクリックします。
9. [対象のコンピュータの変更] ダイアログで、ファイルを配布するコンピュータを指定して、[OK] ボタンをクリックします。
10. [次へ] ボタンをクリックします。
11. [設定内容を確認する] 画面で、設定内容を確認して [完了] ボタンをクリックします。
12. [完了!] 画面で、[閉じる] ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータにファイルが配布されます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク一覧] 画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でファイルの配布を延期できます。

関連リンク

- 12.6 利用者側でダウンロードやインストールを延期する
- 12.5.5 タスクを中止する手順

(3) タスクの実行結果を確認する流れ

配布（ITDM 互換）画面の「タスク」画面で、タスクの実行状況を確認できます。

タスク種別	タスク名	操作種別	タスク状態	開始日時	経過時間	失敗コンピ...	状況(%)	操作
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー
管理者が...	TestTask...	パッケージ...	予約中	-	-	0	0	編集 コピー

タスク情報の詳細		タスク状態の詳細	
タスク種別	管理者が実行するタスク	タスク状態	予約中
タスク名	TestTask0001	開始日時	(2099/12/31 00:00:00 実行予定)
説明		完了日時(経過時間)	-
操作種別	パッケージ配布	進捗状況(完了/対象)	0%(0/10,000 台)
実行スケジュール	2099/12/31 00:00:00	失敗	0%(0 台)
対象のコンピュータでの動作		成功	0%(0 台)
実行タイミング	すぐに実行	キャンセル	0%(0 台)
自動起動	しない	実行中	100%(10,000 台)
上書き禁止	しない		
実行前メッセージの表示	しない		
実行後メッセージの表示	しない		

タスクの実行状況は、完了するまで定期的に確認することをお勧めします。タスクの実行に失敗したコンピュータがある場合は、タスクが失敗した原因を確認して対処したあと、タスクを再実行してください。

ポイント

配布管理のイベント（タスク完了、タスク失敗など）が発生したときに自動的にメールで通知するように設定できます。

1.タスクの実行状況を確認する

配布（ITDM 互換）画面の［タスク］画面で、実行状況を確認したいタスクを選択します。タスクを選択すると、下部のタブにタスクの情報が表示されます。［タスク情報］タブで［タスク状態の詳細］－［進捗状況（完了／対象）］を確認して、タスクが問題なく完了しているか確認します。

2.失敗したタスクの原因を確認して対処する

タスクの実行に失敗したコンピュータがある場合は、［タスク情報］タブの［失敗］のリンクをクリックしてください。［タスク状態］タブに移動して、タスクの実行に失敗したコンピュータの一覧が表示されます。

［タスク状態］のリンクをクリックすると、表示されるダイアログでタスク状態の詳細が確認できます。タスクが失敗した原因を確認して対処してください。

3.タスクを再実行する

タスクが失敗した原因を取り除いたら、タスクを再実行します。

タスクの設定を変えないで、すぐにタスクを再実行する場合

同じ設定でタスクをすぐに実行する場合は、タスクを再実行します。

タスクの設定を変えて再実行する場合

実行スケジュールや対象コンピュータを変更する場合は、タスクを編集またはコピーしてからタスクを実行します。

指定したコンピュータに対して、タスクが再実行されます。

関連リンク

- [15.7.1 イベント通知の設定をする手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.5 タスクを中止する手順](#)

1.13.3 ソフトウェアをアンインストールする流れ

業務に不要なソフトウェアや、使用を禁止しているソフトウェアがインストールされていた場合、組織内のコンピュータからソフトウェアをアンインストールするときに配布機能を利用できます。

組織内のコンピュータからソフトウェアをアンインストールする流れを次に示します。

1.アンインストールが必要なソフトウェアのインストール状況を調査する

業務に不要なソフトウェアや使用を禁止しているソフトウェアなど、アンインストールが必要なソフトウェアのインストール状況を調査します。

2.ソフトウェアのアンインストール計画を立てる

ソフトウェアをアンインストールする前に計画を立てます。また、アンインストール計画は事前に利用者に通知しておきます。

3.コンピュータからソフトウェアをアンインストールする

ソフトウェアをアンインストールするには、ソフトウェアをアンインストールするタスクを作成します。タスクに指定したスケジュールに従って、アンインストールが実行されます。

4.タスクの実行結果を確認する

アンインストールの実行状況を確認します。アンインストールに失敗したコンピュータがある場合は、原因を確認して対処したあと、タスクを再実行します。

指定したすべてのコンピュータからソフトウェアがアンインストールされます。

関連リンク

- 1.13 ソフトウェアやファイルの配布

(1) アンインストールが必要なソフトウェアのインストール状況を調査する

業務に不要なソフトウェアや使用を禁止しているソフトウェアなど、アンインストールが必要なソフトウェアのインストール状況を調査します。

ソフトウェアのインストール状況は、機器画面の[ソフトウェア情報]画面で確認できます。ソフトウェアを選択すると、下部の[インストール済みコンピュータ]タブでソフトウェアをインストールしているコンピュータを確認できます。

The screenshot displays the 'IT Desktop Management 2' application. The main window is divided into two panes. The top pane, titled 'ソフトウェア情報 - ソフトウェア一覧: 25', shows a list of installed software. The bottom pane, titled 'ソフトウェア情報 - インストール済みコンピュータ', shows a list of computers where the software is installed.

ソフトウェア名	バージョン	メーカー	購入形態	プロダクト	インストール日時	確認状態	必須ソ...	禁止ソ...	管...
JP1/D...	1.0.0	Hitachi	0	2012/06/21 17:36:17	-	未確認	✓		
JP1/IT...	09.5.0...	Hitachi...	0	2012/06/21 14:13:22	-	未確認	✓		
JP1/IT...	09.5.1...	Hitachi...	10000	2012/06/21 15:17:18	-	未確認	✓		
JP1/IT...	09.5.1...	Hitachi...	0	2012/06/21 16:57:42	-	未確認	✓		
JP1/IT...	10.0.0...	Hitachi...	0	2012/11/30 13:12:12	-	未確認	✓		
JP1/IT...	10.0.0...	Hitachi...	0	2012/12/04 12:18:09	-	未確認	✓		
JP1/IT...	10.0.1...	Hitachi...	0	2012/11/30 15:18:58	-	未確認	✓		
JP1/IT...	10.1.0...	Hitachi...	0	2014/06/27 11:32:45	-	未確認	✓		
JP1/IT...	09.5.1...	Hitachi...	10000	2012/06/21 15:17:18	-	未確認	✓		
JP1/IT...	09.5.0...	Hitachi...	0	2012/06/21 14:13:22	-	未確認	✓		
JP1/IT...	10.0.0...	Hitachi...	0	2012/12/04 12:01:50	-	未確認	✓		
JP1/IT...	09.5.1...	Hitachi...	0	2012/11/30 15:18:58	-	未確認	✓		

機器種別	管...	接...	機...	ホスト名	メーカー	IP アドレス	OS	利用者名	登録日時	インストール日
PC				Sim10...	Panas...	192.168.101.101	Micros...		2014/07/18 22:37:58	2012/03/30
PC				Sim10...	Panas...	192.168.101.102	Micros...		2014/07/18 22:37:57	2012/03/30
PC				Sim10...	Panas...	192.168.101.103	Micros...		2014/07/18 22:37:35	2012/03/30
PC				Sim10...	Panas...	192.168.101.104	Micros...		2014/07/18 22:49:31	2012/03/30
PC				Sim10...	Panas...	192.168.101.105	Micros...		2014/07/18 22:37:36	2012/03/30
PC				Sim10...	Panas...	192.168.101.106	Micros...		2014/07/18 22:37:51	2012/03/30
PC				Sim10...	Panas...	192.168.101.107	Micros...		2014/07/18 22:37:51	2012/03/30
PC				Sim10...	Panas...	192.168.101.108	Micros...		2014/07/18 22:37:43	2012/03/30
PC				Sim10...	Panas...	192.168.101.109	Micros...		2014/07/18 23:20:29	2012/03/30
PC				Sim10...	Panas...	192.168.101.110	Micros...		2014/07/18 22:37:51	2012/03/30
PC				Sim10...	Panas...	192.168.101.111	Micros...		2014/07/18 23:11:52	2012/03/30

業務に不要なソフトウェアがインストールされていないか確認する場合は、ソフトウェアの一覧を調査してください。使用を禁止しているソフトウェアがインストールされていないか確認する場合は、[ソフトウェア情報] 画面の一覧の [禁止ソフトウェア] 欄にチェックが付いているソフトウェアを確認してください。

ポイント

[インストール済みコンピュータ] タブで、表示されているコンピュータからソフトウェアをアンインストールすることもできます。

ポイント

使用禁止ソフトウェアは、セキュリティポリシーを適用したコンピュータにインストールされていた場合に自動的にアンインストールするように自動対策を設定できます。

業務に不要なソフトウェアや使用を禁止しているソフトウェアをインストールしているコンピュータを発見した場合は、利用者に使用状況や使用目的を確認して、必要に応じてアンインストールします。

関連リンク

- [1.7.1 セキュリティポリシーを設定する](#)

(2) ソフトウェアのアンインストール計画を立てる流れ

ソフトウェアをアンインストールする前に計画を立てます。また、アンインストール配布計画は事前に利用者に通知しておきます。

1. ソフトウェアのアンインストール計画を立てる

アンインストール計画として、次のような項目を検討します。

- ソフトウェアをアンインストールするコンピュータ
- ソフトウェアをアンインストールする日時

ソフトウェアをアンインストールする日時は、業務への影響を考慮して検討してください。例えば、業務に支障がないように夜間にアンインストールする、コンピュータの台数が多いので複数日に分けてアンインストールするなどの計画を立てます。

なお、配布機能を実行するには事前に必要な準備があります。

ポイント

アンインストールを実行する前に、テスト用のコンピュータを使用して、ソフトウェアが正常にアンインストールされるか確認することをお勧めします。

2.利用者にソフトウェアのアンインストール計画を通知する

アンインストールが計画どおりに実行されるように、また、アンインストールに伴う問い合わせが発生しないように、アンインストール計画を事前にコンピュータの利用者に通知しておきます。例えば、次のような情報を通知します。

- ソフトウェア名
- バージョン
- アンインストール理由
- アンインストール日時
- 注意事項

コンピュータからソフトウェアをアンインストールするための準備が整います。

関連リンク

- [12.3 コンピュータからソフトウェアをアンインストールする手順](#)

(3) コンピュータからソフトウェアをアンインストールする手順

[ソフトウェアをアンインストールしましょう] ウィザードを使って、利用者のコンピュータからソフトウェアをアンインストールできます。

[ソフトウェアをアンインストールしましょう] ウィザードでは、ソフトウェアをアンインストールするためのタスクを作成します。ウィザードを完了すると、指定したスケジュールに従って、アンインストールタスクが実行されます。

コンピュータからソフトウェアをアンインストールするには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [操作メニュー] から [アンインストールウィザードを起動する] を選択してウィザードを起動します。
4. [はじめに...] 画面でウィザードの流れを確認して、[次へ] ボタンをクリックします。
5. [アンインストールタスクを作成する] 画面で、アンインストールするソフトウェアの情報や、タスクを実行するスケジュールなどを設定して、[次へ] ボタンをクリックします。
[対象のコンピュータでの動作] をクリックすると、アンインストールを実行するタイミングや、利用者に通知するメッセージなどを設定できます。
この画面で設定したソフトウェア名およびバージョンに完全一致するソフトウェアだけがアンインストールされます。
6. [対象のコンピュータを選択する] 画面で、[変更] ボタンをクリックします。

7. [対象のコンピュータの変更] ダイアログで、ソフトウェアをアンインストールするコンピュータを指定して、[OK] ボタンをクリックします。
8. [次へ] ボタンをクリックします。
9. [設定内容を確認する] 画面で、設定内容を確認して [完了] ボタンをクリックします。
10. [完了!] 画面で、[閉じる] ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータからソフトウェアがアンインストールされます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク一覧] 画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でソフトウェアのアンインストールを延期できます。詳細については、「[12.6 利用者側でダウンロードやインストールを延期する](#)」を参照してください。

関連リンク

- [12.5.5 タスクを中止する手順](#)

(4) タスクの実行結果を確認する流れ

配布 (ITDM 互換) 画面の [タスク] 画面で、タスクの実行状況を確認できます。

The screenshot shows the 'IT Desktop Management 2' application. The main window is titled 'タスク一覧' (Task List). It features a table with the following columns: 'タスク種別' (Task Type), 'タスク名' (Task Name), '操作種別' (Operation Type), 'タスク状態' (Task Status), '開始日時' (Start Date/Time), '経過時間' (Elapsed Time), '失敗コン...' (Failure Count), and '状況(%)' (Status (%)). The table lists several tasks, all with a status of '予約中' (Reserved). Below the table, there are tabs for 'タスク情報' (Task Information), 'タスク状態' (Task Status), 'パッケージ情報' (Package Information), and 'ノート' (Note). The 'タスク情報' tab is selected, showing details for 'TestTask0001'. The details are organized into two sections: 'タスク情報の詳細' (Task Information Details) and 'タスク状態の詳細' (Task Status Details). The 'タスク情報の詳細' section includes fields for 'タスク種別' (管理者が実行するタスク), 'タスク名' (TestTask0001), '説明' (説明), '操作種別' (パッケージ配布), '実行スケジュール' (2099/12/31 00:00:00), '対象のコンピュータでの動作' (実行タイミング: すぐに実行, 自動起動: しない, 上書き禁止: しない, 実行前メッセージの表示: しない, 実行後メッセージの表示: しない). The 'タスク状態の詳細' section includes fields for 'タスク状態' (予約中), '開始日時' (2099/12/31 00:00:00 実行予定), '完了日時(経過時間)' (-), '進捗状況(完了/対象)' (0%(0/10,000 台)), '失敗' (0%(0 台)), '成功' (0%(0 台)), 'キャンセル' (0%(0 台)), and '実行中' (100%(10,000 台)).

タスクの実行状況は、完了するまで定期的を確認することをお勧めします。タスクの実行に失敗したコンピュータがある場合は、タスクが失敗した原因を確認して対処したあと、タスクを再実行してください。

ポイント

配布管理のイベント（タスク完了、タスク失敗など）が発生したときに自動的にメールで通知するように設定できます。

1. タスクの実行状況を確認する

配布（ITDM 互換）画面の [タスク] 画面で、実行状況を確認したいタスクを選択します。タスクを選択すると、下部のタブにタスクの情報が表示されます。[タスク情報] タブで [タスク状態の詳細] - [進捗状況（完了／対象）] を確認して、タスクが問題なく完了しているか確認します。

2. 失敗したタスクの原因を確認して対処する

タスクの実行に失敗したコンピュータがある場合は、[タスク情報] タブの [失敗] のリンクをクリックしてください。[タスク状態] タブに移動して、タスクの実行に失敗したコンピュータの一覧が表示されます。

[タスク状態] のリンクをクリックすると、表示されるダイアログでタスク状態の詳細が確認できます。タスクが失敗した原因を確認して対処してください。

3. タスクを再実行する

タスクが失敗した原因を取り除いたら、タスクを再実行します。

タスクの設定を変えないで、すぐにタスクを再実行する場合

同じ設定でタスクをすぐに実行する場合は、タスクを再実行します。

タスクの設定を変えて再実行する場合

実行スケジュールや対象コンピュータを変更する場合は、タスクを編集またはコピーしてからタスクを実行します。

指定したコンピュータに対して、タスクが再実行されます。

関連リンク

- [15.7.1 イベント通知の設定をする手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.5 タスクを中止する手順](#)

1.14 職制変更に伴い部署の定義を変更する流れ

期首や年度の始めに組織の職制変更を実施する場合、JP1/IT Desktop Management 2 の部署の定義も合わせて変更する必要があります。

職制変更に伴い部署の定義を変更する流れを次に示します。

1.新体制の部署の規定を検討する

職制変更前に、新体制の部署に割り当てるセキュリティポリシーやエージェント設定などを検討します。

2.部署の定義を新体制に合わせて変更する

`ioassetsfieldutil export` コマンドと `ioassetsfieldutil import` コマンドを利用して、部署の定義を変更します。また、新体制の部署にセキュリティポリシーやエージェント設定などを割り当てます。

3.資産情報を新体制に合わせて更新する

移行期間に、[利用者情報の入力] ダイアログで利用者に部署を選択してもらいます。また、旧体制だけで使われていた部署に関連づいている資産情報を、部門管理者が新体制に合わせて更新します。

4.旧体制だけで使われていた情報を削除する

資産情報の更新が完了したら、旧体制だけで使われていた部署の階層は不要になるため削除します。また、旧体制だけで使われていた部署の階層を部門管理者の管轄範囲に設定している場合は、管轄範囲から削除します。

1.14.1 新体制の部署の規定を検討する

職制変更前に、新体制の部署の規定を検討する必要があります。規定する項目は次のとおりです。

- 新体制の部署に割り当てるセキュリティポリシー
- 新体制の部署に割り当てるエージェント設定
- 新体制の部署の部門管理者
- 旧体制の部署から次の資産情報の関連づけを移行する、新体制の部署
 - ハードウェア資産情報
 - ソフトウェアライセンス情報
 - 契約情報

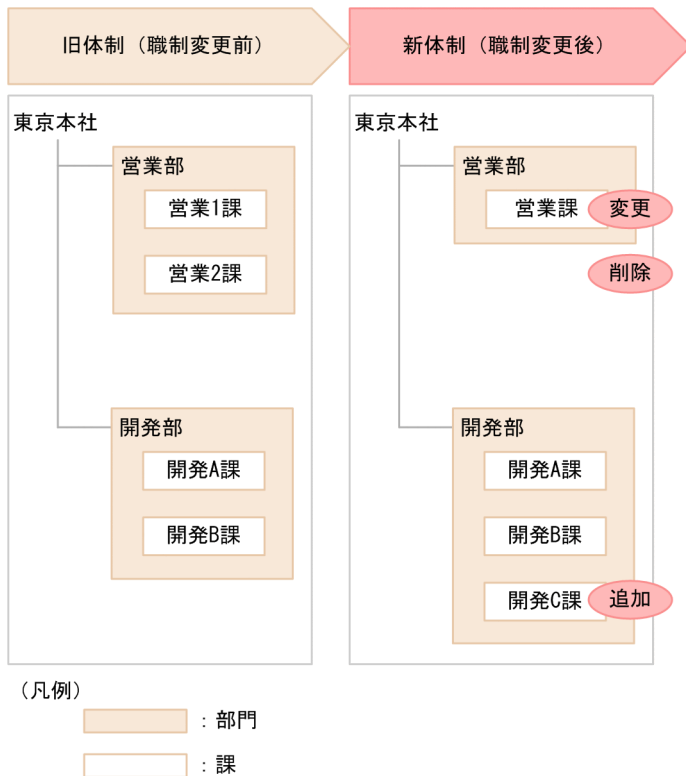
関連リンク

- [1.7.1 セキュリティポリシーを設定する](#)
- [15.1.1 エージェント設定の管理](#)
- [1.3.1 ユーザーアカウントの設定内容を検討する流れ](#)

1.14.2 部署の定義を新体制に合わせて変更する流れ

部署の定義を新体制に合わせて変更するには、`ioassetsfieldutil export` コマンドと `ioassetsfieldutil import` コマンドを利用して、部署の定義を編集したあと、新体制の部署にセキュリティポリシーやエージェント設定を割り当てます。

ここでは、次の図のとおり職制変更する場合を例に説明します。



例では、4月1日の職制変更に伴い、「営業1課」から「営業課」への名称変更、「営業2課」の削除、および「開発C課」の追加を、部署の定義に反映します。

部署の定義を新体制に合わせて変更する流れを次に示します。

1. 部署の定義を変更する期間と、資産情報の移行期間を決める

部署の定義を変更したあとには、資産情報を新体制に合わせて移行する必要があります。部署の定義を変更する期間と資産情報を移行する期間を、それぞれ設定します。期間の設定例を次に示します。

- 部署の定義の変更期間：3月15日～3月31日
- 資産情報の移行期間：4月1日～4月15日

職制変更日は4月1日ですが、移行期間は資産情報に旧体制の部署が混在するため、JP1/IT Desktop Management 2で部署が実態どおりに表示されるのは、4月16日からになります。

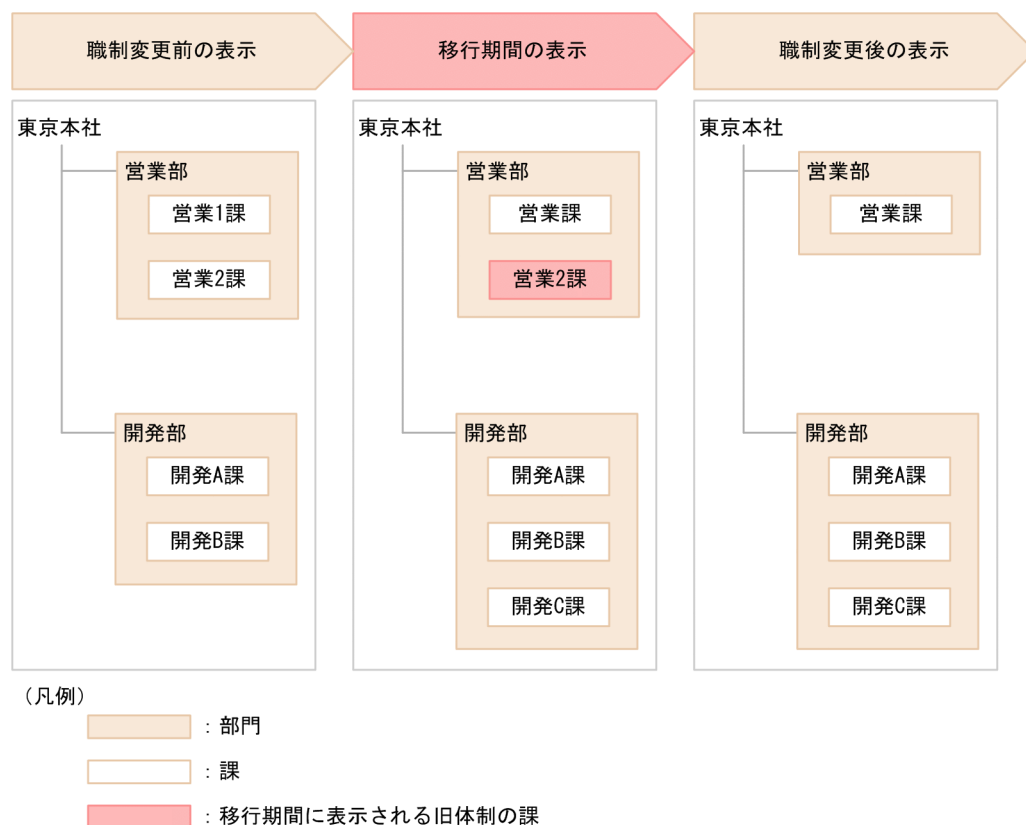
2. システム管理者および部門管理者に、JP1/IT Desktop Management 2 を利用する上での制限事項を連絡する

部署の定義、および資産画面や機器画面のメニューエリアに表示される部署の階層を、職制変更日を経過するまで更新してはならないことをシステム管理者に連絡します。

また、メニューエリアが次のように表示されることを、システム管理者と部門管理者に連絡します。

- 部署の定義の変更期間：現在の部署と混在して、新体制の部署が表示される
- 資産情報の移行期間：新体制の部署と混在して、旧体制の部署が表示される

移行期間のメニューエリアの表示状態を、次の図に示します。



3. 部署の定義を CSV 形式でエクスポートする

`ioassetsfieldutil export` コマンドを利用して、部署の定義を CSV 形式でエクスポートします。

4. エクスポートした CSV ファイルを編集する

次のとおり部署の定義を編集します。

- 「営業 1 課」を「営業課」に名称変更
- 「営業 2 課」を削除
- 「開発 C 課」を追加

5. データベースをバックアップする

手順 7.での CSV ファイルのインポートに失敗したときのために、データベースマネージャでデータベースをバックアップします。

6. 利用者情報の入力開始日時を指定する

設定画面の [資産管理] - [資産管理項目の設定] 画面で、利用者情報の入力開始日時に職制変更日を指定します。例の場合は、4月1日を指定します。

7. CSV ファイルをインポートする

`ioassetsfieldutil import` コマンドを利用して、JP1/IT Desktop Management 2 に部署の定義をインポートします。

インポートに失敗した場合は、手順 5. でバックアップしたデータベースを、データベースマネージャでリストアしてください。

8. 新体制の部署に、セキュリティポリシーとエージェント設定を割り当てる

規定どおりのセキュリティポリシーとエージェント設定を、新体制の部署に割り当てます。

割り当てが完了したら、オフライン管理用のエージェント設定のインストールセットを作成できます。

9. 部門管理者の管轄範囲に、新体制の部署を追加する

設定画面の [ユーザーアカウントの管理] 画面で、部門管理者の管轄範囲に新体制の部署を追加します。

部署の定義が、新体制のとおりに変更されます。

関連リンク

- [17.30 ioassetsfieldutil export](#) (共通管理項目と追加管理項目の定義のエクスポート)
- [付録 A.5 共通管理項目と追加管理項目の定義のインポートファイルの設定項目](#)
- [16.2 データベースをバックアップする](#)
- [17.31 ioassetsfieldutil import](#) (共通管理項目と追加管理項目の定義のインポート)
- [16.3 データベースをリストアする](#)
- [9.3.5 セキュリティポリシーを割り当てる手順](#)
- [15.1.6 エージェント設定を割り当てる手順](#)
- [4.7 管轄範囲を追加する手順](#)

1.14.3 資産情報を新体制に合わせて更新する

部署の定義の変更が完了したら、移行期間に、[利用者情報の入力] ダイアログで利用者に部署を選択してもらいます。

また、部門管理者が旧体制だけで使われていた部署に関連づいている資産情報を、新体制に合わせて更新します。更新する資産情報は、次のとおりです。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 契約情報

関連リンク

- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [11.2.5 ソフトウェアライセンス情報を編集する手順](#)
- [11.3.2 契約情報を編集する手順](#)
- [11.4 資産情報をインポートする](#)
- [11.5 資産情報をエクスポートする手順](#)

1.14.4 旧体制だけで使われていた情報を削除する流れ

資産情報の更新が完了したら、旧体制だけで使われていた部署の階層は不要になるため削除します。また、旧体制だけで使われていた部署の階層を部門管理者の管轄範囲に設定している場合は、管轄範囲から削除します。これらの旧体制だけで使われていた情報を削除する流れを次に示します。

1.定義から削除した旧体制の部署を、部門管理者の管轄範囲から削除する

定義から削除した旧体制の部署を部門管理者の管轄範囲に設定している場合は、設定画面の[ユーザー管理] – [ユーザーアカウントの管理] 画面で、管轄範囲から削除します。

2.定義から削除した旧体制の部署の階層を削除する

資産画面と機器画面のメニューエリアから表示できる[旧体制で使われていた階層の削除] ダイアログで、定義から削除した旧体制の部署の階層を一括で削除します。旧体制の部署の階層を削除することで、部署の定義の階層とメニューエリアに表示される階層が一致します。

なお、資産情報が割り当たっている状態で部署の階層を削除すると、割り当たっている資産情報の部署が「不明」に変更されます。

注意事項

削除した部署に割り当てていたセキュリティポリシーと「不明」に割り当てているセキュリティポリシーが異なる場合、機器には「不明」に割り当てられているセキュリティポリシーが適用されます。セキュリティポリシーの割り当てを変更したくない場合は、必ず新体制の部署に移行してから旧体制の部署を削除してください。

旧体制だけで使われていた情報の削除が完了します。

関連リンク

- [4.8 管轄範囲を削除する手順](#)
- [6.31 旧体制で使われていた階層だけを削除する手順](#)

2

製品ライセンスを登録する

ここでは、製品ライセンスを登録する方法について説明します。

2.1 製品ライセンスを登録する手順

製品ライセンスを JP1/IT Desktop Management 2 に登録することで、登録したライセンス数分だけ機器を管理できるようになります。

製品ライセンスを登録するには：

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 [ライセンスを登録] ボタンをクリックします。
4. 表示されたダイアログでライセンスキーファイルを選択して、[開く] ボタンをクリックします。

ライセンス登録が完了します。

ポイント

初回登録時以外は、設定画面の [製品ライセンス] — [製品ライセンスの設定] 画面でもライセンスを登録できます。[ライセンスを登録] ボタンをクリックしてください。表示されたダイアログでライセンスキーファイルを選択して、[開く] ボタンをクリックすると、ライセンス登録が完了します。

ポイント

初回登録時以外は、画面左上の [ヘルプ] — [製品ライセンス情報] から表示される [製品ライセンス情報] ダイアログでもライセンスを登録できます。[ライセンスを登録] ボタンをクリックしてください。表示されたダイアログでライセンスキーファイルを選択して、[開く] ボタンをクリックすると、ライセンス登録が完了します。

関連リンク

- [2.3 製品ライセンスを追加する手順](#)

2.2 製品ライセンスの情報を確認する方法

登録済みの製品ライセンスの情報は、次の3種類の方法で確認できます。

- ログイン画面で [ライセンス] ボタンをクリックして [製品ライセンス情報] ダイアログを表示する。
- 設定画面の [製品ライセンス] – [製品ライセンスの設定] 画面を表示する。
- 画面左上の [ヘルプ] – [製品ライセンス情報] を選択して、[製品ライセンス情報] ダイアログを表示する。

製品ライセンスが不足している場合は、製品ライセンスを追加購入してください。購入した製品ライセンスを登録するには、上記の方法で表示したダイアログまたは画面から [ライセンスを登録] ボタンをクリックして、表示されるダイアログでライセンスキーファイルを選択してください。

2.3 製品ライセンスを追加する手順

組織内の機器を JP1/IT Desktop Management 2 で管理するためには、製品ライセンスが必要です。

製品ライセンスが不足した場合は、製品ライセンスを追加購入してください。購入した製品ライセンスを登録することで、ライセンスを追加できます。

3

操作画面にログインする

ここでは、JP1/IT Desktop Management 2 の操作画面にログインする方法について説明します。

3.1 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 JP1/IT Desktop Management 2 にログインできます。

初めてログインする場合は、JP1/IT Desktop Management 2 のライセンスを登録する必要があります。ライセンスを登録するには、[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
※/jplitdm/

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

- [4.9 ユーザーアカウントのロックを解除する手順](#)

3.2 ユーザーアカウントの情報を設定する手順

JP1/IT Desktop Management 2 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、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。

3.3 デフォルトパスワードを変更する手順

JP1/IT Desktop Management 2 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。

3.4 ログアウトする手順

JP1/IT Desktop Management 2 の操作を終了する場合は、操作画面からログアウトします。

ログアウトするには：

1. 画面上部にある［ログアウト］ 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。

操作画面からログアウトされ、ログイン画面が表示されます。

ポイント

画面上部の［システム］メニューから［ログアウト］を選択してログアウトすることもできます。

4

ユーザーアカウントを管理する

ここでは、ユーザーアカウントを管理する方法について説明します。

4.1 ユーザーアカウントを追加する手順

設定画面の [ユーザー管理] – [ユーザーアカウントの管理] 画面で、ユーザーアカウントを追加できます。付与する権限によって、利用できる機能が異なります。適切な権限を付与してください。

なお、ユーザーアカウントを追加するには、ユーザーアカウント管理権限が必要です。

ユーザーアカウントを追加するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] – [ユーザーアカウントの管理] を選択します。
3. インフォメーションエリアで [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ユーザーアカウントの情報を入力して、[OK] ボタンをクリックします。

ユーザーアカウントが追加され、ユーザーアカウントの一覧に表示されます。

関連リンク

- [4.2 ユーザーアカウントを編集する手順](#)
- [4.3 ユーザーアカウントを削除する手順](#)

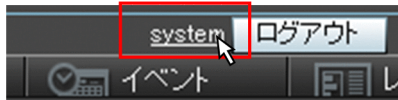
4.2 ユーザーアカウントを編集する手順

パスワードを変更したい場合や、権限を変更したい場合にユーザーアカウントを編集できます。

割り当てられている権限によって、編集できるユーザーアカウントの範囲が異なります。ユーザーアカウント管理権限が付与されていない場合は、自分のユーザーアカウントだけ編集できます。ユーザーアカウント管理権限が付与されている場合は、すべてのユーザーアカウントを編集できます。

自分のユーザーアカウントを編集するには：

1. 操作画面で画面上部に表示される [ユーザーアカウント名] のリンクをクリックします。



2. 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して、[OK] ボタンをクリックします。

自分のユーザーアカウントが更新されます。

ほかの管理者のユーザーアカウントを編集するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] - [ユーザーアカウントの管理] 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アカウントの [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ユーザーアカウントの情報を編集して、[OK] ボタンをクリックします。

選択したユーザーアカウントが更新されます。

ポイント

ユーザーアカウントがロックされてしまった管理者がいる場合は、[ユーザーアカウントの編集] ダイアログで、アカウントのロックを解除してください。

関連リンク

- [4.1 ユーザーアカウントを追加する手順](#)
- [4.3 ユーザーアカウントを削除する手順](#)

4.3 ユーザーアカウントを削除する手順

利用しなくなったユーザーアカウントを削除できます。なお、「ビルトインアカウント」と自分のユーザーアカウントは削除できません。ユーザーアカウントを削除するには、ユーザーアカウント管理権限が必要です。

ユーザーアカウントを削除するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] – [ユーザーアカウントの管理] を選択します。
3. インフォメーションエリアで削除したいユーザーアカウントを選択して、[削除] ボタンをクリックします。
複数のユーザーアカウントを選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したユーザーアカウントが削除されます。

関連リンク

- [4.1 ユーザーアカウントを追加する手順](#)
- [4.2 ユーザーアカウントを編集する手順](#)

4.4 自分のパスワードを変更する手順

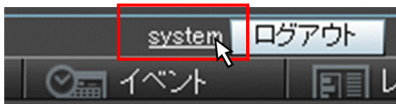
ユーザーアカウントのパスワードは、セキュリティ対策として定期的に変更することをお勧めします。

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。

自分のパスワードを変更するには：

1. 操作画面で画面上部に表示される［ユーザーアカウント名］のリンクをクリックします。



2. 表示されるダイアログで、［パスワードを変更］ボタンをクリックします。
3. 表示されるダイアログでパスワードを変更して、［OK］ボタンをクリックします。
4. ［OK］ボタンをクリックします。

自分のユーザーアカウントのパスワードが更新されます。

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

関連リンク

- [4.5 ほかの管理者のパスワードを変更する手順](#)
- [4.6 パスワードを初期化する手順](#)

4.5 ほかの管理者のパスワードを変更する手順

ユーザーアカウントのパスワードは、セキュリティ対策として定期的に変更することをお勧めします。

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。

割り当てられている権限によって、変更できるパスワードの範囲が異なります。ユーザーアカウント管理権限が付与されていない場合は、自分のパスワードだけ変更できます。ユーザーアカウント管理権限が付与されている場合は、すべてのユーザーアカウントのパスワードを変更できます。

ほかの管理者のパスワードを変更するには：

1. 設定画面を表示します。
2. メニューエリアで［ユーザー管理］－［ユーザーアカウントの管理］を選択します。
3. インフォメーションエリアでパスワードを変更したいユーザーアカウントの［編集］ボタンをクリックします。
4. 表示されるダイアログでパスワードを変更して、[OK] ボタンをクリックします。

選択したユーザーアカウントのパスワードが更新されます。

ほかの管理者のパスワードを変更した場合、パスワードが初期化されたと見なされます。この場合、変更後のパスワードでログインした管理者は、ログイン後にパスワードの変更が要求されます。

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

関連リンク

- 4.4 自分のパスワードを変更する手順
- 4.6 パスワードを初期化する手順

4.6 パスワードを初期化する手順

管理者がパスワードを忘れた場合に、ほかの管理者がパスワードを変更することで、パスワードを初期化できます。

パスワードの初期化には、ユーザーアカウント管理権限が必要です。

パスワードを初期化するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] – [ユーザーアカウントの管理] を選択します。
3. インフォメーションエリアでパスワードを初期化したいユーザーアカウントの [編集] ボタンをクリックします。
4. 表示されるダイアログでパスワードを入力して、[OK] ボタンをクリックします。
選択したユーザーアカウントにパスワードが設定されます。
5. パスワードを初期化された管理者に、設定したパスワードを連絡します。
初期化したパスワードで JP1/IT Desktop Management 2 にログインしたあとに、パスワードの変更が必要であることも連絡します。

パスワードを初期化された管理者は、連絡されたパスワードで JP1/IT Desktop Management 2 にログインします。ログイン後、パスワードの変更が要求されます。

関連リンク

- [4.4 自分のパスワードを変更する手順](#)

4.7 管轄範囲を追加する手順

ユーザーアカウントに、管轄範囲を追加できます。管轄範囲を追加すると、管轄範囲に限定した機器、ハードウェア資産などを管理できます。管轄範囲を付与する権限によって、利用できる機能が異なります。適切な権限を付与してください。

なお、管轄範囲を追加するには、ユーザーアカウント管理権限が必要です。

管轄範囲を追加するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] – [ユーザーアカウントの管理] を選択します。
3. インフォメーションエリアで [追加] ボタンまたは [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 [このユーザーアカウントの管轄情報を設定する] をチェックします。
5. [管轄範囲] の [追加] ボタンをクリックします。

表示されるダイアログで追加したい管轄範囲を選択して、[OK] ボタンをクリックします。

ユーザーアカウントの管轄範囲が追加されます。

関連リンク

- [4.8 管轄範囲を削除する手順](#)

4.8 管轄範囲を削除する手順

ユーザーアカウントから、管轄範囲を削除できます。

なお、管轄範囲を削除するには、ユーザーアカウント管理権限が必要です。

管轄範囲を削除するには：

1. 設定画面を表示します。
2. メニューエリアで [ユーザー管理] – [ユーザーアカウントの管理] を選択します。
3. インフォメーションエリアで [編集] ボタンをクリックします。
4. 表示されるダイアログの [管轄範囲] で削除したい管轄範囲を選択し、[削除] ボタンをクリックします。
5. [OK] ボタンをクリックします。

ユーザーアカウントの管轄範囲が削除されます。

関連リンク

- [4.7 管轄範囲を追加する手順](#)

4.9 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。

5

操作画面を利用する

ここでは、JP1/IT Desktop Management 2 の操作画面での共通操作について説明します。

5.1 表示されるパネルとレイアウトを設定する手順

ホーム画面または各画面の [サマリ] – [ダッシュボード] 画面に表示されるパネルの種類と、パネルのレイアウトを変更できます。

表示されるパネルとレイアウトを設定するには：

1. ホーム画面または各画面を表示します。
2. 画面左上の [表示] メニューの [パネルのレイアウト設定] を選択します。
3. 表示されるダイアログで、表示したいパネルとレイアウトを選択します。
4. [OK] ボタンをクリックします。

設定した内容に従って、画面に表示されるパネルとレイアウトが変更されます。

ポイント

表示をデフォルトに戻す場合は、[表示] メニューの [表示設定の初期化] を選択してください。

5.2 表示中の画面の情報を更新する手順

画面中の更新アイコン（）をクリックすると、表示中の画面の情報やパネルの情報を更新できます。画面表示は定期的に更新されますが、任意のタイミングで最新情報を確認したい場合は、画面表示を手動で更新してください。

更新アイコンは、画面上部のボタンやメニューエリア、インフォメーションエリアの見出しに表示されます。



また、各画面に表示されるパネルのタイトルバーにも表示されます。



ポイント

パネルを自動で更新するように設定する場合、各パネルのメニュー（）から「表示の更新間隔を設定する」を選択して表示されるダイアログで、表示更新の間隔を指定できます。指定した表示間隔は、すべてのパネルに適用することもできます。

5.3 一覧の表示項目を変更する手順

インフォメーションエリアに表示する管理項目を変更できます。

運用上、よく確認する管理項目を表示することをお勧めします。

表示項目を変更するには：

1. 表示項目を変更するインフォメーションエリアを表示します。
2. 一覧の項目名を右クリックして「表示項目の選択」を選択します。



3. 表示されるダイアログで、一覧に表示する管理項目をチェックします。

4. [OK] ボタンをクリックします。

インフォメーションエリアに表示する管理項目が変更されます。

ポイント

表示項目をデフォルトに戻す場合は、一覧の項目名を右クリックして「ユーザー操作状態を初期値に戻す」を選択してください。

ポイント

資産画面では、インフォメーションエリアに表示する管理項目を任意に作成できます。管理項目を作成するには、設定画面の「資産管理」－「資産管理項目の設定」画面で管理項目を追加してください。

関連リンク

- [15.4.1 資産管理項目を追加する手順](#)

5.4 各画面での共通操作

JP1/IT Desktop Management 2 の各画面で共通する操作について説明します。

履歴に沿って画面を移動する

操作画面の上部に表示される  をクリックすると、参照した履歴に沿って操作画面を移動できます。このボタンは、[表示] メニューー [オプション] から表示/非表示を設定できます。

画面の情報を更新する

表示中の画面の情報やパネルに表示されている情報を更新できます。

一覧の表示項目を変更する

インフォメーションエリアに表示する管理項目を変更できます。

フィルタを利用して一覧の情報を絞り込む

フィルタを利用すると、条件を指定して一覧に表示される情報を絞り込めます。

一覧の項目を複数選択する

インフォメーションエリアの一覧に表示されている情報を複数選択できます。

一覧の項目名の左端にあるチェックボックスをクリックすると、全選択できます。一覧の左端に表示されているチェックボックスをクリック、または [Ctrl] キーを押しながらクリックして個別に複数選択できます。また、項目を選択してから、別の項目を [Shift] キーを押しながらクリックすると一括選択できます。キーを押しながらの操作は、チェックボックス以外の場所をクリックしてください。

複数選択した状態で、[Ctrl] キーを押しながら選択行をクリック、または選択行のチェックボックスをクリックすると、個別に選択を解除できます。

右クリックで表示されるメニューを利用する

画面上を右クリックすると、そのときに実行できるさまざまな操作が表示されます。

例えば、メニューエリアに表示されるグループを右クリックすると、インフォメーションエリアに新しいタブを表示できます。そのほかにも、グループ、フィルタ、カスタムグループなどを編集したり、表示されている情報を更新したりできます。

また、インフォメーションエリアの一覧を右クリックすると、表示されているボタンや [操作メニュー] と同等の操作を実行できます。そのほかにも、一覧に表示されている情報をクリップボードにコピーしたり、表示項目を変更したりできます。

カスタムグループを利用する

機器情報や資産情報などを任意にグルーピングできます。任意のグループを作成して、目的に応じた情報を登録して管理します。このグループをカスタムグループと呼びます。

一覧のページを切り替える

表示される項目の件数が多い場合、一覧はページごとに表示されます。一覧の右上にある  をクリックすると、次のページに進み、 をクリックすると、前のページに戻ります。また、 の部分にページ数を指定して、特定のページにジャンプすることもできます。

1 ページ中に表示される件数を変更したい場合は、 をクリックして、100 件、250 件、500 件、1,000 件の中から選択してください。なお、デフォルトでは 250 件に設定されています。

関連リンク

- [5.2 表示中の画面の情報を更新する手順](#)
- [5.3 一覧の表示項目を変更する手順](#)
- [5.6.1 カスタムグループを追加する手順](#)

5.5 ユーザー定義のグループを管理する

5.5.1 ユーザー定義のグループを追加する手順

メニューエリアの「機器一覧（ユーザー定義）」から、ユーザー定義のグループを追加できます。

ユーザー定義のグループを追加するには：

1. メニューエリアの「機器一覧（ユーザー定義）」にマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるダイアログで、「追加」 ボタンをクリックします。
5. 表示されるダイアログで、ユーザー定義のグループ名およびユーザー定義のグループ条件を設定して、「OK」 ボタンをクリックします。
6. 「OK」 ボタンをクリックします。

メニューエリアにユーザー定義のグループが追加されます。

関連リンク

- [5.5.2 ユーザー定義のグループ名を変更する手順](#)
- [5.5.3 ユーザー定義のグループを削除する手順](#)
- [5.5.4 ユーザー定義のグループ条件を変更する手順](#)

5.5.2 ユーザー定義のグループ名を変更する手順

ユーザー定義のグループ名は、メニューエリアから変更できます。

ユーザー定義のグループ名を変更するには：

1. メニューエリアの「機器一覧（ユーザー定義）」で、名称を変更したいグループにマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。

4. 表示されるテキストエリアにユーザー定義のグループ名を入力します。

ユーザー定義のグループ名が変更されます。

ポイント

メニューエリアの「機器一覧（ユーザー定義）」から表示できるダイアログで、ユーザー定義のグループを編集するときにも、ユーザー定義のグループ名を変更できます。

関連リンク

- 5.5.1 ユーザー定義のグループを追加する手順
- 5.5.3 ユーザー定義のグループを削除する手順
- 5.5.4 ユーザー定義のグループ条件を変更する手順

5.5.3 ユーザー定義のグループを削除する手順

不要になったユーザー定義のグループは、メニューエリアから削除できます。

ユーザー定義のグループを削除するには：

1. メニューエリアの「機器一覧（ユーザー定義）」で、削除したいグループにマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるダイアログで「OK」ボタンをクリックします。

ユーザー定義のグループが削除されます。

ポイント

メニューエリアの「機器一覧（ユーザー定義）」から表示できるダイアログも、ユーザー定義のグループを削除できます。

関連リンク

- 5.5.1 ユーザー定義のグループを追加する手順
- 5.5.2 ユーザー定義のグループ名を変更する手順
- 5.5.4 ユーザー定義のグループ条件を変更する手順

5.5.4 ユーザー定義のグループ条件を変更する手順

メニューエリアの「機器一覧（ユーザー定義）」から表示できるダイアログで、ユーザー定義のグループ条件を変更できます。

ユーザー定義のグループ条件を変更するには：

1. メニューエリアの「機器一覧（ユーザー定義）」にマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるダイアログで、条件を変更したいユーザー定義のグループの「編集」ボタンをクリックします。
5. 表示されるダイアログで、ユーザー定義のグループ条件を編集し、「OK」ボタンをクリックします。
6. 「OK」ボタンをクリックします。

ユーザー定義のグループ条件が変更されます。

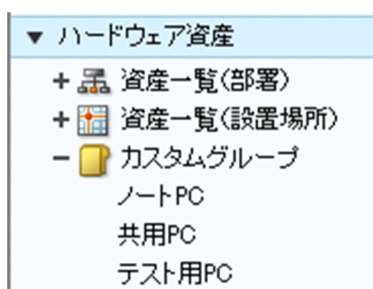
関連リンク

- [5.5.1 ユーザー定義のグループを追加する手順](#)
- [5.5.2 ユーザー定義のグループ名を変更する手順](#)
- [5.5.3 ユーザー定義のグループを削除する手順](#)

5.6 カスタムグループを管理する

5.6.1 カスタムグループを追加する手順

ハードウェア資産情報や機器情報などは、メニューエリアで任意のグループに振り分けて管理できます。このグループのことをカスタムグループと呼びます。特定の情報だけを任意にグルーピングしたい場合に、カスタムグループを追加してください。



例えば、次のようにカスタムグループを活用できます。

- 資産画面のハードウェア資産のカスタムグループに「修理中」というカスタムグループを追加して、修理中の機器の情報を管理する。
- 機器画面のソフトウェア情報のカスタムグループに「自社ソフト」というカスタムグループを追加して、自社で作成したソフトウェア情報を管理する。

カスタムグループを追加するには：

1. メニューエリアの「カスタムグループ」にマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるテキストエリアにカスタムグループの名称を入力します。

メニューエリアにカスタムグループが追加されます。

ポイント

カスタムグループは、メニューエリアの「カスタムグループ」を右クリックして表示されるメニューから追加することもできます。

関連リンク

- [5.6.2 カスタムグループ名を変更する手順](#)

- 5.6.3 カスタムグループを削除する手順
- 5.6.4 カスタムグループに情報を追加する手順
- 5.6.5 カスタムグループから情報を削除する手順

5.6.2 カスタムグループ名を変更する手順

グルーピングしていた情報の観点が変わった場合は、カスタムグループ名を変更できます。

カスタムグループ名を変更するには：

1. メニューエリアの「カスタムグループ」で変更したいグループにマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるテキストエリアにカスタムグループの名称を入力します。

カスタムグループ名が変更されます。

ポイント

メニューエリアのカスタムグループを右クリックして表示されるメニューから変更することもできます。

関連リンク

- 5.6.1 カスタムグループを追加する手順
- 5.6.3 カスタムグループを削除する手順
- 5.6.4 カスタムグループに情報を追加する手順
- 5.6.5 カスタムグループから情報を削除する手順

5.6.3 カスタムグループを削除する手順

不要になったカスタムグループを削除できます。

カスタムグループを削除するには：

1. メニューエリアの「カスタムグループ」で削除したいグループにマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。

3. 表示されるメニューで  をクリックします。

4. 表示されるダイアログで [OK] ボタンをクリックします。

カスタムグループが削除されます。

ポイント

メニューエリアのカスタムグループを右クリックして表示されるメニューから削除することもできます。

関連リンク

- [5.6.1 カスタムグループを追加する手順](#)
- [5.6.2 カスタムグループ名を変更する手順](#)
- [5.6.4 カスタムグループに情報を追加する手順](#)
- [5.6.5 カスタムグループから情報を削除する手順](#)

5.6.4 カスタムグループに情報を追加する手順

目的に応じて情報をグルーピングするには、作成したカスタムグループに情報を追加します。

カスタムグループに情報を追加するには：

1. カスタムグループに追加したい情報をインフォメーションエリアに表示します。
2. 追加したい情報を選択して、[操作メニュー] の [カスタムグループに追加する] を選択します。
3. 表示されるダイアログで、情報を追加するカスタムグループを選択して [OK] ボタンをクリックします。

選択したカスタムグループに、情報が追加されます。

ポイント

インフォメーションエリアの情報を右クリックして、[カスタムグループに追加する] を選択して追加することもできます。

ポイント

インフォメーションエリアの情報を、メニューエリアの任意のカスタムグループにドラッグ&ドロップして追加することもできます。

関連リンク

- [5.6.1 カスタムグループを追加する手順](#)
- [5.6.2 カスタムグループ名を変更する手順](#)
- [5.6.3 カスタムグループを削除する手順](#)
- [5.6.5 カスタムグループから情報を削除する手順](#)

5.6.5 カスタムグループから情報を削除する手順

カスタムグループに追加した情報を別の観点でグルーピングしたい場合、カスタムグループに追加した情報を削除できます。

カスタムグループから情報を削除するには：

1. 情報を削除したいカスタムグループを選択します。
2. インフォメーションエリアで削除したい情報を選択して、[操作メニュー] の [カスタムグループから削除する] を選択します。
3. 表示されるダイアログで [OK] ボタンをクリックします。

選択したカスタムグループから、情報が削除されます。

ポイント

インフォメーションエリアの情報を右クリックして、[カスタムグループから削除する] を選択して削除することもできます。

関連リンク

- [5.6.1 カスタムグループを追加する手順](#)
- [5.6.2 カスタムグループ名を変更する手順](#)
- [5.6.3 カスタムグループを削除する手順](#)
- [5.6.4 カスタムグループに情報を追加する手順](#)

5.7 フィルタを管理する

5.7.1 フィルタを保存する手順

フィルタの条件を保存して繰り返し利用できます。業務で頻繁に使う条件を保存しておくで、すぐに目的の情報を絞り込めます。

フィルタを保存するには：

1. メニューエリアの「フィルタ」にマウスカーソルを合わせて、 をクリックします。
2. 「フィルタ」に追加されたフィルタの名称を入力します。
3. 表示される「フィルタ条件の編集」でフィルタの条件を設定します。
4. 「名前を付けて保存」ボタンをクリックします。
保存する前に「適用」ボタンをクリックしてフィルタの適用結果を確認すると、目的どおりの条件を設定できているか確認できます。

フィルタが保存されます。保存されたフィルタは、メニューエリアの「フィルタ」に追加されます。

なお、「フィルタ条件の編集」ダイアログは、 ボタンをクリックしても表示できます。

ポイント

メニューエリアの「フィルタ」を右クリックして、「フィルタを追加する」を選択して保存することもできます。

ポイント

フィルタの設定は、コマンドを実行してエクスポートおよびインポートできます。

関連リンク

- [17.17 ioutils exportfilter](#)（フィルタの設定のエクスポート）
- [17.18 ioutils importfilter](#)（フィルタの設定のインポート）
- [5.7.2 フィルタを削除する手順](#)

5.7.2 フィルタを削除する手順

不要になったフィルタを削除できます。

フィルタを削除するには：

1. メニューエリアで削除したいフィルタにマウスカーソルを合わせます。
2. 項目の右側に表示される  をクリックします。
3. 表示されるメニューで  をクリックします。
4. 表示されるダイアログで [OK] ボタンをクリックします。

フィルタが削除されます。

ポイント

メニューエリアのフィルタを右クリックして、[フィルタを削除する] を選択して削除することもできます。

関連リンク

- [5.7.1 フィルタを保存する手順](#)

5.8 操作画面利用時の注意事項

- Windows の拡大鏡機能を利用している場合にログアウトするときは、拡大鏡機能を終了させてからログアウトしてください。
- Web ブラウザが Cookie をブロックするように設定されている場合、操作画面が正しく表示されないことがあります。このときは、次の手順で管理用サーバを信頼済みサイトに登録してください。

Internet Explorer の場合

1. [ツール] – [インターネットオプション] メニューをクリックします。
2. [インターネットオプション] ダイアログで、[セキュリティ] タブの [信頼済みサイト] をクリックします。
3. [サイト] ボタンをクリックします。
4. [信頼済みサイト] ダイアログで次に示すとおりを設定して、[追加] ボタンをクリックします。
 - ・ [このゾーンのサイトにはすべてサーバーの確認 (https:) を必要とする] のチェックを外す
 - ・ [次の Web サイトをゾーンに追加する] に管理用サーバのアドレスを入力する
5. [閉じる] ボタンをクリックします。
6. [レベルのカスタマイズ] ボタンをクリックして、[アクティブ スクリプト] が [有効にする] になっていることを確認します。
[有効にする] になっていない場合は、[有効にする] を選択します。Web ブラウザの設定で JavaScript を無効にしていることで、ヘルプのリンクが正しく表示されないまたはヘルプが動作しない状態になることを防ぎます。
7. [インターネットオプション] ダイアログが閉じるまで [OK] ボタンをクリックします。
8. Web ブラウザを再起動します。

管理用サーバが信頼済みサイトに登録されます。

Firefox の場合

1. [ツール] – [オプション] メニューをクリックします。
2. [オプション] ダイアログで、[プライバシー] をクリックします。
3. [記憶させる履歴を詳細設定する] を選択し、[例外サイト] ボタンをクリックします。
4. [Cookie フィルタ] ダイアログで、[サイトのアドレス] に管理用サーバのアドレスを入力して、[許可] ボタンをクリックします。
5. [閉じる] ボタンをクリックします。
6. Web ブラウザを再起動します。

管理用サーバが信頼済みサイトに登録されます。

- 各ダイアログを表示したまま [OK] ボタンをクリックしない状態が 60 分以上続くと、タイムアウトが発生します。それまで作業していた内容は保存されませんので、注意してください。

- Web ブラウザが Internet Explorer 9 および Internet Explorer 10 の場合、次の画面で [参照] ボタンをクリックしてファイル選択の画面を開いたまま JP1/IT Desktop Management 2 の操作画面を操作すると、内部エラーが発生したり操作が継続できなくなったりすることがあります。必ずファイル選択の画面を閉じてから、JP1/IT Desktop Management 2 の操作画面を操作してください。
 - [資産情報をインポートしましょう] 画面
 - [ソフトウェアをインストールしましょう] 画面
 - [ファイルを配布しましょう] 画面
- 操作画面を開いたときやログインしたときに「異常なリクエスト」または「予期せぬエラー」のダイアログが表示される場合は、Web ブラウザのインターネット一時ファイルを削除してください。特に、JP1/IT Desktop Management 2 のインストール後に発生しやすいため注意してください。インターネット一時ファイルの削除方法を、Web ブラウザごとに示します。

Internet Explorer 7 の場合

1. [ツール] - [インターネットオプション] メニューを選択します。
2. [インターネットオプション] 画面で、[全般] タブを選択して [閲覧の履歴] の [削除] ボタンをクリックします。
3. [閲覧の履歴の削除] 画面で、インターネット一時ファイルの [ファイルの削除] ボタンをクリックします。
4. [ファイルの削除] 画面で、[はい] ボタンをクリックします。

Internet Explorer 8、9、10 の場合

1. [セーフティ] - [閲覧の履歴の削除] メニューを選択します。
2. [閲覧の履歴の削除] 画面で、[インターネット一時ファイル] をチェックして、[削除] ボタンをクリックします。

Firefox の場合

1. [ツール] - [最近の履歴を消去] メニューを選択します。
 2. [最近の履歴を消去] 画面で、[消去する項目] の左側の [レ] ボタンをクリックします。
 3. 表示したリストから [キャッシュ] をチェックして、[今すぐ消去] ボタンをクリックします。
- Web ブラウザが Internet Explorer の場合でポップアップブロックを有効にしているときは、ポップアップ画面を表示する操作をしても、画面が表示されないことがあります。この場合は、次の手順で許可するサイトに管理用サーバのアドレスを追加してください。
 1. [ツール] - [インターネットオプション] メニューを選択します。
 2. [インターネットオプション] 画面で、[プライバシー] タブを選択して [設定] ボタンをクリックします。
 3. [ポップアップブロックの設定] 画面の [許可する Web サイトのアドレス] に、管理用サーバのアドレスを入力して [追加] ボタンをクリックします。

6

機器を管理する

ここでは、組織内の機器から情報を収集して、現状を把握する方法について説明します。

6.1 機器の管理を始める方法

機器の管理を始めるためには、はじめに機器を管理対象にする必要があります。機器を管理対象にすると、自動的に収集された情報から現状を把握したり、セキュリティ管理、資産管理、および配布管理をしたりできます。

機器を管理対象にするには、次の方法があります。

機器を探索する方法

機器を探索して、発見された機器を管理対象にする方法です。

機器の現状を把握できていない場合に、ネットワークに接続されている機器を検出して管理対象にできます。また、Active Directory を探索することで、Active Directory で管理している機器をそのまま JP1/IT Desktop Management 2 の管理対象にできます。

コンピュータにエージェントをインストールする方法

管理したいコンピュータにエージェントをインストールして、ネットワークに接続します。エージェント導入済みのコンピュータが管理用サーバに接続されると自動的に管理対象になります。

ネットワークモニタ機能で検知する方法

ネットワークモニタ機能を利用して、新規にネットワークに接続しようとした機器を検知して発見する方法です。発見した機器を JP1/IT Desktop Management 2 の管理対象にできます。

MDM システムと連携してスマートデバイスを管理する方法

MDM システムと連携することで、MDM システムで管理しているスマートデバイスを、JP1/IT Desktop Management 2 の管理対象にできます。

組織内の機器を管理する場合、すべて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ます。

コンピュータにエージェントをインストールするためには、ワンタッチでインストールとセットアップを完了できるエージェントのインストーラー（エージェントインストールセット）を作成して手動でインストールするか、機器を探索すると同時にエージェントを配信して自動でインストールします。コンピュータ以外の機器を管理するためには、機器を探索して、発見された機器を管理対象にしてください。

エージェントインストールセットを作成したい場合は、ホーム画面に表示される「始めましょう」ボタンをクリックしてください。クリックすると、「機器の管理を始めましょう」ウィザードが起動します。このウィザードでエージェントインストールセットを作成できます。機器を探索したい場合は、設定画面の「機器の探索」画面を使用してください。「機器の探索」画面で探索条件を設定したり、探索を実行したりできます。

ポイント

「機器の管理を始めましょう」ウィザードは、「実行」メニューの「機器の管理を始めましょう」からも起動できます。

発見した機器の登録

探索やネットワークモニタの検知で発見した機器が、すでに管理対象になっているかどうかは、次の情報を基に判定されます。

- ホスト識別子※1
- IMEI※2
- ホスト名
- MAC アドレス
- IP アドレス

注※1 ホスト識別子とは、エージェントによって生成される、機器を識別するためのユニークな ID です。

注※2 MDM システムと連携してスマートデバイスを管理している場合に使用されます。

上の情報を基に、一致する管理対象の機器が存在しないと判定された場合は、新規に発見した機器として扱われます。

6.2 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、[次へ] 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。

コンポーネントの設定

インストールするコンポーネントの種別（エージェントとしてインストールするか、中継システムとしてインストールするか）とサブコンポーネントのリモコンエージェントをインストールするかどうかを指定します。

登録先の ID の設定

エージェントを登録する ID（配布管理システムからのジョブを受け取るためのグループ）を指定します。

展開するファイルの設定

エージェントのインストールと同時に展開するファイルと展開先のフォルダを指定します。

自動実行するファイルの設定

エージェントのインストール後に自動実行するファイル、自動実行に必要なファイル、および引数を指定します。

上書きインストールの設定

エージェントがすでにインストールされている場合、上書きインストールするかどうかを設定します。

4. 設定内容を確認して、[作成] ボタンをクリックします。

インストールセットをダウンロードするダイアログが表示されます。

5. 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「ITDM2Agt.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。

ポイント

上位接続先情報ファイル (dmhost.txt) を作成して、JP1/IT Desktop Management 2 - Manager のデータフォルダに格納しておく、インストールセットの作成時にインストールセットに取り込まれます。上位接続先情報ファイルの詳細については、マニュアル「JP1 Version 10 JP1/IT Desktop Management 2 配布機能 運用ガイド」の、エージェントの接続先の自動変更についての説明を参照してください。

関連リンク

- [15.1.2 エージェント設定を追加する手順](#)
- [\(2\) エージェントをコンピュータに導入する方法](#)

6.3 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

- [15.2.2 探索条件を設定する手順（Active Directory の探索）](#)
- [15.2.4 機器の探索状況の確認](#)

6.4 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すため、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

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

6.5 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。

6.6 機器を除外対象にする手順

探索で発見された機器や管理対象の機器のうち、管理する必要がない機器は、除外対象にします。

機器を除外対象にすることで、機器を探索しても発見されなくなります。これによって、定期的に機器を探索している場合に、新規に発見された機器だけを確認できます。

機器を除外対象にするには：

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」または「管理対象機器」を選択します。
3. 除外対象にする機器を選択します。
4. 「除外対象にする」ボタンをクリックします。

機器が除外対象になります。

管理対象の機器を除外対象にした場合、機器画面に表示されなくなります。また、ハードウェア資産情報に関連づいていた機器情報も削除されます。

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。機器を除外対象に設定すると、自動的にネットワーク接続が許可されます。

ポイント

除外対象にした機器を再度管理対象にした場合、IP アドレス、ホスト名、シリアルナンバー、または MAC アドレスが一致するハードウェア資産情報があるときは、その資産情報に機器情報が自動的に関連づけられます。

注意事項

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。

6.7 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［基本設定］で、［上位システムと通信する］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］－［JP1_IT Desktop Management 2 - 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、［上位システムと通信する］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［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ンライン管理となります。

6.8 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 [基本設定] で、[上位システムと通信する] 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。

6.9 機器を削除する手順

エージェントをアンインストールしないで機器を撤去した場合や、エージェントのアンインストール時に管理用サーバと通信できなかった場合、機器情報が管理用サーバに残ったままになっていることがあります。このような状況を発見したとき、機器の状況を正しく把握するために、不要な機器情報を削除する必要があります。

機器を削除するには：

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]、[管理対象機器] または [除外対象機器] を選択します。
3. 削除する機器を選択します。
4. [操作メニュー] から [削除する] を選択します。

機器が削除されます。機器を削除すると、データベースから機器情報が削除されます。

削除された機器は、探索で再度発見できます。この場合、新規機器として扱われ、以前の設定は引き継がれません。

注意事項

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削除できません。

6.10 機器情報を編集する手順

機器管理するためには、機器のさまざまな情報を把握しておく必要があります。しかし、機器の環境によっては機器情報を収集できないこともあります。このような機器に対して、機器情報を手動で編集できます。未取得の情報を編集するだけでなく、すでに収集されている情報を編集することもできます。

例えば、OS の情報が収集されていない場合や、未サポートの OS のコンピュータから OS の情報が収集された場合は、OS のグループには登録されないで「不明」という扱いになり、グループ構成が実際のコンピュータの分類と異なってしまいます。このような場合に、手動で OS の情報を編集することで、コンピュータを正しく管理できるようにします。

機器情報を編集するには：

1. 機器画面を表示します。
2. メニューエリアの「機器情報」で任意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情報を編集する機器を選択します。
機器は複数選択できます。
4. 「操作メニュー」の「機器情報を編集する」を選択します。
5. 表示されるダイアログで機器情報を編集します。
6. 「OK」ボタンをクリックします。

機器情報が更新されます。

注意事項

手動で編集した機器情報よりも、収集された機器情報が優先されます。このため、機器情報を編集したあとで情報が収集されると、収集された情報で更新されます。ただし、「機器種別」だけは手動で設定した情報が優先されます。

注意事項

ハードウェア資産情報に関連づけている機器情報の「ホスト名」を変更しても、ハードウェア資産情報の「機器名称」は自動で変更されません。ハードウェア資産情報の「機器名称」と機器情報の「ホスト名」を統一している場合に、機器情報の「ホスト名」を変更したときは、ハードウェア資産情報の「機器名称」を手動で変更してください。

6.11 最新の機器情報を取得する手順

オンライン管理用のエージェントを導入済みのコンピュータから、任意のタイミングで最新の機器情報を取得できます。

利用者によって入力された利用者情報を収集している場合で、エージェント設定の［利用者への通知設定］で利用者情報の入力画面を表示するように設定したときは、機器情報を取得するタイミングで［利用者情報の入力］画面が利用者のコンピュータに表示されます。

最新の機器情報を取得するには：

1. 機器画面を表示します。
2. メニューエリアの［機器情報］で任意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情報を取得する機器を選択します。
機器は複数選択できます。
4. [操作メニュー] の［最新の情報を取得する］を選択します。
5. エージェントが導入されている機器を、情報の取得と同時に電源を ON にしたい場合、[選択したコンピュータが稼働していない場合に起動する] をチェックします。
6. [OK] ボタンをクリックします。

最新の機器情報が取得されます。利用者の情報は、最後に入力されたものが収集されます。

[選択したコンピュータが稼働していない場合に起動する] をチェックすると、電源が OFF のときでも自動的に電源を ON にしてから機器情報を取得します。機器情報を取得したあとは、自動的に電源が OFF になります。すでに電源が ON のときは、電源は OFF にはなりません。

注意事項

Wake on LAN の機能で電源を ON にできるのは、管理用サーバと同一のネットワークセグメントにあるコンピュータだけです。

次の場合は、機器情報の収集後に自動的に電源が OFF になることがあります。

- 自動的に電源が ON になる直前に、コンピュータの利用者が手動で電源を ON にした場合
- ネットワークの状態によって、コンピュータの電源の ON/OFF を正確に判定できなかった場合

また、マネージャから対象のコンピュータへの通信に失敗した場合は、機器情報の収集後に自動的に OFF にならないことがあります。この場合は、[操作メニュー] の［電源 OFF にする］を選択することで、対象のコンピュータの電源を OFF にしてください。

関連リンク

- [15.5.6 AMT の認証情報を設定する手順](#)
- [6.23 コンピュータの電源を制御する手順](#)

6.12 情報収集用ツールを生成する手順

情報収集用ツールは、オフライン管理のコンピュータの機器情報を収集する際に利用します。

情報収集用ツールを生成するには：

1. 機器画面を表示します。
2. メニューエリアの「機器情報」で任意の機器一覧を選択します。
3. 「操作メニュー」の「情報収集用ツールを生成する」を選択します。

情報収集用ツールをダウンロードするダイアログが表示されます。デフォルトで表示されるファイル名は「ITDM2Offline.zip」です。

情報収集用ツールのダウンロードが開始されます。

ダウンロードした情報収集用ツールは、保存先で解凍したあとで外部記憶媒体に格納してください。ログオンスクリプトを利用して機器情報を収集する場合は、オフライン管理のコンピュータと接続している共有サーバに格納してください。

関連リンク

- [6.13 情報収集用ツールで収集した機器情報を通知する手順](#)

6.13 情報収集用ツールで収集した機器情報を通知する手順

情報収集用ツールで収集したオフライン管理のコンピュータの機器情報を、オンライン管理のコンピュータから管理用サーバに通知します。機器情報を通知することで、オフライン管理のコンピュータの機器情報が、最新の機器情報に更新されます。

機器情報を通知するには、情報収集用ツールで収集した情報を格納しているフォルダのフルコントロール権限を持つユーザーで、オンライン管理のコンピュータにログオンする必要があります。機器情報を通知するときは管理用サーバと接続するため、オフライン管理のコンピュータからは機器情報を通知できません。

注意事項

古い機器情報を通知した場合、現在 JP1/IT Desktop Management 2 に登録されている機器情報に、古い機器情報が上書きされます。この場合、対象のコンピュータから最新の機器情報を収集したあと、機器情報を再度通知し直す必要があります。

注意事項

変更履歴の取得設定をしている場合は、機器情報が実際に変更された順序で通知してください。実際の順序どおり通知しないと、正しい変更履歴の日時が取得されません。

情報収集用ツールを使用して収集した機器情報を通知するには：

ログオンスクリプトを利用して機器情報を収集した場合、手順 1.は不要です。

1. 情報収集用ツールで収集した機器情報が格納されている外部記憶媒体を、オンライン管理のコンピュータに接続します。
2. Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Agent] - [管理者ツール] - [収集情報の通知] を選択します。
外部記憶媒体を使用した情報通知をパスワードで保護するように設定している場合、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の [パスワードの設定] - [外部記憶媒体を使用した情報通知の保護設定] で設定したパスワードを入力してください。新規に作成したエージェント設定の場合、デフォルトではパスワードで保護されていません。
3. [通知情報の格納先の指定] ダイアログで、通知する機器情報を格納しているフォルダを指定します。
フォルダを指定するときは、[¥Data] を含めて 133 文字以内の、ASCII コードの制御文字を除いた文字列を用いたパスで指定してください。
4. [OK] ボタンをクリックします。

機器情報の通知が開始されます。通知が完了するまで、進捗状況を示すダイアログが表示されます。

通知結果を示すダイアログが表示されて、機器情報の通知が完了します。

機器情報の通知に失敗したコンピュータがある場合は、通知失敗リスト（result_failed.txt）の情報を基に機器情報を収集し直したあと、再通知してください。詳細については、「[18.4 情報収集用ツールで収集した機器情報の通知に失敗した場合のトラブルシューティング](#)」を参照してください。

機器情報の通知に成功したコンピュータを確認したい場合は、通知成功リスト（result_success.txt）を確認してください。通知成功リストは、通知に成功したコンピュータがある場合に生成されます。通知成功リストには、機器情報の通知に成功したコンピュータのホスト名の一覧が出力されます。

生成先

［通知情報の格納先の指定］ダイアログで指定した「Data」フォルダ

出力形式

YYYY/MM/DD△hh:mm:ss△ホスト名※

注※ YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

出力例

2012/10/11 14:15:16 Host1

2012/10/11 14:15:18 Host2

2012/10/11 14:15:19 Host3

関連リンク

- [6.12 情報収集用ツールを生成する手順](#)

6.14 利用者情報を取得する手順

利用者のコンピュータに「利用者情報の入力」画面を表示させて、利用者が入力した情報を取得できます。定期的に利用者に情報を入力してもらうことで、管理業務の負担を軽減できます。「利用者情報の入力」画面の例を次に示します。

なお、「利用者情報の入力」画面を表示させるには、利用者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必要があります。利用者情報の入力画面の表示は、エージェント設定の「利用者への通知設定」の設定に従います。

「利用者情報の入力」画面を、随時表示させる場合の手順と、指定した日時以降に表示させる場合の手順を、それぞれ示します。

利用者情報を取得するには（随時）：

1. 設定画面を表示します。

2. メニューエリアの [資産管理] – [資産管理項目の設定] を選択します。

3. 利用者情報を取得したい項目の [入力方法] を「利用者が入力」に設定します。

「利用者が入力」を設定できるのは、[資産情報と機器情報の共通管理項目] および [ハードウェア資産情報の追加管理項目] だけです。

[利用者情報の入力] 画面で利用者が情報を入力して [OK] ボタンをクリックすると、利用者情報が取得されます。

利用者情報を取得するには (日時を指定) :

1. 設定画面を表示します。

2. メニューエリアの [資産管理] – [資産管理項目の設定] を選択します。

3. インフォメーションエリアの [利用者情報の入力開始日時] で [編集] ボタンをクリックします。

4. [利用者の入力開始のタイミング] で [指定 (利用者のコンピュータのローカルタイムで指定する入力開始日時)] を選択し、入力開始日時を指定します。

5. [OK] ボタンをクリックします。

6. 利用者情報を取得したい項目の [入力方法] を「利用者が入力」に設定します。

「利用者が入力」を設定できるのは、[資産情報と機器情報の共通管理項目] および [ハードウェア資産情報の追加管理項目] だけです。

[入力方法] を設定するダイアログにある [入力開始日時を編集] ボタンをクリックして表示されるダイアログで、入力開始日時を編集することもできます。

[利用者情報の入力] 画面で利用者が情報を入力して [OK] ボタンをクリックすると、利用者情報が取得されます。

関連リンク

- [15.4.1 資産管理項目を追加する手順](#)

6.15 機器画面で [利用者情報の入力] 画面の表示間隔を設定する手順

オンライン管理のコンピュータに、[利用者情報の入力] 画面を表示させる間隔を設定できます。定期的に利用者に情報を入力してもらうことで、管理業務の負担を軽減できます。

例えば、部署の情報を利用者に入力してもらう場合、更新頻度が少ないと、組織内で異動があったときに操作画面の情報と現状が合わなくなるおそれがあります。環境に応じて、適切なスケジュールを設定してください。

利用者情報の表示間隔を設定するには：

1. 機器画面を表示します。
2. メニューエリアの [機器情報] で任意のグループを選択します。
3. [操作メニュー] の [[利用者情報の入力] 画面を定期的に表示させる] を選択します。
4. 表示されるダイアログで、表示間隔を設定して [OK] ボタンをクリックします。

[利用者情報の入力] 画面の表示間隔が設定されます。

[利用者情報の入力] 画面の表示間隔が設定されている場合、[操作メニュー] の項目に緑色のチェックが付きます。再度メニューを選択すると、設定を解除できます。

関連リンク

- [6.14 利用者情報を取得する手順](#)

6.16 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。

6.17 機器情報をエクスポートする手順

機器画面の[機器情報] 画面のインフォメーションエリアに表示された機器情報を、CSV ファイルにエクスポート（一括出力）できます。

特定の機器情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、[機器種別] が「PC」の機器情報だけエクスポートする場合は、[機器種別] が「PC」の機器情報をフィルタリングして表示します。

機器情報をエクスポートするには：

1. 機器画面を表示します。
2. [機器情報] で任意のグループを選択します。
3. エクスポートする機器をインフォメーションエリアに表示します。
4. [操作メニュー] の[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。
5. [エクスポートする項目の選択] ダイアログで、エクスポートする項目をチェックして、[OK] ボタンをクリックします。
エクスポートされる CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトでは文字コードは「UTF-8」になります。
6. 表示された画面の[保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

ポイント

[機器一覧（詳細）をエクスポートする] では、画面下部のタブに表示される情報もエクスポートできます。主な情報だけの一覧を作成したい場合は [機器一覧をエクスポートする] を、詳細な情報の一覧を作成したい場合は [機器一覧（詳細）をエクスポートする] を利用してください。

6.18 ソフトウェア情報をエクスポートする手順

機器画面の [ソフトウェア情報] 画面のインフォメーションエリアに表示されたソフトウェア情報を、CSV ファイルにエクスポート（一括出力）できます。

特定のソフトウェア情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、使用必須ソフトウェアに指定されているソフトウェア情報だけエクスポートする場合は、[必須ソフトウェア] が「必須」のソフトウェア情報をフィルタリングして表示します。

機器情報をエクスポートするには：

1. 機器画面を表示します。
2. [ソフトウェア情報] - [ソフトウェア一覧] を選択します。
3. エクスポートするソフトウェアをインフォメーションエリアに表示します。
4. [操作メニュー] から [ソフトウェア一覧をエクスポートする] を選択します。
5. [エクスポートする項目の選択] ダイアログで、エクスポートする項目をチェックして、[OK] ボタンをクリックします。
エクスポートされる CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトでは文字コードは「UTF-8」になります。
6. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

6.19 ソフトウェア情報を削除する手順

機器画面の [ソフトウェア情報] 画面に表示されるソフトウェア情報を削除できます。

ライセンス消費数が 0 で管理が不要なソフトウェア情報は削除することをお勧めします。

ソフトウェア情報を削除するには：

1. 機器画面の [ソフトウェア情報] 画面を表示します。
2. インフォメーションエリアで、削除するソフトウェア情報を選択します。
3. [操作メニュー] の [ソフトウェアの削除] を選択します。
4. [ソフトウェア情報の削除] ダイアログで、削除してもよいか確認します。
削除する場合は、[操作を続行する] をチェックします。
5. [OK] ボタンをクリックします。

ソフトウェア情報が削除されます。

削除したソフトウェア情報が管理対象のコンピュータから収集された場合、ソフトウェア情報は再度表示されます。

なお、ソフトウェア情報を削除しても、セキュリティポリシーの使用必須ソフトウェアや使用禁止ソフトウェアの設定、および管理ソフトウェア情報の設定には影響しません。また、各機器情報のインストールソフトウェア情報にも影響しません。

6.20 使用禁止ソフトウェアを設定する手順

ソフトウェア情報の一覧で確認したソフトウェアを、使用禁止ソフトウェアに設定できます。

業務に不要なソフトウェアや、セキュリティ上問題となるソフトウェアは、使用禁止ソフトウェアとしてセキュリティポリシーに登録することで、インストール状況を把握したり、ソフトウェアの利用を抑止したりできます。

使用禁止ソフトウェアを設定するには：

1. 機器画面を表示します。
2. メニューエリアで [ソフトウェア情報] – [ソフトウェア一覧] を選択します。
3. インフォメーションエリアで、使用禁止ソフトウェアとして登録したいソフトウェアの [禁止ソフトウェアへ追加] ボタンをクリックします。
4. 表示されるダイアログで、登録先のセキュリティポリシーを選択して、使用禁止ソフトウェアを設定します。
5. [OK] ボタンをクリックします。

ソフトウェアが使用禁止ソフトウェアとしてセキュリティポリシーに登録されます。

使用禁止ソフトウェアに登録したソフトウェアは、インフォメーションエリアの [禁止ソフトウェア] 欄に印が付きます。また、[ソフトウェア情報] タブの [セキュリティ関連情報] で、登録内容を確認できます。

使用禁止ソフトウェアの登録内容を変更したい場合は、セキュリティポリシーを編集してください。

関連リンク

- [1.7.1 セキュリティポリシーを設定する](#)

6.21 機器画面でコンピュータからソフトウェアをアンインストールする手順

業務に不要なソフトウェアや、使用を禁止しているソフトウェアがインストールされていた場合、コンピュータからソフトウェアをアンインストールできます。

なお、ソフトウェアをアンインストールできるのは、オンライン管理のコンピュータだけです。

コンピュータからソフトウェアをアンインストールするには：

1. 機器画面を表示します。
2. メニューエリアで [ソフトウェア情報] - [ソフトウェア一覧] を選択します。
3. インフォメーションエリアで、コンピュータからアンインストールしたいソフトウェアを選択して、[インストール済みコンピュータ] タブを表示します。
4. ソフトウェアをアンインストールしたいコンピュータを選択して、タブ内の [アンインストール] ボタンをクリックします。
複数のコンピュータを選択して、一括でアンインストールすることもできます。
5. 表示されるダイアログでアンインストールタスクを作成して、[OK] ボタンをクリックします。

アンインストールタスクに設定したスケジュールに従って、ソフトウェアがアンインストールされます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク一覧] 画面で確認してください。

ポイント

配布 (ITDM 互換) 画面からアンインストールタスクを作成・実行することもできます。

ポイント

セキュリティポリシーの使用禁止ソフトウェアを設定する際に、自動対策としてソフトウェアのアンインストールを設定することもできます。

関連リンク

- 1.7.1 セキュリティポリシーを設定する

6.22 利用者にメッセージを通知する手順

コンピュータの利用者に通知したいメッセージがある場合は、メッセージを作成して個別に通知できます。

なお、メッセージを通知できるのは、オンライン管理のコンピュータだけです。

利用者にメッセージを通知するには：

1. 機器画面を表示します。
2. メニューエリアの [機器情報] でメッセージを通知したいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアで、メッセージを通知したいコンピュータを選択して、[操作メニュー] の [利用者にメッセージを通知する] を選択します。
複数のコンピュータを選択して、同じ内容のメッセージを一斉に通知することもできます。
4. 表示されるダイアログで、通知するメッセージを設定して、[OK] ボタンをクリックします。
[選択したコンピュータが稼働していない場合に起動する] をチェックすると、稼働していない対象コンピュータにもメッセージを通知できます。
[ノートに追記する] をチェックすると、メッセージを通知した履歴や理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

コンピュータの利用者にメッセージが通知されます。

6.23 コンピュータの電源を制御する手順

コンピュータの電源を ON または OFF にしたり、コンピュータを再起動したりできます。

なお、コンピュータの電源を制御するには、対象のコンピュータが一定の条件を満たしている必要があります。

コンピュータの電源を制御するには：

1. 機器画面を表示します。
2. メニューエリアの [機器情報] で電源を制御したいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアで、電源を制御したいコンピュータを選択して、[操作メニュー] の [電源 ON にする]、[電源 OFF にする]、または [再起動する] を選択します。
複数のコンピュータを選択すると、選択したコンピュータの電源を一括で制御できます。
4. 表示されるダイアログで、[操作を続行する] にチェックして、[OK] ボタンをクリックします。

コンピュータの電源が ON または OFF になります。または、コンピュータが再起動されます。

コンピュータの電源の状態は、機器の一覧の [機器状態] 欄で確認できます。

6.24 スマートデバイスの情報を取得する手順

連携している MDM システムから、任意のタイミングでスマートデバイスの最新情報を取得できます。

スマートデバイスの情報を取得するには：

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] - [MDM 連携の設定] を選択します。
3. インフォメーションエリアの [MDM 連携の設定] で、取得するスマートデバイスの情報を管理している MDM システムの設定を選択します。
4. [操作メニュー] から [MDM システムから機器情報を取得する] を選択します。
5. 表示されるダイアログで、[OK] ボタンをクリックします。

一覧が更新され、スマートデバイスの情報が取得されます。

機器情報の取得状況を知りたい場合は、[操作メニュー] から [一覧を最新の情報に更新する] を選択してください。[MDM 連携の設定] の一覧が最新の情報に更新され、取得状況を確認できます。

ポイント

MDM 連携の設定でスマートデバイスの情報を定期的に取得するように設定している場合、管理対象のスマートデバイスの機器情報はスケジュールに従って自動的に更新されます。

ポイント

JP1/IT Desktop Management 2 が取得する機器情報は、MDM システムがスマートデバイスから取得した情報です。このため、スマートデバイスの最新情報と、JP1/IT Desktop Management 2 で管理している機器情報が異なる場合があります。

6.25 スマートデバイスをロックする手順

利用者がスマートデバイスを紛失した場合、拾得者が操作できないように管理者がスマートデバイスをロックできます。

スマートデバイスをロックするには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】でロックしたいスマートデバイスが含まれるグループを選択します。
3. インフォメーションエリアで、ロックしたいスマートデバイスを選択して、【操作メニュー】の【ロックする（スマートデバイス）】を選択します。
複数のスマートデバイスを選択すると、選択したスマートデバイスを一括でロックできます。
4. 表示されるダイアログで、【OK】ボタンをクリックします。

選択したスマートデバイスがロックされます。

注意事項

スマートデバイスにパスコードが設定されていない場合、ロックを実行してもスマートデバイスを操作できます。操作させたくない場合は、必ずスマートデバイスにパスコードを設定してください。

ポイント

スマートデバイスのロックは、JP1/IT Desktop Management 2 が出す要求に従って、MDM システムから実行されます。そのため、MDM システムが JP1/IT Desktop Management 2 から操作の要求を受けた時点で、スマートデバイスのロックが完了したと見なされます。

6.26 スマートデバイスのパスコードをリセットする手順

利用者がスマートデバイスのパスコードを忘れた場合、パスコードを再設定できるように、管理者がスマートデバイスのパスコードをリセットできます。

一度にパスコードをリセットできるのは1台のスマートデバイスだけです。複数のスマートデバイスのパスコードをリセットしたい場合は、1台ずつリセットしてください。

スマートデバイスのパスコードをリセットするには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】でパスコードをリセットしたいスマートデバイスが含まれるグループを選択します。
3. インフォメーションエリアでパスコードをリセットしたいスマートデバイスを選択して、【操作メニュー】の【パスコードをリセットする（スマートデバイス）】を選択します。
4. 表示されるダイアログで、【操作を続行する】をチェックします。
【ノートに追記する】をチェックすると、スマートデバイスのパスコードをリセットした履歴や理由などを記録できます。ここで入力した情報は【ノート】タブに追記されます。
5. 【OK】ボタンをクリックします。

選択したスマートデバイスのパスコードがリセットされます。

スマートデバイスのパスコードをリセットしたあとは、利用者にパスコードを再設定するように指示してください。

ポイント

スマートデバイスのパスコードのリセットは、JP1/IT Desktop Management 2 が出す要求に従って、MDM システムから実行されます。そのため、MDM システムが JP1/IT Desktop Management 2 から操作の要求を受けた時点で、スマートデバイスのパスコードのリセットが完了したと見なされます。

6.27 スマートデバイスを初期化する手順

スマートデバイスを初期化して、工場から出荷されたときの状態にできます。

一度に初期化できるのは 1 台のスマートデバイスだけです。複数のスマートデバイスを初期化したい場合は、1 台ずつ初期化してください。

スマートデバイスを初期化するには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】で初期化したいスマートデバイスが含まれるグループを選択します。
3. インフォメーションエリアで初期化したいスマートデバイスを選択して、【操作メニュー】の【初期化する（スマートデバイス）】を選択します。
4. 表示されるダイアログで、【操作を続行する】をチェックします。
【ノートに追記する】をチェックすると、スマートデバイスを初期化した履歴や理由などを記録できます。ここで入力した情報は【ノート】タブに追記されます。
5. 【OK】 ボタンをクリックします。

選択したスマートデバイスが初期化されます。

ポイント

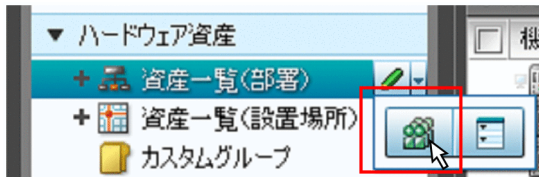
スマートデバイスの初期化は、JP1/IT Desktop Management 2 が出す要求に従って、MDM システムから実行されます。そのため、MDM システムが JP1/IT Desktop Management 2 から操作の要求を受けた時点で、スマートデバイスの初期化が完了したと見なされます。

6.28 部署・設置場所の定義を追加する手順

管理する部署や設置場所が増えた場合、部署・設置場所の定義を追加できます。定義を追加すると、追加した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を追加するには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」で、「資産一覧（部署）」または「資産一覧（設置場所）」を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の「資産管理」－「資産管理項目の設定」を選択して表示される画面で、「資産情報と機器情報の共通管理項目」の「部署」または「設置場所」の「編集」ボタンをクリックしても追加できます。

3. 表示されるダイアログで「データ型」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部署・設置場所を追加します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が追加されて、資産画面や機器画面などのメニューエリアに追加したグループが表示されます。

関連リンク

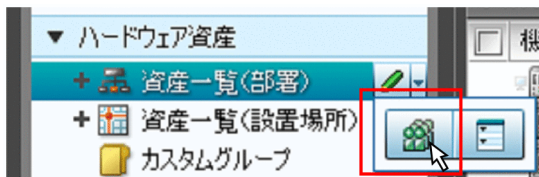
- [6.29 部署・設置場所の定義を編集する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)

6.29 部署・設置場所の定義を編集する手順

管理する部署が統合されたり設置場所の名称が変更になったりした場合、部署・設置場所の定義を編集できます。定義を編集すると、編集した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を編集するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で、[資産一覧 (部署)] または [資産一覧 (設置場所)] を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の [資産管理] - [資産管理項目の設定] を選択して表示される画面で、[資産情報と機器情報の共通管理項目] の [部署] または [設置場所] の [編集] ボタンをクリックしても編集できます。

3. 表示されるダイアログで [データ型] 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部署・設置場所の名称や階層を編集します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が編集されて、資産画面や機器画面などのメニューエリアに編集したグループが表示されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除します。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が変更されると、資産画面の [ソフトウェアライセンス] – [ソフトウェアライセンス一覧]、[ソフトウェアライセンス状況] – [ソフトウェアライセンス状況一覧] および資産画面の [契約] – [契約一覧] に表示される部署の情報も変更されます。

関連リンク

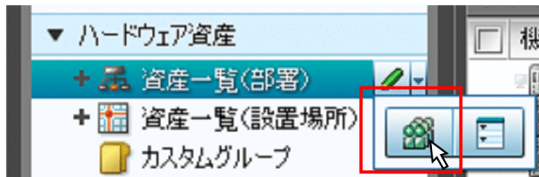
- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)

6.30 部署・設置場所の定義を削除する手順

管理していた部署や設置場所を管理しなくなった場合、部署・設置場所の定義を削除できます。定義を削除すると、削除した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を削除するには：

1. 資産画面を表示します。
2. メニューエリアの［ハードウェア資産］で、［資産一覧（部署）］または［資産一覧（設置場所）］を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで［データ型］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部署・設置場所の定義を削除します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が削除されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除します。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が削除されると、資産画面の次の画面に表示されていた該当する部署の情報は、「不明」と表示されます。

- [ソフトウェアライセンス] — [ソフトウェアライセンス一覧] 画面
- [ソフトウェアライセンス状況] — [ソフトウェアライセンス状況一覧] 画面
- [契約] — [契約一覧] 画面

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)

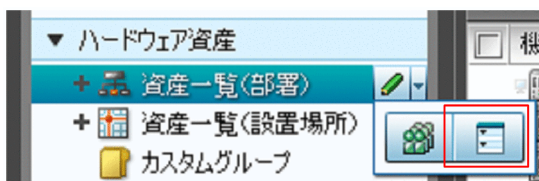
6.31 旧体制で使われていた階層だけを削除する手順

職制変更に伴い設定画面で部署・設置場所の階層（定義）を削除しても、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。メニューエリアの表示を定義に合わせるためには、旧体制で使われていた階層だけを削除する必要があります。メニューエリアの階層は、資産画面、機器画面およびセキュリティ画面のメニューエリアから表示できるダイアログで削除できます。

資産画面で削除する場合を例に、手順を次に示します。

旧体制で使われていた階層だけを削除するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで、削除したい階層を選択します。
4. 【削除】 ボタンをクリックします。
5. 表示されるダイアログで、【OK】 ボタンをクリックします。
6. 【閉じる】 ボタンをクリックします。

旧体制で使われていた階層だけが削除されて、資産画面や機器画面のメニューエリアの表示が定義と一致します。

6.32 部署・設置場所の名称を変更する手順

管理する部署が統合されたり設置場所の名称が変更になったりした場合、部署・設置場所の名称を変更できます。

部署・設置場所の名称を変更するには：

1. 資産画面を表示します。
2. メニューエリアの［ハードウェア資産］で、［資産一覧（部署）］または［資産一覧（設置場所）］で名称を変更したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるテキストエリアに部署または設置場所の名称を入力します。

部署・設置場所のグループの名称が変更されます。また、機器の利用者情報も変更後のグループ名に変更されます。

ポイント

メニューエリアの部署または設置場所を右クリックして表示されるメニューから変更することもできます。

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)
- [6.33 部署・設置場所を削除する手順](#)

6.33 部署・設置場所を削除する手順

不要になった部署・設置場所を削除できます。

部署・設置場所を削除するには：

1. 資産画面を表示します。
2. メニューエリアの［ハードウェア資産］で、［資産一覧（部署）］または［資産一覧（設置場所）］で削除したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるダイアログで［OK］ボタンをクリックします。

部署・設置場所のグループが削除されます。また、機器の利用者情報の部署・設置場所も削除されます。

ポイント

メニューエリアの部署・設置場所を右クリックして表示されるメニューから削除することもできます。

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)
- [6.32 部署・設置場所の名称を変更する手順](#)

7

機器をリモートコントロールする

ここでは、組織内の機器をリモートコントロールする方法について説明します。

7.1 コントローラをインストールする手順

コントローラは、JP1/IT Desktop Management 2 のインストール時にはインストールされません。操作画面でコントローラをダウンロードしてインストールします。

なお、インストールするには、Administrator 権限が必要です。

コントローラをインストールするには：

1. 機器画面を表示します。
2. 機器一覧で任意のコンピュータを選択して [リモートコントロールを開始する] ボタンをクリックします。
3. 表示されるダイアログで [実行] ボタンをクリックします。

操作画面を表示しているコンピュータに、コントローラがインストールされます。

なお、続けてリモートコントロールを開始するためのダイアログが表示されます。ダイアログに応答してリモートコントロールを開始してください。

注意事項

Web ブラウザが Firefox の場合、コントローラを自動でインストールできません。手順 3 で [保存] ボタンをクリックして、インストーラーを保存してから手動でインストールしてください。

注意事項

コントローラをインストールする際には、次の点に注意してください。

- インストール時は、Windows のドライバ署名オプションが一時的に「警告」に変更されます。Windows Server 2003 および Windows XP の場合、インストールが完了しても設定が元に戻らない場合があります。このとき、ドライバ署名オプションを手動で設定し直してください。
- OS をバージョンアップする場合、コントローラをアンインストールしてから、OS をバージョンアップしてください。アンインストール方法については、「[7.2 コントローラをアンインストールする手順](#)」を参照してください。
- Windows 7 の「Windows XP Mode」上にコントローラをインストールしないでください。

ポイント

リモコンエージェントは、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と、自動的にインストールされます。

関連リンク

- [7.3 コントローラの環境設定を変更する手順](#)
- [7.4 リモコンエージェントの動作環境を設定する手順](#)

7.2 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. 「JP1/IT Desktop Management 2 - 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。

7.3 コントローラの環境設定を変更する手順

コンピュータをリモートコントロールする場合に、接続方法や接続モード、コンピュータから送信されるデータの転送方法などの動作環境を変更できます。

環境設定は「環境の設定」ダイアログで変更します。設定できる項目を次の表に示します。

タブ	項目
「接続環境」タブ	- ポート番号 - 電源制御の有無 - 接続失敗時のリトライの設定 - 自動切断の有無 - 接続モード
「高速化」タブ	- データ転送関連（データ圧縮、暗号化の有無など） - デスクトップ関連（壁紙表示、アニメーションの抑止など） - 描画処理関連（減色、ビットマップのキャッシュなど） - クリップボード関連
「キーボードの設定」タブ	特殊キーの登録、送信の設定
「ログ情報」タブ	- ログ出力の有無 - ログ出力環境の設定 - リモートコントロールの録画の設定
「高度な設定」タブ	- 設定内容の保存と読み込み - AMT の設定（ユーザー ID、パスワード） - キーボード、マウスの設定（マウスボタンの設定など） - スクロール（オートスクロールの有無など）

コントローラの環境設定を変更するには：

1. 「リモートコントロール」ウィンドウのツールバーで「環境の設定」ボタンをクリックします。
2. 表示されるダイアログで各タブを設定したあと、「OK」ボタンをクリックします。

設定した値が保存され、コントローラの環境設定が変更されます。

ポイント

コントローラの環境設定は、各コンピュータにインストールされているコントローラごとに適用されます。ほかのコンピュータ上のコントローラには影響しません。

7.4 リモコンエージェントの動作環境を設定する手順

リモコンエージェントの動作環境は、エージェント設定の「リモートコントロールの設定」画面で設定します。

エージェント設定の設定方法については、「[15.1.1 エージェント設定の管理](#)」を参照してください。

7.5 リモートコントロールを利用する

7.5.1 コントローラを直接起動する手順

JP1/IT Desktop Management 2 にログインしなくても、直接コントローラを起動してコンピュータに接続できます。操作画面へのログインが不要なので、リモートコントロールだけを実行したい場合に、すぐに操作を開始できます。

直接コントローラを起動するには：

1. Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Manager] - [リモートコントロール] を選択します。

コントローラが起動します。

このとき、コンピュータには接続されていません。リモートコントロールを開始するためには、接続先を指定する必要があります。コントローラでの接続先の指定方法については、「[7.5.2 コンピュータを選択してリモートコントロールを開始する手順](#)」を参照してください。

ポイント

コマンドを利用して直接コントローラを起動することもできます。次のコマンドを実行します。

```
jdngrcctr.exe /agent IPアドレス
```

接続先をホスト名または IP アドレスで指定してください。コントローラが起動して指定したコンピュータと接続されます。指定を省略した場合は接続されません。

7.5.2 コンピュータを選択してリモートコントロールを開始する手順

コントローラから、接続先のコンピュータを選択して、リモートコントロールを開始できます。

コンピュータを選択して接続するには：

1. コントローラを起動します。
2. [リモートコントロール] ウィンドウのツールバーで [接続] ボタンをクリックします。
3. 表示されるメニューからコンピュータを選択します。

ポイント

[接続] ボタンをクリックして表示されるメニューには、接続リストに登録されているコンピュータが表示されます。

選択したコンピュータに接続され、コンピュータの画面が表示されます。

コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の [リモートコントロールの設定] - [ユーザー認証] に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ポイント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

関連リンク

- [7.5.1 コントローラを直接起動する手順](#)

7.5.3 ホスト名または IP アドレスを直接指定してリモートコントロールを開始する手順

コントローラから、接続先のコンピュータの IP アドレスまたはホスト名を直接指定して、リモートコントロールを開始できます。

ホスト名または IP アドレスを直接指定して接続するには：

1. コントローラを起動します。
2. [リモートコントロール] ウィンドウのツールバーの [対象のコンピュータの指定] に、接続先のホスト名または IP アドレスを入力します。

[接続] ボタン () - [接続] を選択して表示されるダイアログからも、ホスト名または IP アドレスを直接指定して接続できます。

3. [Enter] キーを押します。

指定したホスト名または IP アドレスのコンピュータに接続され、コンピュータの画面が表示されます。

コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の [リモートコントロールの設定] - [ユーザー認証] に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ポイント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

関連リンク

- [7.5.1 コントローラを直接起動する手順](#)

7.5.4 接続履歴を利用してリモートコントロールを開始する手順

過去に接続したコンピュータに対して、接続履歴を基に接続して、リモートコントロールを開始できます。

接続履歴から接続するには：

1. コントローラを起動します。
2. [リモートコントロール] ウィンドウのツールバーの [対象のコンピュータの指定] で、右端のボタンをクリックします。
3. プルダウンメニューに表示された履歴から接続先を選択します。

選択したコンピュータに接続され、コンピュータの画面が表示されます。

コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の [リモートコントロールの設定] - [ユーザー認証] に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ポイント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

関連リンク

- 7.5.1 コントローラを直接起動する手順

7.5.5 コンピュータを検索してリモートコントロールを開始する手順

リモートコントロールできるコンピュータがわからない場合、ネットワーク上に接続できるコンピュータがあるかどうかを検索できます。検索されたコンピュータに接続して、リモートコントロールを開始できます。

コンピュータを検索して接続するには：

1. コントローラを起動します。
2. コンピュータを検索します。
3. 検索結果に表示されたコンピュータに接続します。

接続リストからコンピュータを検索した場合は、検索されたコンピュータを選択して、 をクリックしてください。

［リモートコントロール］ウィンドウからコンピュータを検索した場合は、検索されたコンピュータのうち「接続待ち」状態のコンピュータを選択して［接続］ボタンをクリックしてください。

コンピュータに接続され、コンピュータの画面が表示されます。

コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の［リモートコントロールの設定］－［ユーザー認証］に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ポイント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、

接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

関連リンク

- 7.5.1 コントローラを直接起動する手順
- 7.5.26 [リモートコントロール] ウィンドウから接続できるコンピュータを検索する手順
- 7.5.27 接続リストからリモートコントロールできるコンピュータを検索する手順

7.5.6 操作画面からリモートコントロールを開始する手順

JP1/IT Desktop Management 2 の操作画面から、選択したコンピュータに接続してリモートコントロールできます。

コンピュータに接続するには：

1. 機器画面を表示します。
2. [機器情報] 画面で、接続するコンピュータを選択します。
複数のコンピュータを選択できます。

ポイント

フィルタを利用すると、目的のコンピュータを効率良く検索できます。

3. [リモートコントロールを開始する] ボタンをクリックします。

コントローラ（[リモートコントロール] ウィンドウ）が起動して、接続先のコンピュータの画面が表示されます。複数のコンピュータに接続すると、接続先の数だけウィンドウが起動します。

なお、コンピュータ側で認証情報が設定されている場合は、接続時に認証情報を入力するダイアログが表示されます。この場合、エージェント設定の [リモートコントロールの設定] - [ユーザー認証] に設定された認証情報、または接続先の VNC サーバに設定された認証情報を入力してください。デフォルトエージェント設定では、ユーザー ID が「system」、パスワードが「manager」の認証情報が設定されています。

また、コンピュータ側で接続要求が表示される設定の場合は、要求が拒否されると、コントローラに接続拒否のメッセージが表示されます。

ポイント

操作中のコンピュータにコントローラがインストールされていない場合は、リモートコントロール開始時に自動的にコントローラが、操作中のコンピュータにインストールされます。

ポイント

1 台のコンピュータに、同時に接続できるコントローラの数 は 255 台までです。

ポイント

コンピュータへの接続が拒否されたり、タイムアウトが発生したりした場合は、RFB で再接続を試みます。なお、接続時に、接続先のコンピュータの電源を ON にするよう設定されている場合は、接続先のコンピュータの電源 OFF によって RFB での再接続に失敗（タイムアウト）したときに、Wake on LAN および AMT によって接続先のコンピュータが起動され、再度接続を試みます。

7.5.7 リモートコントロール中のコンピュータとの接続を切断する手順

任意のタイミングで、リモートコントロール中のコンピュータとの接続を切断できます。

コンピュータとの接続を切断するには：

1. [リモートコントロール] ウィンドウのツールバーで [切断] ボタンをクリックします。

コンピュータとの接続が切断されます。

複数のコンピュータと接続していて、[リモートコントロール] ウィンドウが複数起動している場合は、切断を実行したウィンドウだけ切断されます。

ポイント

切断したあと、[リモートコントロール] ウィンドウのメニューで [ファイル] - [再接続] を選択すると、そのウィンドウで直前に接続していたコンピュータに再接続できます。

ただし、コンピュータ側の設定によって、切断と同時にリモコンエージェントが自動的に終了する場合があります。その場合、リモコンエージェントを再起動したあとに再接続してください。

7.5.8 リモートコントロール中のコンピュータとの接続を自動切断する設定手順

コンピュータを操作しない状態や、[リモートコントロール] ウィンドウの非アクティブ状態を監視し、一定の時間が経過すると自動的にコンピュータとの接続を切断できます。

自動切断を設定するには：

1. [リモートコントロール] ウィンドウのメニューでツールバーの [環境の設定] ボタンをクリックします。
2. 表示されるダイアログの [接続環境] タブで [自動切断する] をチェックして、無操作状態になってから切断されるまでの時間を設定します。

設定に従って、コンピュータを操作していない（送信データのない）状態になってから指定時間が経過したときに、自動的にコンピュータと切断されるようになります。

ポイント

切断したあと、[リモートコントロール] ウィンドウのメニューで [ファイル] - [再接続] を選択すると、そのウィンドウで直前に接続していたコンピュータに再接続できます。

ただし、コンピュータ側の設定によって、切断と同時にリモコンエージェントが自動的に終了する場合があります。その場合、リモコンエージェントを再起動したあとに再接続してください。

7.5.9 コントローラを終了する手順

リモートコントロールを終了するには、コントローラを終了します。

コントローラを終了するには：

1. [リモートコントロール] ウィンドウのメニューで [ファイル] - [終了] を選択します。

[リモートコントロール] ウィンドウが閉じて、リモートコントロールが終了します。コンピュータと接続中の場合は、自動的に切断されます。

複数のコンピュータと接続していて、[リモートコントロール] ウィンドウが複数起動している場合は、終了を実行したウィンドウだけが終了します。

ポイント

ウィンドウが複数起動している場合に、起動中のすべてのウィンドウを終了させたいときは、メニューで [ファイル] - [すべて終了] を選択してください。

7.5.10 接続モードを変更する手順

対象のコンピュータに対するリモートコントロールの内容に応じて、コントローラの接続モードを設定します。ただし、エージェント設定でコントローラよりも権限の高いモードを設定している場合は、接続時にコントローラのモードが変更になる場合があります。

接続モードを変更するには：

1. [リモートコントロール] ウィンドウのメニューで [ツール] - [接続モード] を選択します。
2. 下位項目の [監視モード]、[共有モード]、または [制御モード] を選択します。

接続モードが変更されます。

設定された接続モードは、[リモートコントロール] ウィンドウのステータスバー、またはツールバーで確認できます。

なお、接続モードは、ツールバーの [環境の設定] ボタンをクリックして表示されるダイアログの [接続環境] タブからも変更できます。

7.5.11 電源が OFF のコンピュータをリモートコントロールする手順

コントローラで、電源が OFF のコンピュータに接続する場合、コンピュータの電源を ON にして接続できます。電源を ON にしてコンピュータに接続するためには、コントローラの環境設定が必要です。

ポイント

デフォルトでは、コンピュータの電源を ON にして接続できる設定が有効になっています。

電源を ON にしてコンピュータに接続するには：

1. [リモートコントロール] ウィンドウのメニューでツールバーの [環境の設定] ボタンをクリックします。
2. 表示されるダイアログの [接続環境] タブで [対象のコンピュータの電源が OFF の場合、自動的に電源を ON にする] をチェックします。

コンピュータの電源が OFF の場合に、電源を ON にして接続できるようになります。

7.5.12 リモートコントロール中のコンピュータの電源を OFF にする手順

コントローラからの指示で、コンピュータの電源を OFF にできます。

注意事項

RFB で接続しているコンピュータは、コントローラから電源を OFF にできません。操作画面の機器画面から電源を OFF にしてください。詳細については、「[6.23 コンピュータの電源を制御する手順](#)」を参照してください。

接続先のコンピュータの電源を OFF するには：

1. [リモートコントロール] ウィンドウのメニューで [ツール] - [シャットダウン] を選択します。

接続先のコンピュータの電源が OFF になります。

7.5.13 リモートコントロール中のコンピュータを再起動する手順

コントローラからの指示で、コンピュータを再起動できます。リモコンエージェントが自動起動するように設定されている場合は、しばらく待ったあと管理用サーバから接続を開始することで、リモートコントロールを続行できます。

注意事項

RFB で接続しているコンピュータは、コントローラから再起動できません。操作画面の機器画面から再起動してください。詳細については、「[6.23 コンピュータの電源を制御する手順](#)」を参照してください。

接続先のコンピュータを再起動するには：

1. [リモートコントロール] ウィンドウのメニューで [ツール] - [再起動] を選択します。
2. 表示されるダイアログで、再起動後の動作を設定して [OK] ボタンをクリックします。

接続先のコンピュータが再起動します。

ポイント

[再起動] メニューを選択すると表示されるダイアログで、再起動後に接続するように設定すると、コンピュータが再起動したあとで自動的にリモートコントロールを再開できます。

7.5.14 リモートコントロール中に [Ctrl] + [Alt] + [Delete] キーを入力する手順

接続先のコンピュータに対して、キーボードから直接 [Ctrl] + [Alt] + [Delete] キーは入力できません。[Ctrl] + [Alt] + [Delete] キーを入力したい場合は、専用のメニューを利用します。

[Ctrl] + [Alt] + [Delete] キーを入力するには：

1. [リモートコントロール] ウィンドウで、[Ctrl+Alt+Del] ボタン () をクリックします。

接続先のコンピュータに、[Ctrl] + [Alt] + [Delete] キーと同様の操作を実行できます。

なお、[リモートコントロール] ウィンドウのメニューで [ツール] - [Ctrl+Alt+Del を送信] を選択しても、同様の操作ができます。

7.5.15 コントローラに特殊キーを登録する手順

対象のコンピュータに特殊キーを入力するためには、あらかじめ特殊キーを登録しておく必要があります。

特殊キーを登録するには：

1. [リモートコントロール] ウィンドウのメニューで [表示] - [キーボードの入力バー] - [キーボードの設定] を選択します。
2. 表示されるダイアログで特殊キーを設定し、[OK] ボタンをクリックします。

特殊キーが登録されます。

ポイント

次の4種類のキーは、コントローラで入力すると対象のコンピュータで実行できるよう設定できます。

- [Windows]
- [Ctrl] + [Esc]
- [Alt] + [Esc]
- [Alt] + [Tab]

これらのキーの入力を対象のコンピュータで実行するには、[リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタンをクリックして表示されるダイアログで、[高度な設定] タブの [対象のコンピュータでシステムキーの入力を実行する] をチェックしてください。

7.5.16 リモートコントロール中に特殊キーを入力する手順

対象のコンピュータに特殊キーを入力するには、キーボードの入力バーを利用します。キーボードの入力バーには、あらかじめ登録した特殊キーが表示されます。

特殊キーを入力するには：

1. [リモートコントロール] ウィンドウのメニューで [表示] - [キーボードの入力バー] - [キーボードの入力バー] を選択します。
キーボードの入力バーが表示されます。
2. キーボードの入力バーでボタンをクリックします。

クリックしたボタンに登録された特殊キーが、接続先のコンピュータに送信されます。

7.5.17 リモートコントロール中の送受信データを暗号化する手順

リモートコントロール時に、コンピュータと送受信するデータ（クリップボードのデータを含む）を暗号化できます。暗号化することで、コントローラとリモコンエージェント間でデータの内容が第三者から守られます。

送受信データを暗号化するには：

1. [リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタンをクリックします。
2. 表示されるダイアログの [高速化] タブで、[転送データを暗号化する] をチェックし、[OK] ボタンをクリックします。

リモートコントロール中の送受信データが暗号化されます。

送受信データの暗号化を設定すると、ステータスバーの送受信アイコンにかぎのアイコンが表示されます。

7.5.18 コントローラのウィンドウに合わせてコンピュータの画面を拡大、縮小する手順

コントローラのウィンドウサイズは、接続先のコンピュータの画面の解像度に応じて自動的に変化します。コンピュータの画面を操作しやすくするため、コンピュータの画面をウィンドウに合わせて拡大または縮小して表示できます。

コントローラのウィンドウに合わせてコンピュータの画面を拡大、縮小するには：

1. [リモートコントロール] ウィンドウのツールバーで [サイズ自動調整] ボタンをクリックします。

対象のコンピュータの画面が、コントローラのウィンドウサイズに合わせて拡大または縮小されて表示されます。再度ボタンをクリックすると、拡大、縮小されなくなります。

コンピュータの画面を等倍表示に戻す場合は、ツールバーの [自動調整を取消] ボタンをクリックします。

7.5.19 フルスクリーン表示で機器をリモートコントロールする手順

コントローラをフルスクリーン表示して、コンピュータを直接操作するのと同じ感覚で、接続先のコンピュータをリモートコントロールできます。

フルスクリーン表示でコンピュータをリモートコントロールするには：

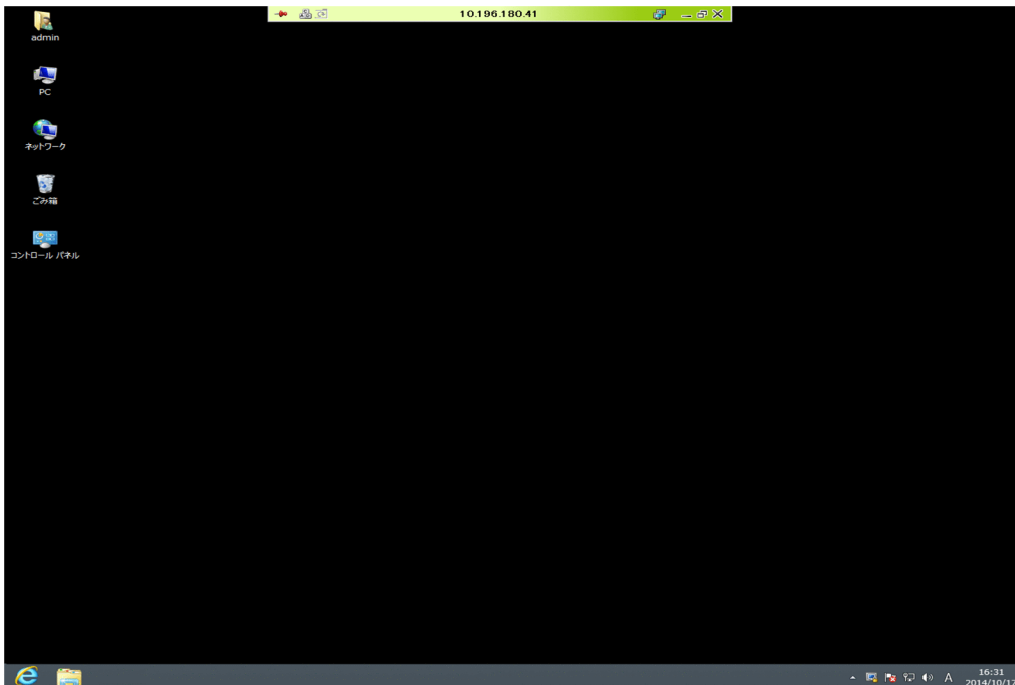
1. [リモートコントロール] ウィンドウのツールバーから  を選択します。

コントローラがフルスクリーン表示に切り替わります。

ポイント

解像度を変更できないなどの理由で、フルスクリーンで表示できないことがあります。

フルスクリーン表示中にマウスカーソルを画面上部へ移動させると、メニューバーが表示されます。このメニューバーから、画面表示状態を設定したり、接続先のコンピュータに [Ctrl] + [Alt] + [Delete] キーと同様の操作を実行したりできます。マウスカーソルを画面上部から遠ざけると、メニューバーは消えますが、常にメニューバーを表示させるように設定することもできます。



メニューバーの色は、接続モードに応じて変化します。そのため、メニューバーの色を見るだけで、現在の接続モードを確認できます。

- 緑色の場合：制御モード
- 黄色の場合：共有モード
- オレンジ色の場合：監視モード

なお、フルスクリーンモードを解除する場合は、メニューバーから実行します。

7.5.20 複数のコントローラの画面を整列表示させる手順

複数のコンピュータをリモートコントロールしている場合、操作しやすいようにコントローラを整列して表示できます。

複数のコントローラの画面を整列表示させるには：

1. [リモートコントロール] ウィンドウのメニューで、[ウィンドウ] – [上下に並べて整列]、[左右に並べて整列]、または [左上から順に整列] を選択します。

選択したメニューに従って、コントローラが整列されます。[左上から順に整列] を選択した場合は、コンピュータの画面が上下左右で均等に配置されます。

7.5.21 コントローラのバーの表示を切り替える手順

ツールバー、アドレスバー、およびキーボードの入力バーの表示、非表示を切り替えられます。各バーを非表示にすることで、コンピュータ画面の表示領域が拡大し、操作しやすくなります。

バーの表示を切り替えるには：

1. [リモートコントロール] ウィンドウのメニューで、[表示] – [ツールバー] – [ツールバー] を選択します。

ステータスバーの場合は [表示] – [ステータスバー] – [ステータスバー] を、キーボードの入力バーの場合は [表示] – [キーボードの入力バー] – [キーボードの入力バー] を選択してください。

メニューがチェックされている場合に、バーが表示されます。

ポイント

ツールボタンの文字列の表示、非表示を切り替えることもできます。ボタンの文字列の表示を切り替えるには、[表示] メニューで [ツールバー] – [ボタンラベル] を選択します。

7.5.22 オートスクロールでリモートコントロールする手順

コントローラのウィンドウよりもコンピュータの画面が大きい場合、コントローラにスクロールバーが表示されます。このとき、マウスカーソルを画面の端に近づけると、自動的にコンピュータの画面がスクロールされるようにするオートスクロール機能を利用できます。

オートスクロールを利用するには：

1. [リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタンをクリックします。
2. 表示されるダイアログの [高度な設定] タブで、[マウスポインタでスクロールする] をチェックします。

3. オートスクロールの方法を選択して、[OK] ボタンをクリックします。

オートスクロール機能が有効になります。

なお、オートスクロールの方法は、次の 2 種類から選択できます。

- ・ 常時：マウскарソルをウィンドウの端に近づけたとき、常に自動的に画面をスクロールさせる
- ・ ドラッグ時：ドラッグしているときだけ、自動的に画面をスクロールさせる

7.5.23 リモートコントロール中のマウスホイールでのスクロールを制御する手順

接続先のコンピュータの画面上のウィンドウに対して、マウスホイールを使用してスクロールできます。

ただし、コントローラにも、接続先のコンピュータの画面にもスクロールバーが表示されているような場合、マウスホイールを使用すると、両方のウィンドウが同時にスクロールされてしまい操作しづらくなります。これを防ぐために、マウスホイールを使用したときの動作を制御できます。

マウスホイールでのスクロールを制御するには：

1. [リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタンをクリックします。
2. 表示されるダイアログの [高度な設定] タブで、[ホイールスクロールを無効にする] をチェックして [OK] ボタンをクリックします。

コントローラに対するマウスホイールの操作が無効になり、接続先のコンピュータの画面内だけがスクロールされるようになります。

ポイント

リモートコントロール機能の各ウィンドウは、マウスホイールを使用してスクロールできます。ホイールを回転させると、垂直方向にスクロールできる場合は垂直方向に、水平方向にスクロールできる場合は水平方向にスクロールされます。また、[リモートコントロール] ウィンドウでは、垂直および水平の両方向にスクロールできる状態のとき、[Shift] キーを押しながらホイールを回転させると、水平方向にスクロールできます。

7.5.24 リモートコントロール中の画面を画像として保存する手順

リモートコントロール中のコンピュータ画面を、BMP ファイルに保存できます。リモートコントロール中にエラーメッセージが表示された状況を保存しておき、あとでエラー要因を分析したり、手順書を作成する際に画面図を採取したりするために利用できます。

コンピュータの画面を保存するには：

1. [リモートコントロール] ウィンドウのメニューで [ファイル] – [スクリーンを保存] を選択します。
2. 表示されるダイアログで保存するファイル名と保存先を指定します。

保存するファイルの色数を指定できます。デフォルトは、コンピュータの画面の色数となります。

操作中の画面が BMP ファイルとして保存されます。

7.5.25 リモート CD-ROM を利用する手順

コントローラ側のコンピュータの CD/DVD ドライブ（ドライブ種別が CD-ROM のドライブ）を、接続先のコンピュータのドライブとして利用できます。リモートコントロール中にファイル転送することなく CD-ROM からソフトウェアをインストールしたり、RFB で接続する場合に、ブートドライブにリモート CD-ROM のドライブを指定して OS の修復作業に当たったりできます。

注意事項

リモート CD-ROM 機能を利用する場合、接続先のコンピュータが AMT の IDE-R 機能を利用できる必要があります。接続方法は、標準接続と RFB での接続の両方で利用できます。

リモート CD-ROM を利用するには：

1. [リモートコントロール] ウィンドウのメニューで、[ツール] – [CD/DVD のマウント] を選択します。

コントローラ側の CD/DVD ドライブが、接続先のコントローラのドライブとして利用できるようになります。このとき、メニューの項目名に続いて、接続先名と接続先でのドライブ名が表示されます。

リモート CD-ROM を解除するには、メニューで [ツール] – [CD/DVD のアンマウント] を選択してください。

ポイント

リモートコントロールの接続が切断された状態でも、リモート CD-ROM をマウントした状態を保てます。これによって、接続先のコンピュータ起動時にブートドライブとして、リモート CD-ROM のドライブを利用できます。

7.5.26 [リモートコントロール] ウィンドウから接続できるコンピュータを検索する手順

[リモートコントロール] ウィンドウから、ネットワーク上に接続できるコンピュータがあるかどうかを検索できます。検索されたコンピュータに接続して、リモートコントロールを開始できます。

[リモートコントロール] ウィンドウからコンピュータを検索するには：

1. [リモートコントロール] ウィンドウの [接続] ボタンから [接続] を選択します。
2. 表示されるダイアログで [コンピュータを検索] ボタンをクリックします。
3. 表示されるダイアログで、検索したい IP アドレスの範囲を設定します。
4. [検索] ボタンをクリックします。

コンピュータの検索が開始され、検索状況が表示されます。

検索されたコンピュータのうち「接続待ち」状態のコンピュータを選択して [接続] ボタンをクリックすると、リモートコントロールを開始できます。

なお、検索されたコンピュータと接続すると、それ以外の検索されたコンピュータの情報はすべて削除されます。検索結果を保存しておきたい場合は、接続リストからコンピュータを検索することをお勧めします。

関連リンク

- [7.5.27 接続リストからリモートコントロールできるコンピュータを検索する手順](#)

7.5.27 接続リストからリモートコントロールできるコンピュータを検索する手順

接続リストから、ネットワーク上に接続できるコンピュータがあるかどうかを検索できます。検索されたコンピュータに接続して、リモートコントロールを開始できます。

接続リストからコンピュータを検索するには：

1. [リモートコントロール] ウィンドウのメニューで、[接続リスト] - [接続リストを編集] を選択します。
2. 表示された接続リスト上で、[ネットワーク] アイコンを作成する位置を選択します。

ポイント

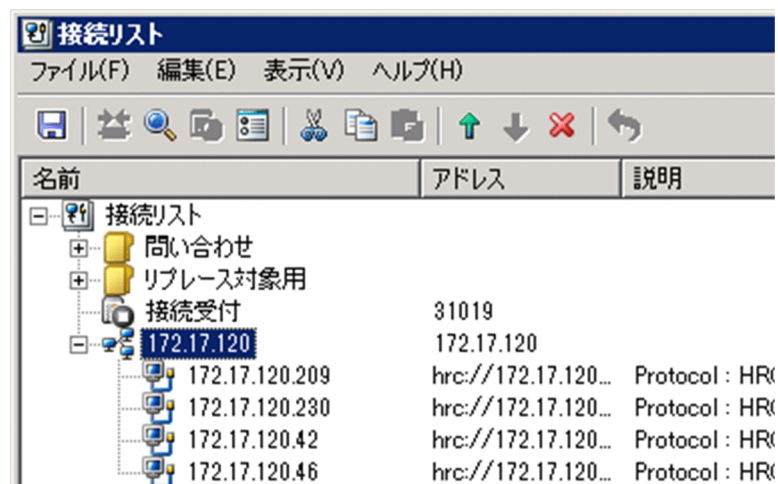
[ネットワーク] アイコンとは、エージェントを検索するときの検索範囲を設定したアイコンです。[ネットワーク] アイコン 1 つにつき、同一サブネット内に存在する任意の範囲のアドレス

を指定できます。[ネットワーク] アイコンを接続リスト上に作成しておくことで、同じ範囲を繰り返し検索できます。また、[リモートコントロール] ウィンドウの[接続できるコンピュータの検索] ダイアログからリモートコントロールできるコンピュータを検索できます。

3. 接続リストのメニューで、[ファイル] - [新規作成] から [ネットワーク] を選択します。
4. 表示されるダイアログでネットワークの名前と IP アドレスの範囲を設定して、[OK] ボタンをクリックします。
5. 作成した [ネットワーク] アイコンをダブルクリックします。

コンピュータの検索が開始され、検索状況を示す [接続できるコンピュータの検索] ダイアログが表示されます。

検索が完了したあと [接続できるコンピュータの検索] ダイアログを閉じると、ダイアログの [コンピュータ] タブに表示されていたコンピュータが、[ネットワーク] アイコンの下位に追加されます。検索途中で [閉じる] ボタンをクリックしても、それまでに検出されたコンピュータが追加されます。



↑
検索されたコンピュータ

ポイント

接続リストには、[接続できるコンピュータの検索] ダイアログの [コンピュータ] タブに表示されているコンピュータだけが追加されます。このため、検索が完了したあと、ダイアログを閉じる前にアイコンをチェックして、接続リストに追加するコンピュータが [コンピュータ] タブに表示されている状態にしてください。例えば、接続できるかどうかに関係なく、ネットワーク上の全コンピュータの構成を接続リスト上で管理したい場合は、「接続待ち」から「無応答」まですべての項目をチェックする必要があります。逆に、現時点で接続できるコンピュータだけを接続リストに追加したい場合は、「接続待ち」だけをチェックします。

なお、検索されたコンピュータは、検索結果が一時的に表示されたもので、このままでは情報として保存されません。接続リストを閉じると削除されます。検索されたコンピュータの情報を保存したい場合は、ドラッグ&ドロップで別のグループへ移動させる必要があります。グループ下に移動されることで、接続リスト上のコンピュータとして扱えるようになり、名前や説明を変更できます。

7.5.28 リモートコントロール接続できるコンピュータの検索方法をカスタマイズする手順

接続できるコンピュータを検索するときの、名前解決の有無や接続確認の方法など、検索方法をカスタマイズできます。

エージェントの検索方法をカスタマイズするには：

[リモートコントロール] ウィンドウから検索する場合

[接続できるコンピュータの検索] ダイアログで [設定] ボタンをクリックすると、[コンピュータの検索の設定] ダイアログが表示されます。このダイアログで、検索方法をカスタマイズします。

接続リストから検索する場合

次に示すダイアログで、検索方法をカスタマイズできます。設定内容は、[コンピュータの検索の設定] ダイアログと同様です。ただし、接続リストでは、検索されたコンピュータのエージェントの接続オプションも設定できます。

- ・ ネットワークを新規作成するときに表示される [新しいネットワークの作成] ダイアログの [接続先の設定] タブ
- ・ ネットワークのプロパティで表示される [プロパティ] ダイアログの [接続先の設定] タブ
- ・ フォルダや複数アイテムの [プロパティ] ダイアログから表示したネットワークの [接続環境の設定] ダイアログ

7.6 ファイル転送を利用する

7.6.1 [ファイル転送] ウィンドウを起動する手順

[ファイル転送] ウィンドウを起動するには、コンピュータと接続している必要があります。

[ファイル転送] ウィンドウを起動するには：

1. [リモートコントロール] ウィンドウのツールバーで [ファイル転送] ボタン () をクリックします。

[ファイル転送] ウィンドウが起動します。メニューの [ツール] - [ファイル転送] からでも起動できます。

ポイント

コントローラに表示されているコンピュータの画面に、ファイルをドラッグ&ドロップしてファイルを転送することもできます。この場合、[ファイル転送] ウィンドウが起動したあとすぐにファイルの転送が開始されます。

関連リンク

- [7.6.3 \[ファイル転送\] ウィンドウを終了する手順](#)

7.6.2 ファイル転送の接続を切断する手順

コンピュータとのファイル転送用の接続を切断できます。ファイル転送用の接続は、コンピュータをログオフした場合も切断されます。なお、ファイル転送用の接続を切断しても、リモートコントロールの接続は切断されません。

ファイル転送の接続を切断するには：

1. [ファイル転送] ウィンドウのメニューで [ファイル] - [切断] から、切断するコンピュータを選択します。

ファイル転送用の接続が切断されます。

ただし、ファイルが転送中または削除中の場合、処理は中断されます。

注意事項

リモートコントロールの接続が切断されると、ファイル転送用の接続は自動的に切断されます。

注意事項

接続モードが監視モードに変更された場合も、該当するコンピュータとのファイル転送用の接続は切断されます。このときファイルが転送中または削除中だった場合は、処理を中断するかどうかを確認するダイアログが表示されます。

7.6.3 【ファイル転送】 ウィンドウを終了する手順

ファイル転送が完了したら、ファイル転送用の接続は切断してかまいません。切断するには、【ファイル転送】 ウィンドウを終了します。

【ファイル転送】 ウィンドウを終了するには：

1. 【ファイル転送】 ウィンドウのメニューで、【ファイル】－【ファイル転送の終了】を選択します。

【ファイル転送】 ウィンドウが終了します。

ウィンドウを終了すると、ファイル転送用の接続はすべて自動的に切断されます。ただし、終了時にファイルが転送中または削除中の場合、処理は中断されます。

7.6.4 ファイル転送先のコンピュータを追加する手順

【ファイル転送】 ウィンドウを起動すると、ウィンドウを起動したコントローラの接続先のコンピュータが、ツリービューに表示されます。ツリービューにコンピュータを追加して、複数のコンピュータとファイルの転送ができます。

なお、【ファイル転送】 ウィンドウに追加できるのは、リモートコントロール中のコンピュータだけです。また、コンピュータが OS にログオンしている必要があります。

ファイル転送先のコンピュータを追加するには：

1. 任意のコンピュータと接続しているコントローラで 【ファイル転送】 ウィンドウを起動します。

既存のウィンドウにコンピュータが追加されていきます。【ファイル転送】 ウィンドウは複数起動されません。

7.6.5 転送するファイル情報を確認する手順

【ファイル転送】 ウィンドウで選択中のファイルや、【編集】メニューからコピーファイルまたは移動ファイルに指定したファイルの、詳細情報や合計サイズを確認できます。ファイル情報を確認するためには、【ファイルの確認】ダイアログを表示します。

選択ファイルの情報を確認するには：

1. ファイルまたはフォルダを選択し、[ファイル転送] ウィンドウのメニューで [編集] - [ファイルを確認] から [選択ファイル] を選択します。

予約ファイルの情報を確認するには：

1. [ファイル転送] ウィンドウのメニューで、[編集] - [ファイル確認] から [予約ファイル] を選択します。
[予約ファイル] メニューは、コピーファイルまたは移動ファイルを予約すると活性化されます。
2. [OK] ボタンをクリックすると、ファイルの確認を終了します。

[削除] ボタンで予約ファイルを取り消した場合、[OK] ボタンをクリックした時点で取り消しが有効になります。[キャンセル] ボタンをクリックすると、[削除] ボタンでの取り消しは無効になります。

なお、[ファイルの確認] ダイアログでは、ファイルの転送種別を変更できます。選択ファイルの情報を確認している場合、[種別] を「選択」から「コピー」または「移動」に変更することで、コピーファイルや移動ファイルとして予約できます。また、予約ファイルの情報を確認している場合は、予約の内容（コピーまたは移動）を変更できます。

7.6.6 ファイル転送時のセキュリティ設定をする手順

安全にファイルを転送するために、セキュリティの設定ができます。ファイル転送でのセキュリティには、次の 2 種類があります。

- 転送データの暗号化
ネットワーク上に転送されるデータは、そのままでは第三者によって内容が漏えいするおそれがあります。そこで、データを暗号化することで、コントローラとリモコンエージェント間でのファイルの内容を、第三者から守れます。
- ファイルへのアクセス権の設定
[ファイル転送] ウィンドウでは、コントローラからも対象のコンピュータと同じアクセスができます。このため、業務用のサーバで誤ってファイルを操作してしまうことなどを防ぐために、コントローラからのアクセス権を設定できます。

転送データを暗号化するには：

1. [リモートコントロール] ウィンドウのツールバーで [環境の設定] ボタン () をクリックします。
2. 表示されるダイアログの [高速化] タブで、[転送データを暗号化する] をチェックして [OK] ボタンをクリックします。

転送されるデータが暗号化されます。

なお、暗号化を設定すると、コントローラとコンピュータにかぎのアイコンが表示されます。

ファイルへのアクセス権を設定するには：

1. エージェント設定の [リモートコントロールの設定] で [ファイルへのアクセス権] を設定します。

設定したアクセス権に従って、コントローラ側からのファイルへのアクセスが制限されます。

アクセス権には読み取りと書き込みがあります。これらのアクセス権の設定によって、実行できるファイル操作が異なります。例えば、読み取りの権限だけ設定した場合、コンピュータにファイルを送信しようとするエラーメッセージが表示されます。

7.6.7 ファイルを転送する手順

[ファイル転送] ウィンドウでは、コントローラとコンピュータとの間で、双方向のファイル転送ができます。また、複数のコンピュータと接続している場合に、接続先のコンピュータ間でファイル転送することもできます。

[ファイル転送] ウィンドウでのファイルの転送方法には、大きく分けて 3 種類の方法があります。ここでは、それぞれの操作方法について説明します。

ドラッグ&ドロップで転送するには：

[ファイル転送] ウィンドウ上のファイルおよびフォルダを、ドラッグ&ドロップで転送できます。ファイルをドラッグ&ドロップするとコピーされます。ファイルを移動する場合は [Shift] キーを押しながらドロップしてください。また、マウスの右ボタンでドラッグすると、ドロップしたときにメニューが表示され、[移動]、[コピー]、[キャンセル] の 3 つから動作を選択できます。

さらに、システムのエクスプローラと [ファイル転送] ウィンドウの間でも、ファイルをドラッグ&ドロップで転送できます。この場合はすべてコピーとなり、[Shift] キーを押しても無効になります。

ファイルを登録して転送するには：

1. 転送するファイルまたはフォルダを選択し、[ファイル転送] ウィンドウのツールバーで [コピーファイル予約] ボタン () または [移動ファイル予約] ボタン () をクリックします。
2. 転送先のドライブまたはフォルダを選択し、ツールバーの [転送] ボタン () をクリックします。

ファイルの転送が始まります。

マルチ転送するには：

マルチ転送とは、複数のコンピュータに一度にファイルを転送できる方法です。転送先のフォルダはデフォルトで設定したり、転送元と同じフォルダを設定したりできるので、フォルダを入力する手間を省けます。

1. 転送するファイルまたはフォルダを選択し、[ファイル転送] ウィンドウのツールバーで [マルチ転送] ボタン () をクリックします。
2. 表示されるダイアログで転送先コンピュータおよび転送先フォルダを設定し、[転送] ボタンをクリックします。

ファイルの転送が始まります。複数のコンピュータを選択した場合は、それぞれのコンピュータの同一フォルダに一斉に転送されます。

7.6.8 リモートコントロール中のコンピュータのファイルの操作手順

コントローラでコンピュータのファイル进行操作する場合、コンピュータの画面を呼び出して操作するほかに、[ファイル転送] ウィンドウを利用することもできます。

[ファイル転送] ウィンドウからコンピュータのファイルを開くと、そのファイルはコンピュータからコントローラに転送されます。ファイルの編集時にコンピュータの利用者に影響を与えることはありません。ファイルの受信先は、[ファイル転送] ウィンドウのオプションで設定したフォルダとなります。

複数のコンピュータから同じ名称のファイルを開いた場合は、開いた順序でコントローラがファイルを受信します。このとき、前回受信したファイルを上書きして受信するので、最後に受信したファイルを開くこととなります。

[ファイル転送] ウィンドウからコンピュータのファイルを編集するには：

1. [ファイル転送] ウィンドウでコンピュータのファイルを選択し、メニューで [ファイル] - [開く] を選択します。

ポイント

ファイルをダブルクリックして開くこともできます。

2. 表示されたファイルを編集します。
3. 編集終了後、ファイルを閉じます。
4. 表示されるダイアログで [はい] ボタンをクリックします。

コントローラ上で編集したファイルがコンピュータの元の場所に転送され、元のファイルを上書きします。

ファイルの転送と削除を自動的に処理したり、コントローラ上にファイルを残すようにしたりしたい場合は、ツールバーの [環境の設定] ボタンをクリックして表示されるダイアログの [ファイル] タブで、リモートファイルの設定を変更してください。

なお、ファイルの転送と削除の自動処理を設定していない場合は、ファイルを閉じるとコントローラのファイルは転送されないで一時フォルダに残ります。

手動でファイルを転送および削除するには：

［ファイル転送］ ウィンドウからコンピュータのファイルを開いた場合、コントローラにそのファイルが一時的に保存されます。また、ファイルの転送と削除の自動処理を設定していない場合は、ファイルを閉じてでもコントローラのファイルは転送されないで残ります。

これらコントローラに残っているファイルは、リモートファイルの一覧の［ファイル転送］ ウィンドウで確認できます。このウィンドウから、コントローラに残っているファイルをコンピュータに転送したり、コントローラから削除したりできます。

1. [ファイル転送] ウィンドウのメニューから、[表示] - [リモートファイルの一覧] を選択します。
2. リモートファイルの一覧の [ファイル転送] ウィンドウのメニューで、[編集] - [転送] または [転送後に削除] を選択します。

編集終了したファイルが、コンピュータの元の場所に転送されます。

［転送］ を選択した場合はコピーと同様の処理となり、コントローラにファイルが残ります。［転送後に削除］ を選択した場合は移動と同様の処理となり、コントローラにファイルは残りません。

なお、ファイルをコントローラから削除する場合は、[ファイル] - [削除] メニューを選択してください。削除状況を示すダイアログが表示され、コントローラに保存されたファイルが削除されます。

関連リンク

- [7.6.10 ファイル転送のオプションを設定する手順](#)

7.6.9 [ファイル転送] ウィンドウからファイルを編集する手順

［ファイル転送］ ウィンドウを使用すると、ファイルの転送以外に、コントローラおよび接続先コンピュータのフォルダやファイルに対して次の操作ができます。ただし、対象となるフォルダやファイルに対するアクセス権がなければ操作できません。

- フォルダの作成
- フォルダおよびファイルの削除
- フォルダおよびファイルの属性変更
- フォルダおよびファイルの名前の変更

フォルダを作成するには：

1. 新しいフォルダを作成する場所（ドライブまたはフォルダ）を選択します。
2. ツールバーの [新規作成] ボタン () をクリックします。
3. フォルダ名を入力します。

選択した場所に、新規にフォルダが作成されます。

フォルダおよびファイルを削除するには：

1. 削除するフォルダまたはファイルを選択します。
2. ツールバーの [削除] ボタン () をクリックします。

ポイント

キーボードの [Delete] キーを押しても削除できます。

3. 表示されるダイアログで、[はい] ボタンまたは [すべて削除] ボタンをクリックします。

選択したフォルダまたはファイルが削除されます。コントローラでは、削除状況を表すダイアログが表示されます。

フォルダおよびファイルの属性を変更するには：

1. 属性を変更したいフォルダまたはファイルを選択します。
2. [ファイル] - [プロパティ] メニューを選択します。
3. 表示されるダイアログで必要な属性を設定し、[OK] ボタンをクリックします。

設定した内容で属性が変更されます。属性が変更されるのは、選択しているフォルダまたはファイルです。選択したフォルダ下のファイルまたはフォルダの属性は変更されません。

フォルダおよびファイルの名称を変更するには：

1. 名称を変更したいフォルダまたはファイルを 1 つ選択します。
2. 名称部分をもう一度クリックします。または [ファイル転送] ウィンドウのメニューで、[ファイル] - [名前の変更] を選択します。
3. 名称を入力します。

フォルダまたはファイルの名称が変更されます。

7.6.10 ファイル転送のオプションを設定する手順

[ファイル転送] ウィンドウで効率良く操作するために、[環境の設定] ダイアログでオプションを設定することをお勧めします。オプションでは、表示するファイルの種類やファイル転送完了時の動作などを設定できます。

ファイル転送のオプションを設定するには：

1. [ファイル転送] ウィンドウのツールバーで [環境の設定] ボタン () をクリックします。
2. 表示されるダイアログでオプションを設定したあと、[OK] ボタンをクリックします。

設定した内容が保存されます。

[環境の設定] ダイアログの設定項目を次に示します。

- [表示] タブ
[表示] タブでは、[ファイル転送] ウィンドウの表示に関するオプションを設定します。
- [ファイル] タブ
[ファイル] タブでは、コンピュータのファイルを開いたとき、および閉じたときの動作について設定します。

7.7 接続リストを利用する

7.7.1 コンピュータごとの接続環境を設定する手順

コンピュータごとに接続環境を設定できます。これによって、毎回環境を変更することなく、適切な設定でコンピュータと接続できるようになります。

1 台のコンピュータに接続環境を設定するには：

1. 接続環境を設定するコンピュータを選択します。
2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されるダイアログの [設定] タブで [接続環境を設定する] をチェックします。
4. 必要なオプションを設定し、[OK] ボタンをクリックします。
項目によっては、選択すると [詳細] 欄に詳細設定項目が表示されるので、これらも設定してください。

選択したコンピュータに接続環境が設定されます。次回以降、ここで設定した接続環境でコンピュータと接続します。

複数のコンピュータの接続環境を設定するには：

複数のコンピュータに同じ条件で接続したい場合、一括して接続環境を設定できます。

1. 接続環境を設定する複数のコンピュータを選択します。
2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されるダイアログの [設定] タブで、[接続先コンピュータ] の [設定] ボタンをクリックします。
4. 表示されるダイアログで [接続環境を設定する] をチェックします。
5. 必要なオプションを設定し、[OK] ボタンをクリックします。

選択した複数のコンピュータに、接続環境が設定されます。

グループやネットワーク下の複数のコンピュータに接続環境を一括設定する場合は、[グループ] アイコンまたは [ネットワーク] アイコンを選択して同様の操作をしてください。

検索されたコンピュータに接続環境を設定するには：

ネットワーク検索で検索されたコンピュータに、特定の接続環境を設定できます。この場合、検索されたコンピュータではなく、検索に使用したネットワークに対して接続環境を設定します。検索されたコンピュータには接続環境を設定できません。接続環境は、検索実行前にも設定できます。

1. ネットワークを選択します。

2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されるダイアログの [接続先の設定] タブで [接続できるコンピュータ発見時の動作] の [設定] ボタンをクリックします。
4. 表示されるダイアログで、[接続環境を設定する] をチェックします。
5. 必要なオプションを設定し、[OK] ボタンをクリックします。

検索コンピュータに設定する接続環境が保存されます。次回以降、検索されたコンピュータに、ここで設定した接続環境が適用されます。

リクエストエージェントに接続環境を設定するには：

リクエストエージェントからリモートコントロールを開始する場合の、接続環境を設定できます。この場合、リクエストエージェントではなく、リクエストサーバに対して接続環境を設定します。リクエストエージェントには、接続環境を設定できません。接続環境は、接続要求の受信前でも設定できます。

1. リクエストサーバを選択します。
2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されるダイアログの [設定] タブで [リクエストエージェント] の [設定] ボタンをクリックします。
4. 表示されるダイアログで、[接続環境を設定する] をチェックします。
5. 必要なオプションを設定し、[OK] ボタンをクリックします。

このリクエストサーバに接続したコンピュータ (リクエストエージェント) に対する接続環境が設定されます。

7.7.2 接続リストを表示・終了する手順

接続リストを表示するには：

接続リストの起動方法は、次の 2 とおりがあります。

- [リモートコントロール] ウィンドウのメニューで、[接続リスト] - [接続リストを編集] を選択する。
- [リモートコントロール] ウィンドウの [接続] ボタンをクリックして、表示されるメニューから [接続リストを編集] を選択する。

接続リストは、コンピュータと接続していない状態でも起動できます。また、接続リストから、コンピュータとの接続を指示することもできます。

接続リストを終了するには：

1. 接続リストのメニューで [ファイル] – [接続リストの終了] を選択します。

終了する前に接続リストの内容を編集していた場合は、変更を保存するかどうかを確認するダイアログが表示されます。接続リストを終了しないで内容の保存だけをする場合は、[ファイル] メニューから [保存] または [名前を付けて保存] を選択してください。

7.7.3 接続リストからコンピュータに接続する

接続リストに表示されているコンピュータのアイコンをダブルクリックすると、コンピュータに接続できます。検索されたコンピュータのアイコンからも接続できます。

また、リクエストエージェントのアイコンをダブルクリックすると、接続要求を出したコンピュータと接続できます。このとき、非活性となっている（接続要求がキャンセルされている）リクエストエージェントと接続することもできます。

コンピュータと接続すると、[リモートコントロール] ウィンドウのアドレスバーに、IP アドレス、ホスト名またはコンピュータのパスが記録されます。

7.7.4 接続リストを作成する手順

接続リストを作成する方法は複数あります。管理したいネットワークの規模や運用方法によって選択してください。

- [リモートコントロール] ウィンドウで接続中のコンピュータを追加する
- 接続リスト上で作成する
- コンピュータを検索して追加する
- hosts ファイルからインポートして作成する
- バックアップファイルを利用して作成する

なお、接続リスト上に各項目（グループ、コンピュータ、区切り線など）を作成する場合は、最初を選択した項目によって作成される位置が次のように異なります。

- ルートまたはグループを選択して作成した場合は、選択したルートまたはフォルダの下位階層の最後尾に作成されます。
- コンピュータまたは区切り線を選択して作成した場合は、選択したコンピュータまたは区切り線の次の位置（同じ階層）に作成されます。

[リモートコントロール] ウィンドウで接続中のコンピュータを追加するには：

1. [リモートコントロール] ウィンドウのメニューで [接続リスト] – [接続リストに追加] を選択します。

[接続] ボタンから [接続リストに追加] を選択してもかまいません。

2. [接続リストへの追加] ダイアログで、[接続リストの表示名] にコンピュータに付ける名称を指定します。

ここで指定した名称が、接続リストの [名前] 欄に表示されます。

3. 現在接続中のコンピュータの接続オプションを保存する場合は、[接続環境の設定も保存する] をチェックします。

コンピュータへの接続オプションの設定については、「[7.7.1 コンピュータごとの接続環境を設定する手順](#)」を参照してください。

4. [OK] ボタンをクリックします。

コンピュータが接続リストに追加されます。

接続リスト上で作成するには：

接続リストにコンピュータを追加します。接続リストでは、グループを作成してコンピュータをグルーピングしたり、コンピュータの構成を整理するための区切り線を作成したりできます。区切り線を作成すると [リモートコントロール] ウィンドウで [接続] ボタンをクリックしてメニューを表示させたときに、コンピュータの構成が見やすくなります。

グループ、コンピュータ、および区切り線を作成する手順を次に示します。

1. 接続リスト上で、グループ、コンピュータ、または区切り線を作成する位置を選択します。
2. 接続リストのメニューで、[ファイル] - [新規作成] から、[グループ]、[接続先コンピュータ]、または [区切り線] を選択します。
3. グループまたはコンピュータを作成する場合は、表示されるダイアログの [全般] タブと [設定] タブで情報を設定して、[OK] ボタンをクリックします。

なお、[設定] タブの情報はグループまたはコンピュータ作成後にも変更できます。

グループ、コンピュータ、または区切り線が接続リストに作成されます。

コンピュータを検索して追加するには：

接続リストからネットワーク上のコンピュータを検索し、接続できるコンピュータを接続リストに追加します。コンピュータを検索して接続リストに追加する手順は、大きく次の3段階に分けられます。

1. 検索したいアドレスの範囲を設定した [ネットワーク] アイコンを作成します。
2. [ネットワーク] アイコンを使用してコンピュータを検索します。
3. 検索されたコンピュータを接続リストに追加します。

検索範囲の指定方法や検索結果の確認方法、検索時の制限事項などについては、「[7.5.27 接続リストからリモートコントロールできるコンピュータを検索する手順](#)」を参照してください。

ポイント

[ネットワーク] アイコンとは、コンピュータを検索するときの検索範囲を設定したアイコンです。[ネットワーク] アイコン 1 つにつき、同一サブネット内に存在する任意の範囲のアドレスを指定できます。[ネットワーク] アイコンを接続リスト上に作成しておくことで、同じ範囲を繰り返し検索できます。また、[リモートコントロール] ウィンドウで、[接続] ボタンから表示される接続リストの [ネットワーク] アイコンを選択することで、[リモートコントロール] ウィンドウ上でもコンピュータを検索できます。

コンピュータを検索して接続リストに追加する手順を次に示します。

1. 接続リスト上で、[ネットワーク] アイコンを作成する位置を選択します。
2. 接続リストのメニューで、[ファイル] - [新規作成] - [ネットワーク] を選択します。
3. [新しいネットワークの作成] ダイアログの [全般] タブと [接続先の設定] タブで情報を設定して、[OK] ボタンをクリックします。
なお、[接続先の設定] タブの情報は [ネットワーク] アイコンを作成したあとにも変更できます。
4. 接続リスト上に作成された [ネットワーク] アイコンをダブルクリックします。
[接続できるコンピュータの検索] ダイアログが表示され、指定された範囲のコンピュータの検索が始まります。
5. 検索が完了したら、[詳細] ボタンをクリックして [コンピュータ] タブを表示します。
6. 接続リストに追加したいコンピュータだけが表示されるように、[コンピュータ] タブの表示内容を調整します。

ポイント

例えば、コンピュータが動作しているかどうかに関係なく、ネットワーク上の全コンピュータの構成を接続リスト上で管理したい場合は、[接続待ち] から [無応答] まですべての項目をチェックします。逆に、現時点で接続できるコンピュータだけを接続リストに追加したい場合は、「接続待ち」だけをチェックします。

7. [閉じる] ボタンをクリックします。

[接続できるコンピュータの検索] ダイアログの [コンピュータ] タブに表示されていたコンピュータが、[ネットワーク] アイコンの下位に追加されます。なお、検索途中で [閉じる] ボタンをクリックしても、それまでに検出されたコンピュータが追加されます。

注意事項

検索結果のコンピュータは、一時的に表示されたものです。接続リストを閉じると削除されます。検索されたコンピュータの情報を保存したい場合は、ドラッグ&ドロップで別のグループに移動してください。グループ下に移動することで、接続リスト上の 1 アイテムとして保存できます。保存すると、通常のコンピュータとして扱えるようになり、名前や説明を変更できます。

hosts ファイルからインポートして作成するには：

hosts ファイルを使用すると、hosts ファイルに定義されているすべてのコンピュータを一度に接続リストに追加できます。hosts ファイルからのインポートの手順を次に示します。

1. 接続リスト上で、コンピュータを追加する（hosts ファイルの情報を読み込む）位置を選択します。
2. 接続リストのメニューで、[ファイル] - [インポート] - [Hosts ファイルからのインポート] を選択します。
3. [ファイルを開く] ダイアログで hosts ファイルを選択して、[開く] ボタンをクリックします。

hosts ファイルに定義されているすべてのコンピュータが、接続リストに追加されます。なお、hosts ファイルの内容は、次の規則に従って処理されます。

- 先頭および後方のスペースおよびタブは無視する。
- 1 文字目が「#」の場合、コメントとして無視する。
- 最初のスペースまたはタブから次のスペースまたはタブまでを名前とする。
- エイリアス名は無視する。
- IP アドレスおよびホスト名が設定されている行に「#」がある場合、それ以降の文字列をコンピュータの説明とする。

バックアップファイルを利用して作成するには：

接続リストは、メニューの [ファイル] - [名前を付けて保存] を選択すると、任意の名称でバックアップファイルとして保存できます。

バックアップファイルをインポートすると、保存時の接続リストの項目を追加できます。バックアップファイルからのインポートの手順を次に示します。

1. 接続リスト上で、コンピュータを追加する（バックアップファイルの情報を読み込む）位置を選択します。
2. 接続リストのメニューで、[ファイル] - [インポート] - [管理ファイルからのインポート] を選択します。
3. [ファイルを開く] ダイアログでバックアップファイルを選択して、[開く] ボタンをクリックします。

指定した位置に、保存時の接続リストの情報が追加されます。

7.7.5 接続リストの項目を移動・コピーする

接続リストに表示されているネットワーク、グループ、コンピュータ、リクエストサーバ、および区切り線を移動・コピーできます。

接続リストの項目を移動またはコピーする方法には、次の3とおりがあります。なお、フォルダを移動またはコピーする場合は、フォルダに含まれる下位項目も対象になります。

- ドラッグ&ドロップで移動させる（[Ctrl] キーを押しながら操作することでコピーもできる）。
- ツールバーの「切り取り」ボタン、「コピー」ボタン、「貼り付け」ボタンを使用する。
- ツールバーの「上の項目に移動」ボタンまたは「下の項目に移動」ボタンを選択して移動させる。

開始状態のリクエストサーバを移動・コピーするときの注意

- 切り取りの場合、リクエストサーバの停止を確認するメッセージが表示されます。
- 移動の場合、移動後もそのまま開始している状態となります。
- コピーの場合、コピー先では停止状態となります。

7.7.6 接続リストの項目を削除する手順

接続リストに表示されているネットワーク、グループ、コンピュータ、リクエストサーバ、および区切り線を削除できます。

接続リストの項目を削除するには：

1. 接続リスト上で、削除する項目のアイコンを選択します。
2. ツールバーの「削除」ボタン（）をクリックします。

選択した項目が削除されます。

ポイント

[Delete] キーを押して削除することもできます。

なお、開始状態のリクエストサーバを削除しようとする、リクエストサーバの停止を確認するメッセージが表示されます。開始状態のリクエストサーバを下位に持つフォルダを削除する場合も、同様のメッセージが表示されます。

また、リクエストエージェントを削除すると、コンピュータの接続要求はキャンセルされます。

7.7.7 接続リストの項目名を変更する手順

接続リストに表示されているネットワーク、グループ、コンピュータ、およびリクエストサーバの名前を変更できます。

接続リストの項目名を変更するには：

1. 接続リスト上で、名前を変更する項目のアイコンを選択します。
2. 接続リストのメニューで、[ファイル] - [名前の変更] を選択します。
3. 変更後の名前を入力します。

選択した項目の名前が変更されます。

7.7.8 接続リストの項目の属性を変更する手順

接続リストに表示されているネットワーク、グループ、コンピュータ、およびリクエストサーバの属性を変更できます。

名前、アドレス（リクエストサーバの場合はポート番号）、および説明を変更できます。また、これらに加えて、次に示す属性を変更できます。

- ネットワークの場合
コンピュータの検索方法、および検索されたコンピュータの接続環境を変更できます。
- グループの場合
グループ下のコンピュータ、ネットワーク、およびリクエストサーバの属性を一括して変更できます。
- コンピュータの場合
接続環境を変更できます。
- リクエストサーバの場合
リクエストサーバの属性、および接続要求したコンピュータへの接続環境を変更できます。

接続リストの項目の属性を変更するには：

1. 接続リスト上で、属性を変更したい項目のアイコンを選択します。
複数のアイコンを選択して一括で変更することもできます。
2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されるダイアログで、必要に応じて設定内容を変更します。
4. [OK] ボタンをクリックします。

グループ選択時に下位のグループが存在する場合、または複数の項目を選択した場合は、下位のグループの属性も変更するかどうかを確認するメッセージが表示されます。

選択した項目の属性が変更されます。

なお、検索されたコンピュータおよび接続要求中のコンピュータ（リクエストエージェント）に対する属性の変更はできません。別のグループに移動させてから変更してください。

7.7.9 接続リストの項目を検索する手順

接続リストに表示されている項目を、名前、アドレス、および説明に含まれている文字列をキーとして検索できます。複数のキーを設定すると、すべてのキーに該当する項目が検索対象となります。

接続リストの項目を検索するには：

1. 検索のスタート地点とする項目のアイコンを選択します。
2. 接続リストのメニューで、[編集] - [項目の検索] を選択します。
3. 表示されるダイアログで、必要な項目を入力します。
4. [検索] ボタンをクリックします。

ダイアログが閉じ、最初に選択したアイコンを起点として下方向に検索が実行されます。検索条件に合致する 1 つ目のアイコンが選択状態（反転状態）になります。同じキーで検索を続ける場合は、メニューの [編集] - [次を検索]、または [F3] キーを押してください。

以降に該当する項目が存在しなくなると、[検索終了] ダイアログが表示されます。

7.7.10 接続リストの項目の属性を確認する手順

接続リストに表示されているネットワーク、グループ、コンピュータ、およびリクエストサーバの属性を確認できます。

接続リストの項目の属性を確認するには：

1. 接続リスト上で、属性を確認したい項目のアイコンを選択します。
2. ツールバーの [プロパティ] ボタン () をクリックします。

表示されるダイアログで、選択した項目の属性を確認できます。

7.7.11 リクエストサーバを作成する手順

エージェントからの接続要求を受信するには、接続リスト上にリクエストサーバが必要です。

リクエストサーバを作成するには：

1. 接続リスト上で、[リクエストサーバ] アイコンを作成する位置を指定します。
2. メニューの [ファイル] - [新規作成] - [リクエストサーバ] を選択します。
3. [新しいリクエストサーバの作成] ダイアログの [全般] タブで、[接続リストでの表示名]、[ポート番号]、および [説明] を入力します。
[ポート番号] には、エージェントからの接続時に使用するポート番号を指定します。デフォルトでは、「31019」が指定されています。
4. [設定] タブで、リクエストサーバの属性を設定します。なお、ここで設定しなくても、あとで設定することもできます。
5. [OK] ボタンをクリックします。

リクエストサーバが作成され、指定した位置に [リクエストサーバ] アイコン () が表示されます。

[リクエストサーバ] アイコンは、グループやコンピュータなどのほかのアイテムと同様に、名前や属性を変更できます。リクエストサーバの属性変更については、「[7.7.8 接続リストの項目の属性を変更する手順](#)」を参照してください。

関連リンク

- [7.7.12 リクエストサーバを開始または停止する手順](#)

7.7.12 リクエストサーバを開始または停止する手順

エージェントからの接続要求を受信するには、接続リストを表示し、リクエストサーバを開始しておく必要があります。リクエストサーバの開始と停止の状態は、アイコンの表示形態で確認できます。リクエストサーバの開始状態および停止状態のアイコンを次に示します。

 ：開始状態

 ：停止状態

リクエストサーバは、自動起動させる方法と手動起動させる方法があります。

リクエストサーバを開始するには（自動起動）：

1. 接続リスト上で [リクエストサーバ] アイコンを選択します。

2. ツールバーの [プロパティ] ボタン () をクリックします。
3. 表示されたダイアログの [設定] タブで、[接続リストが表示されたタイミングで開始する] をチェックします。

接続リストの表示時に、リクエストサーバが自動的に開始します。

リクエストサーバを開始するには (手動起動) :

1. 接続リスト上で [リクエストサーバ] アイコンを選択します。
2. ツールバーの [開始] ボタン () をクリックします。

選択したリクエストサーバが開始します。

なお、次の場合はエラーとなり、リクエストサーバを開始できません。

- リクエストサーバが使用するポート番号がすでに使用されている場合
- 前回接続リストから起動したコントローラがコンピュータと接続中の場合

リクエストサーバを停止するには :

1. 接続リスト上で [リクエストサーバ] アイコンを選択します。
2. ツールバーの [停止] ボタン () をクリックします。
3. リクエストサーバの停止を確認するメッセージダイアログで、[はい] ボタンをクリックします。

選択したリクエストサーバが停止します。

また、リクエストサーバが開始している状態で、リクエストサーバを切り取りまたは削除した場合にも、リクエストサーバは停止します。

7.8 録画機能を利用する

7.8.1 再生時にできる操作手順

録画ファイルの再生中に、詳しい説明をするため一時的に再生を中断したり、重点的に説明する部分だけを再生したりする場合があります。リモコンプレーヤーでは、目的に応じて再生を一時停止したり、再生の一部をスキップしたりして、再生をコントロールできます。また、録画を再生するときに、早送りにしたり、スロー再生にしたりして、再生速度を変更できます。再生時にできる操作を次に示します。

再生を停止するには：

1. リモコンプレーヤーのツールバーで [停止] ボタン () をクリックします。

録画の再生が停止します。

再生を一時停止するには：

1. リモコンプレーヤーのツールバーで [一時停止] ボタン () をクリックします。

録画の再生が一時的に停止します。

再生を再開するには：

1. リモコンプレーヤーのツールバーで [再生] ボタン () をクリックします。

一時停止中に [再生] ボタンをクリックした場合は、前回再生を中断した位置から再生が始まります。停止中に [再生] ボタンをクリックした場合は、停止した位置からではなく、録画ファイルの先頭から再生が始まります。

再生をスキップするには：

1. シークバーのスライダを選択し、そのまま任意の位置まで動かします。

停止した位置からスライダを動かした位置までの再生時間をスキップできます。スライダを進行方向の逆方向の端まで動かすと、自動的に再生の開始位置まで戻ります。

ポイント

この機能は、再生中または一時停止中の場合に利用できます。停止中の場合は、スライダを動かせません (スキップできません)。

再生中にスキップした場合は、スキップした位置から再生が進行します。一時停止中にスキップした場合は、スキップした位置で一時停止の状態となります。

再生速度を速くするには（早送り）：

1. リモコンプレーヤーのツールバーで [早送り] ボタン () をクリックします。

通常の再生の 3 倍速で再生されます。

再生速度を遅くするには（スロー再生）：

1. リモコンプレーヤーのツールバーで [スロー再生] ボタン () をクリックします。

通常の再生の 1/3 の速度で再生されます。

7.8.2 再生画面の表示手順

リモコンプレーヤーでは、[リモートコントロール] ウィンドウでのコンピュータ画面の表示と同様に、再生画面を効果的に表示できます。

再生画面を拡大・縮小するには：

1. リモコンプレーヤーのメニューで、[表示] - [拡大／縮小] から [自動] を選択します。

再生画面がリモコンプレーヤーのウィンドウサイズに合わせて自動的に拡大・縮小します。また、再生画面を 50%、100%、または 200% で表示することもできます。この場合は、メニューの [表示] - [拡大／縮小] から [50%]、[100%]、または [200%] を選択してください。デフォルトでは 100% で表示（等倍表示）されます。

再生画面をフルスクリーン表示するには：

1. リモコンプレーヤーのメニューで、[表示] - [フルスクリーン表示] を選択します。

再生画面がフルスクリーンで表示されます。フルスクリーン表示を解除する場合は、ポップアップメニューで [フルスクリーン表示] を選択してください。

再生画面サイズにリモコンプレーヤーのウィンドウを合わせるには：

1. リモコンプレーヤーのメニューで、[ウィンドウ] - [表示幅に合わせる] を選択します。

再生画面サイズに合わせてリモコンプレーヤーのウィンドウサイズが拡大または縮小します。

複数のリモコンプレーヤーを整理して表示させるには：

1. リモコンプレーヤーのメニューで、[ウィンドウ] - [上下に並べて表示]、[左右に並べて表示]、または [左上から順に整理] を選択します。

リモコンプレーヤーがコントローラの画面上で整理して表示されます。

7.8.3 リモートコントロールを録画する手順

コントローラと接続中のコンピュータの画面情報を録画できます。録画は一時停止したり、一時停止した状態から再開したりできます。

リモートコントロールを録画するには：

1. [リモートコントロール] ウィンドウでメニューの [ファイル] - [スクリーン操作を記録] から [開始] を選択します。
2. 表示されるダイアログで、録画ファイルの保存先とファイル名を指定します。
録画ファイルの拡張子は、「jcr」です。
3. [保存] ボタンをクリックします。

コンピュータの画面の録画が開始されます。

録画を終了するには、[ファイル] - [スクリーン操作を記録] から [停止] を選択してください。

ポイント

ステータスバーに表示される録画状態のアイコンを右クリックして、表示されるメニューからも録画の操作ができます。

関連リンク

- [7.8.4 録画を一時停止・再開する手順](#)
- [7.8.5 録画データを再生する手順](#)
- [7.8.7 録画ファイルを AVI 形式に変換する手順](#)

7.8.4 録画を一時停止・再開する手順

録画を一時的に停止したり録画を開始したりできます。この機能を利用すると、必要な画面情報だけを録画できます。

録画を一時停止するには：

[リモートコントロール] ウィンドウの [ファイル] メニューから [スクリーン操作を記録] - [一時停止] を選択すると、録画が一時停止します。

録画を再開するには：

[リモートコントロール] ウィンドウの [ファイル] メニューから [スクリーン操作を記録] - [再開] を選択すると、録画が再開されます。

関連リンク

- [7.8.5 録画データを再生する手順](#)

7.8.5 録画データを再生する手順

リモートコントロールを録画した場合、コンピュータの画面情報は録画ファイルとして保存されています。この録画ファイルを再生するには、リモコンプレーヤーを利用します。

録画データを再生するには：

1. [リモートコントロール] ウィンドウのメニューで、[ファイル] – [スクリーン操作を再生] – [再生] を選択します。
2. 表示されるダイアログで再生する録画ファイルを選択し、[開く] ボタンをクリックします。

リモコンプレーヤーが起動し、自動的に録画ファイルの再生が始まります。

再生の進行状況は、リモコンプレーヤーの下部に表示されるシークバーで確認できます。再生が始まるとシークバーのスライダが左端から右へ移動していきます。

シークバーが表示されていない場合は、リモコンプレーヤーのメニューで [表示] – [シークバー] を選択してください。

関連リンク

- [7.8.3 リモートコントロールを録画する手順](#)
- [7.8.1 再生時にできる操作手順](#)
- [7.8.7 録画ファイルを AVI 形式に変換する手順](#)

7.8.6 録画ファイルの情報を確認する

表示中の録画ファイルの情報を確認するには、リモコンプレーヤーのメニューで [ファイル] – [プロパティ] を選択してください。表示された [プロパティ] ダイアログで、次の情報が確認できます。

- 場所（録画ファイルの保存先）
- サイズ
- 接続先（録画したコンピュータの IP アドレス、ホスト名、またはパス）
- バージョン（録画したコンピュータに導入されているエージェントのバージョン、または RFB のバージョン）
- 解像度（録画したコンピュータの解像度）
- カラーパレット（録画したコンピュータのカラーパレット（色数））

- 記録開始日時（「YYYY/MM/DD hh:mm:ss」の形式で表示。YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒）
- 記録時間※（「mm 分 ss 秒」の形式で表示。mm：分、ss：秒）

注※ 録画時間が1時間以上の場合も、分単位で表示されます。

7.8.7 録画ファイルを AVI 形式に変換する手順

録画ファイルを再生するには、コントローラの提供するリモコンプレーヤーが必要です。このため、録画ファイルを再生できるのはコントローラがインストールされた環境に限られます。しかし、録画ファイルを AVI ファイルに変換することで、コントローラがインストールされていないコンピュータでも録画した内容を再生できるようになります。

また、AVI ファイルに変換しておく、ほかのアプリケーションを利用してタイトルやコメントを付けるなどの編集ができます。なお、録画中にコンピュータの解像度を変更された場合は、AVI ファイルへ変換したあとも正しく再生されませんので注意してください。

AVI ファイルへの変換は、変換ウィザードで実行します。変換ウィザードを使用して、録画ファイルを AVI ファイルに変換する方法を次に説明します。

録画ファイルを AVI 形式に変換するには：

1. [リモートコントロール] ウィンドウのメニューで、[ファイル] - [スクリーン操作を再生] - [変換] を選択します。
変換ウィザードが起動します。
2. 変換したい録画ファイルを選択して、[次へ] ボタンをクリックします。
3. 変換後の AVI ファイルを指定して、[次へ] ボタンをクリックします。
4. AVI ファイルへの変換時に使用する圧縮形式を選択して、[次へ] ボタンをクリックします。
5. フレームレートと画像品質を設定して、[次へ] ボタンをクリックします。
6. 変換が開始され、変換状況が表示されます。
7. 変換が完了したら、[完了] ボタンまたは[再生] ボタンをクリックします。

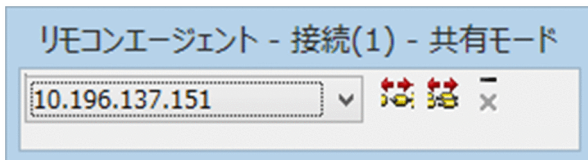
変換ウィザードが終了します。

[再生] ボタンをクリックすると、AVI ファイルに関連づけられているアプリケーションを起動し、変換ウィザードが終了します。Windows のデフォルトでは、Windows Media Player が起動します。

7.9 リモコンエージェントを利用する

7.9.1 リモコンエージェントのステータスウィンドウを表示する手順

タスクバーに表示される［リモコンエージェント］アイコンは、ステータスウィンドウとしてタスクバーから出して表示できます。



ステータスウィンドウを表示するには：

1. [リモコンエージェント] アイコンを右クリックし [メニューを表示する] メニューを選択します。
2. 下位のメニューで、[即時] または [接続時] を選択します。

[即時] を選択すると、選択後すぐに表示されます。[接続時] を選択すると、コントローラとの接続中だけ表示されます。

ステータスウィンドウを非表示にするには：

1. ステータスウィンドウの任意の場所を右クリックし、[最小化] メニューを選択します。

ステータスウィンドウが閉じて、タスクバーに [リモコンエージェント] アイコンが表示されます。

なお、[－] ボタンでステータスウィンドウを非表示にすることもできます。

7.9.2 リモコンエージェントを終了する手順

リモコンエージェントは、コンピュータの OS を終了させると、自動的に終了します。リモコンエージェントを手動で起動した場合は、Windows からのログオフ時に終了します。

Windows を起動したままリモコンエージェントを終了させることもできます。

手動でリモコンエージェントを終了するには：

1. [リモコンエージェント] アイコン、またはステータスウィンドウ上の任意の場所を右クリックします。
2. [終了] を選択します。

ステータスウィンドウを表示している場合は、メニューの代わりに [×] ボタンも使用できます。

リモコンエージェントが終了します。

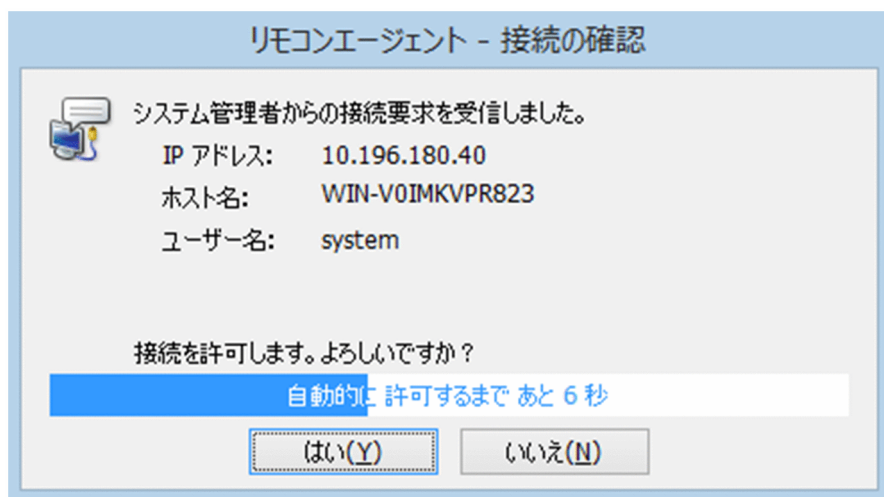
注意事項

エージェント設定で、利用者による終了を許可していない場合は、リモコンエージェントは手動で終了できません。このとき、[終了]メニューは非活性になっています。

7.9.3 コントローラからの接続要求の許可、拒否

コントローラから接続されるタイミングで接続を許可または拒否できます。コントローラからの接続要求に応答するには、エージェント設定の[リモートコントロールの設定] - [利用者のコンピュータに、利用者が応答するためのダイアログを表示する]がオンになっている必要があります。この設定をしておくと、例えば、個人情報などが書かれた文書の編集中にコントローラから接続要求があっても接続を拒否できるので、セキュリティを保持できます。

コントローラから接続要求があると、エージェントでは[接続の確認]ダイアログが表示されます。



このダイアログで、接続を許可するか、拒否するかを選択します。応答しなかった場合は、エージェント設定での設定内容に従って自動的に接続、または接続拒否されます。ただし、エージェントがログオン状態でない場合には、無条件に接続されます。

7.9.4 コンピュータ側で接続モードを変更する手順

コントローラが制御モードの場合は、接続先のコンピュータ側でキーボードやマウスでの操作ができなくなります。しかし、コンピュータ側で操作する必要があるときは、制御モードを強制的に解除し、共有モードに変更できます。

制御モードを強制的に解除するには：

1. 接続先のコンピュータ側で、[Ctrl] + [Alt] + [Delete] キーを押します。

接続先のコンピュータは共有モードになり、コンピュータ側で操作できるようになります。

なお、接続先のコンピュータの接続モードが制御モードから共有モードに変わると、接続モードが変更されたことがコントローラに通知されます。共有モードのコントローラでは何も変化は起きませんが、制御モードのコントローラでは、コントローラの接続モードを制御モードから共有モードに変更するかどうかを問い合わせるダイアログが表示されます。このダイアログで共有モードに変更することが許可されれば、コントローラも共有モードになり、コントローラとコンピュータの両方でコンピュータを操作できます。しかし、共有モードに変更することが許可されないと、コンピュータは制御モードのまま、コンピュータ側では操作できなくなります。

7.9.5 リモートコントロールの対象のコンピュータから接続を切断する手順

エージェント導入済みのコンピュータの場合、コンピュータ側からの操作でコントローラとの接続を切断できます。

ポイント

エージェント設定での設定によって、最後のコントローラとの切断時に、自動的にリモコンエージェントを終了できます。

コントローラとの接続を 1 台ずつ切断するには：

1. [リモコンエージェント] アイコンを右クリックして、[切断] メニューを選択します。
2. 切断するコントローラを選択します。

選択したコントローラとの接続が切断されます。

ステータスウィンドウを表示している場合は、メニューの代わりに [コントローラの切断] ボタン (🔌) を使用します。

すべてのコントローラとの接続を一括で切断するには：

1. [リモコンエージェント] アイコンを右クリックして、[すべて切断する] メニューを選択します。

接続中のすべてのコントローラとの接続が切断されます。

ステータスウィンドウを表示している場合は、メニューの代わりに [すべてのコントローラの切断] ボタン (🔌) を使用します。

関連リンク

- ・ [7.9.1 リモコンエージェントのステータスウィンドウを表示する手順](#)

7.9.6 コントローラに接続要求を出す

コンピュータからコントローラに接続要求を出すには、リクエストウィザードを利用します。

注意事項

リクエストウィザードは、オンライン管理のコンピュータだけで利用できます。

注意事項

コントローラに接続要求を出してリモートコントロールを開始する場合、コントローラ側でリクエストサーバが起動されている必要があります。リクエストサーバの起動方法については、「[7.7.12 リクエストサーバを開始または停止する手順](#)」を参照してください。

ポイント

リクエストウィザードでは、ウィザードの設定内容をファイルにエクスポートできます。複数のコンピュータから、同じコントローラに接続要求を出す場合、エクスポートした設定ファイルを各コンピュータでインポートすると素早く設定できて便利です。

コントローラに接続要求を出すには：

1. リクエストウィザードを起動します。

Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Agent] - [リモコンエージェント] - [リクエストウィザード] を選択してください。

リクエストウィザードが起動します。

2. 接続先のコントローラを指定して、[次へ] ボタンをクリックします。

ポイント

あらかじめリクエストウィザードの設定内容をエクスポートしている場合、[設定情報をインポート] ボタンをクリックしてインポートすることで、ウィザードの内容を一括設定できます。

3. コントローラの応答に対する動作を設定して、[次へ] ボタンをクリックします。

4. 接続要求時にコントローラ側に表示するメッセージを設定して、[次へ] ボタンをクリックします。

5. ウィザード完了後の動作を選択して、[完了] ボタンをクリックします。

ポイント

[エクスポート] ボタンをクリックすると、ウィザードの設定内容をファイルにエクスポートできます。

設定した内容に従って、コントローラに接続要求を出します。コントローラ側で接続が許可されると、リモートコントロールが開始されます。

コンピュータからコントローラに接続要求を出すと、コンピュータのタスクバーにアイコン () が表示されます。このアイコンが表示されている間は、接続要求を出し続けていることを意味します。

ポイント

エージェントでは、アドレス認証（許可コントローラ）とユーザー認証（ユーザー ID およびパスワード）の2種類の認証情報を設定できます。しかし、接続要求を基にコントローラから接続されるときに使用されるのはユーザー認証だけです。

7.9.7 接続要求をキャンセルする手順

コンピュータからコントローラに接続要求を出すと、コンピュータのタスクバーにアイコン () が表示されます。このアイコンが表示されている間は、接続要求を出し続けていることを意味します。

接続要求は、アイコンからキャンセルできます。すべての接続要求をキャンセルするだけでなく、特定の接続要求だけをキャンセルすることもできます。

接続要求をキャンセルするには：

1. アイコンを右クリックします。
2. 表示されるメニューで、[切断] から対象のコントローラを選択するか、[すべて切断する] を選択します。

接続要求がキャンセルされます。接続要求をすべてキャンセルした場合は、タスクバーからアイコンが削除されます。

なお、次の操作をした場合は自動的に接続要求がキャンセルされます。

- エージェントを終了する。
- コンピュータをログオフする。

接続要求はコントローラ側からもキャンセルできます。コントローラ側からキャンセルされた場合、キャンセルされたことを示すメッセージがコンピュータに表示されます。

7.10 チャットを利用する

7.10.1 チャットサーバの動作環境を設定する手順

チャットサーバの接続ポート番号や、接続時のパスワードを設定できます。

チャットサーバの動作環境を設定するには：

1. チャットサーバを起動し、[チャットサーバ] アイコン () を表示させます。
2. [チャットサーバ] アイコンを右クリックして、表示されるメニューから [環境の設定] を選択します。
3. 表示されるダイアログで動作環境を設定して、[OK] ボタンをクリックします。

ダイアログが閉じて設定が適用されます。

関連リンク

- [7.10.3 チャットサーバを起動する手順](#)
- [7.10.4 エージェントでの起動方法によるチャットサーバの機能差異](#)

7.10.2 [チャット] ウィンドウの動作環境を設定する手順

チャット中に表示されるユーザー情報、各種通知の有無、ウィンドウの表示形式などを設定できます。

ポイント

チャットサーバとの接続中は設定できない項目があります。このため、動作環境はチャットサーバと接続していない状態で設定してください。

[チャット] ウィンドウの動作環境を設定するには：

1. [チャット] ウィンドウのメニューで [ツール] - [環境の設定] を選択します。
2. 表示されるダイアログで動作環境を設定して、[OK] ボタンをクリックします。

ダイアログが閉じて設定が適用されます。

7.10.3 チャットサーバを起動する手順

チャットサーバを起動すると、[チャット] ウィンドウがチャットサーバとして動作します。チャットサーバの起動中は、タスクバーに [チャットサーバ] アイコン () が表示されています。なお、[チャット] ウィンドウでメッセージを送受信する操作は、クライアントとして動作していた時と同様です。

チャットサーバを起動するには、自動起動する方法と手動起動する方法の2つがあります。チャットサーバの自動起動を設定することで、チャットサーバを常駐させられます。例えば、ヘルプデスクでチャットを利用する場合は自動起動にしておくなど、利用形態によって適切な方法を選択してください。

チャットサーバを自動起動するには：

コントローラの場合は、チャットサーバをスタートアップに登録します。エージェント導入済みのコンピュータの場合は、エージェントの起動時に自動起動するよう設定するか、またはスタートアップに登録します。

スタートアップに登録する場合

1. [チャット] ウィンドウを起動します。

ポイント

[チャット] ウィンドウは、次の方法で起動できます。

- [リモートコントロール] ウィンドウのメニューで [ツール] - [チャット] を選択する
- Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Manager] - [ツール] - [リモートコントロール チャット] を選択する (コントローラの場合)
- Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Agent] - [リモコンエージェント] - [チャット] を選択する (エージェント導入済みのコンピュータの場合)

2. メニューの [ツール] - [チャットサーバ] から、[スタートアップに登録] を選択します。

ユーザーの [スタートアップ] グループに、[チャットサーバ] ショートカットが作成されます。次のログオン時から、自動的にチャットサーバが起動されます。

エージェント起動時に自動起動させる場合

エージェント起動時にチャットサーバを自動的に起動させるには、エージェント設定の [リモートコントロールの設定] で [リモコンエージェントの起動時に、チャットも開始できる状態にしておく] をチェックしてください。

チャットサーバを手動起動するには：

1. [チャット] ウィンドウを起動します。

ポイント

[チャット] ウィンドウは、次の方法で起動できます。

- [リモートコントロール] ウィンドウのメニューで [ツール] - [チャット] を選択する
- Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Manager] - [ツール] - [リモートコントロール チャット] を選択する (コントローラの場合)
- Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Agent] - [リモコンエージェント] - [チャット] を選択する (エージェント導入済みのコンピュータの場合)

2. メニューの [ツール] - [チャットサーバ] から、[チャットサーバを起動] を選択します。

チャットサーバが起動し、タスクバーに [チャットサーバ] アイコンが表示されます。

ポイント

[チャット] ウィンドウの [ツール] メニューから [チャットサーバ] - [最小化時に隠す] を選択すると、チャットサーバを最小化したときに、タスクバーに表示させないようにできます。タスクバーに表示させないようにしても [チャットサーバ] アイコンは表示されていますので、[チャットサーバ] アイコンをダブルクリックすることで再表示できます。また、ほかの [チャット] ウィンドウから接続されると、自動的にチャットサーバがポップアップ表示されます。

関連リンク

- 7.10.11 [チャットサーバ] アイコンから操作する手順

7.10.4 エージェントでの起動方法によるチャットサーバの機能差異

エージェントで自動起動したチャットサーバは、手動起動したチャットサーバと次の点で機能が異なります。

- [チャット] ウィンドウの次のメニューが使用できません (非活性となります)。
 - [ファイル] - [接続] メニュー
 - [ファイル] - [切断] メニュー
 - [ツール] - [チャットサーバ] メニュー
- [環境の設定] ダイアログの [全般] タブの項目は、常に変更できるようになります。
- [チャット] ウィンドウで次の操作をした場合、[チャット] ウィンドウは閉じられ、タスクバーにも表示されません。[チャットサーバ] アイコンをダブルクリックするか、またはメッセージを受け取ると、再度 [チャット] ウィンドウが表示されます。

- [ファイル] – [終了] メニューを選択した場合
- タイトルバーの [×] をクリックした場合
- アイコン化した場合

7.10.5 チャットを開始する手順

[チャット] ウィンドウがチャットサーバに接続すると、チャットを開始できます。チャットを開始するには、次の2つの方法があります。

- [チャット] ウィンドウからほかのチャットサーバに接続する。
- チャットサーバを起動して、ほかの [チャット] ウィンドウからの接続を待つ。

ここでは、[チャット] ウィンドウからほかのチャットサーバに接続してチャットを開始する手順について説明します。チャットサーバを起動する方法については、「[7.10.3 チャットサーバを起動する手順](#)」を参照してください。

チャットサーバに接続してチャットを開始するには：

1. [チャット] ウィンドウを起動します。

ポイント

[チャット] ウィンドウは、次の方法で起動できます。

- [リモートコントロール] ウィンドウのメニューで [ツール] – [チャット] を選択する
- Windows の [スタート] メニューから [すべてのプログラム] – [JP1_IT Desktop Management 2 - Manager] – [ツール] – [リモートコントロール チャット] を選択する（コントローラの場合）
- Windows の [スタート] メニューから [すべてのプログラム] – [JP1_IT Desktop Management 2 - Agent] – [リモコンエージェント] – [チャット] を選択する（エージェント導入済みのコンピュータの場合）

2. [チャット] ウィンドウのメニューで [ファイル] – [接続] を選択します。

3. 表示されるダイアログで接続するチャットサーバのアドレスを指定し、[OK] ボタンをクリックします。

ポイント

接続先のチャットサーバにパスワードが設定されている場合は、[パスワードの入力] ダイアログが表示されます。この場合、パスワードを指定して [OK] ボタンをクリックしてください。なお、パスワードを3回連続して間違えると接続に失敗します。[チャット] ウィンドウから再度接続し直してください。

指定したチャットサーバと接続したことを知らせるメッセージが表示されます。

ポイント

チャットサーバに接続しているコンピュータの [チャット] ウィンドウからは、1つのチャットサーバだけでなく、複数のチャットサーバと接続できます。ただし、チャットサーバが起動しているコンピュータからは、ほかのチャットサーバに接続できません。チャットサーバが停止している状態で、ほかのチャットサーバに接続してください。

7.10.6 チャットでメッセージを送信する手順

メッセージを送信することで、接続中のユーザーと対話できます。また、ほかのユーザーによって送信されたメッセージは自動的に表示されます。

チャットでメッセージを送信するには：

1. [チャット] ウィンドウのメッセージ入力ボックスにメッセージを入力します。
2. [送信] ボタン () をクリックします。

メッセージが送信されます。

ポイント

特定のユーザーだけにメッセージを送信したい場合、[チャットユーザーリスト] で送信先のユーザーを指定してください。チェックしたユーザーだけにメッセージが送信されます。デフォルトでは、すべてのユーザーがチェックされています。

7.10.7 チャットを終了する手順

チャットを終了する方法は、チャットサーバを起動している場合と、チャットサーバに接続している場合とでは次のように異なります。

チャットサーバを起動している場合

- [チャット] ウィンドウを閉じる。
- チャットサーバを終了する。

チャットサーバに接続している場合

- [チャット] ウィンドウを閉じる。
- チャットサーバとの接続を切断する。

以降では、これらチャットの終了方法について説明します。

【チャット】 ウィンドウを閉じるには：

1. 【チャット】 ウィンドウのメニューで【ファイル】－【終了】を選択します。

【チャット】 ウィンドウが終了します。次の場合はメッセージが表示されますので、状況に応じて対応してください。

- チャット内容を保存していない場合、保存するかどうかを問い合わせるメッセージが表示されます。チャット内容の保存については、「[7.10.8 チャットの内容を保存する手順](#)」を参照してください。
- チャットサーバを起動している場合は、チャットサーバの終了を問い合わせるメッセージが表示されます。

チャットサーバを終了するには：

1. 【チャット】 ウィンドウのメニューの【ツール】－【チャットサーバ】から、【チャットサーバを起動】を選択してチェックを外します。

チャットサーバが終了し、【チャット】 ウィンドウが非活性となります。

チャットサーバとの接続を切断するには：

1. 【チャット】 ウィンドウのツールバーで【切断】 ボタン () をクリックします。
複数のチャットサーバと接続中の場合、切断するチャットサーバを選択するダイアログが表示されます。
2. 切断するチャットサーバを選択して、【OK】 ボタンをクリックします。

選択したチャットサーバと切断されます。正常に切断された場合、【チャット】 ウィンドウにチャットサーバとの切断を示すメッセージが表示されます。

7.10.8 チャットの内容を保存する手順

チャットの内容をファイルに保存できます。対話のログを保存できます。

チャットの内容を保存するには：

1. 【チャット】 ウィンドウのツールバーで【上書き保存】 ボタン () をクリックします。
2. 表示されるダイアログで保存先やファイル名を指定して、【保存】 ボタンをクリックします。

指定したファイル名で、チャットの内容が保存されます。

ポイント

別のファイルに保存する場合は、[チャット] ウィンドウのメニューで [ファイル] - [名前を付けて保存] を選択します。

なお、ファイルを保存するときにファイルの種類を指定できます。ファイルの種類は、次のファイル形式から選択できます。

- テキストファイル (*.txt)
チャットビューに表示されている内容すべてを保存します。
- リッチテキストファイル (*.rtf)
チャットビューに表示されている内容、およびその書式（文字フォント、色）すべてを保存します。
- すべてのファイル (*.*)
チャットビューに表示されている内容すべてを保存します。この場合、任意の拡張子を指定できます。

7.10.9 チャットの内容を印刷する手順

[チャット] ウィンドウで表示されているチャットの内容を印刷できます。

チャットの内容を印刷するには：

1. [チャット] ウィンドウのツールバーで [印刷] ボタン () をクリックします。
2. 表示されるダイアログで出力先のプリンタや印刷部数などを設定して、[OK] ボタンをクリックします。

表示されているチャットの内容が印刷されます。

7.10.10 [チャット] ウィンドウからリモートコントロールを開始する手順

コントローラをインストールしているコンピュータの場合、[チャット] ウィンドウからコントローラを起動できます。チャットで連絡を受けた場合に、接続が必要なときはそのままリモートコントロールを開始できます。

[チャット] ウィンドウからリモートコントロールを開始するには：

1. [チャット] ウィンドウの [チャットユーザーリスト] から接続するユーザーを選択します。
2. メニューの [ツール] - [リモートコントロールの開始] を選択します。

コントローラが起動して、指定したユーザーのコンピュータに接続します。

7.10.11 [チャットサーバ] アイコンから操作する手順

チャットサーバが起動すると、タスクバー上に [チャットサーバ] アイコン () が表示されます。
[チャットサーバ] アイコンから、チャットに関する操作ができます。

接続中のユーザーを確認するには：

1. タスクバーの [チャットサーバ] アイコンを右クリックして、表示される [ユーザー] メニューを選択します。

接続中のユーザー名が、「ニックネーム@ホスト名」の形式で表示されます。

チャットユーザーを切断するには：

1. タスクバーの [チャットサーバ] アイコンを右クリックして、表示される [切断] メニューを選択します。
2. 切断するユーザーを選択して、[OK] ボタンをクリックします。

ポイント

複数のユーザーを選択して、一度に切断することもできます。

指定したユーザーとの接続が切断されます。切断されたユーザーの [チャット] ウィンドウには、サーバから切断されたことを伝えるメッセージが表示されます。

オプションを設定するには：

1. タスクバーの [チャットサーバ] アイコンを右クリックして、[環境の設定] を選択します。
2. 表示されるダイアログでチャットサーバのオプションを設定して、[OK] ボタンをクリックします。

ダイアログが閉じて、設定が保存されます。

8

機器のネットワーク接続を管理する

ここでは、組織内の機器のネットワークを接続したり遮断したりする方法について説明します。

8.1 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  または

  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

エージェント導入済みのコンピュータに、提供媒体から「JP1/IT Desktop Management 2 - Network Monitor」をインストールする方法でも、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。

8.2 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  または  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  または  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 [JP1/IT Desktop Management 2 - Network Monitor] 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

- 8.1 ネットワークモニタを有効にする手順

8.3 ネットワーク接続を許可する手順

安全なことが確認できているコンピュータや、検疫が完了したコンピュータがあった場合に、ネットワーク接続を手動で許可できます。

なお、ネットワーク接続を許可できるのは、ネットワークモニタが有効になっているネットワークセグメント内のコンピュータだけです。

ネットワーク接続を許可するには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】－【機器一覧（ネットワーク）】画面でネットワーク接続を許可したいコンピュータが含まれ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、ネットワーク接続を許可したいコンピュータを選択して、【操作メニュー】の【接続を許可する】を選択します。
4. 表示されるダイアログで、【OK】ボタンをクリックします。

選択したコンピュータのネットワーク接続が許可されます。

【ノートに追記する】をチェックすると、ネットワーク接続を許可した日付や理由などを記録できます。ここで入力した情報は【ノート】タブに追記されます。

ポイント

セキュリティ画面の【機器のセキュリティ状態】－【機器一覧（ネットワーク）】画面、または設定画面の【ネットワーク制御】－【ネットワーク制御リストの設定】画面でもネットワーク接続を許可できます。

関連リンク

- [8.4 ネットワーク接続を遮断する手順](#)

8.4 ネットワーク接続を遮断する手順

外部から持ち込まれたコンピュータや、セキュリティ対策が不十分なコンピュータがあった場合に、ネットワーク接続を手動で遮断できます。

なお、ネットワーク接続を遮断できるのは、ネットワークモニタが有効になっているネットワークセグメント内のコンピュータだけです。

ネットワーク接続を遮断するには：

1. 機器画面を表示します。
2. メニューエリアの【機器情報】－【機器一覧（ネットワーク）】画面でネットワークの接続を遮断したいコンピュータが含まれ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、ネットワーク接続を遮断したいコンピュータを選択して、【操作メニュー】の【接続を許可しない】を選択します。
4. 表示されるダイアログで、【操作を続行する】をチェックして、【OK】ボタンをクリックします。

選択したコンピュータのネットワーク接続が遮断されます。また、ネットワーク制御リストの設定も、【ネットワークへの接続】が「許可しない」に変更されます。

【利用者にメッセージを通知する】をチェックすると、選択したコンピュータの利用者にメッセージを通知できます。複数のコンピュータを選択すると、同じ内容のメッセージを一斉に通知できます。

選択したコンピュータの【ノートに追記する】をチェックすると、ネットワーク接続を遮断した日付や理由などを記録できます。ここで入力した情報は【ノート】タブに追記されます。

注意事項

手動でネットワーク接続を遮断すると、自動でネットワーク接続が許可されなくなります。

注意事項

ネットワークモニタを有効にしていないネットワークセグメントでは、【ネットワークへの接続】が「許可しない」と表示されていても、コンピュータのネットワーク接続は遮断されません。

ポイント

セキュリティ画面の【機器のセキュリティ状態】－【機器一覧（ネットワーク）】画面、または設定画面の【ネットワーク制御】－【ネットワーク制御リストの設定】画面でもネットワーク接続を許可できます。

ポイント

ネットワーク接続が遮断されると、その機器で IP アドレスが競合する旨のメッセージが表示されることがあります。

関連リンク

- [8.3 ネットワーク接続を許可する手順](#)

8.5 自動的にネットワーク接続が遮断された機器を再接続する手順

セキュリティポリシーの判定結果やネットワーク制御リストの期限切れなどで自動的にネットワーク接続を遮断された場合、ネットワークに再接続できます。

自動的にネットワーク接続が遮断される契機は、次の4つがあります。

- 接続が許可されていないネットワークに機器が接続された場合
- セキュリティポリシーに違反した場合
- ネットワーク制御リストで許可する期間外の場合
- ネットワーク制御リストが削除された場合

ネットワーク接続を遮断された機器の再接続方法について説明します。

機器を管理対象または除外対象にして、ネットワーク接続を許可する

ネットワークモニタによって新規発見機器のネットワーク接続が許可されていない場合、発見された機器はネットワーク接続を「許可しない」設定でネットワーク制御リストに登録されるため、ネットワーク接続が自動的に遮断されます。この場合、発見された機器を確認して管理対象または除外対象にすることで、組織内の機器として確認できたと見なされ、自動的にネットワーク制御リストの設定が「許可する」に変更されます。これによって、機器がネットワーク接続できるようになります。

セキュリティ対策を実施して、ネットワーク接続を自動的に許可する

セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］を設定している場合、判定結果によって、自動的にネットワーク接続が遮断されます。この場合、セキュリティ対策を実施します。これによって、セキュリティポリシーに遵守すると、次回の判定時にネットワーク接続できるようになります。

ネットワーク制御リストで期限を変更してネットワーク接続を許可する

ネットワーク制御リストにネットワーク接続を許可する期間を設定している場合、期間外では自動的にネットワーク接続が遮断されます。この場合、該当する機器がネットワーク接続する必要がある場合、期間を変更してネットワーク接続が許可されるようにします。なお、期間外の場合は、その機器の接続設定に利用期間外を示すアイコン（）が表示されます。

ネットワーク制御リストを再登録してネットワーク接続を許可する

機器を削除したり、ハードウェア資産を削除したりした場合、対応するネットワーク制御リストも自動的に削除されます。ネットワークモニタ設定で新規機器のネットワーク接続を許可しない設定にしていると、その機器が再接続してもネットワーク接続は自動的に遮断されます。この場合、発見された機器のネットワーク制御リストを「許可する」設定に変更してください。機器がネットワーク接続できるようになります。

なお、エージェント導入済みのコンピュータは、再接続後にセキュリティの判定に従ってネットワーク接続が制御されます（セキュリティポリシーの［アクション項目］－［ネットワーク接続制御］を設定している場合）。自動的に再接続させるには、セキュリティポリシーを遵守するようにしてください。

ポイント

これらの再接続方法のほかに、手動でネットワークに再接続する方法があります。

ネットワーク接続が遮断された機器に対して、ネットワーク接続を強制的に許可できます。手動でネットワーク接続を許可する方法については、「[8.3 ネットワーク接続を許可する手順](#)」を参照してください。

8.6 ネットワークモニタ設定を管理する

8.6.1 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。

8.6.2 ネットワークモニタ設定を編集する手順

設定画面の［ネットワーク制御の設定］画面の一覧にあるネットワークモニタ設定の内容を編集できます。

ネットワークモニタ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、編集したいネットワークモニタ設定の［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。

選択したネットワークモニタ設定が更新されます。

8.6.3 ネットワークモニタ設定を削除する手順

設定画面の［ネットワーク制御の設定］画面の一覧にあるネットワークモニタ設定を削除できます。

ポイント

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は削除できません。割り当てを解除してから削除してください。

ネットワークモニタ設定を削除するには：

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、削除したいネットワークモニタ設定を選択して、[削除] ボタンをクリックします。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

ネットワークモニタ設定の一覧から、選択したネットワークモニタ設定が削除されます。

8.6.4 ネットワークモニタ設定を割り当てる手順

ネットワークモニタ設定をネットワークセグメントごとに割り当てて、新規に発見された機器のネットワーク接続をネットワークセグメントごとに制御できます。

ポイント

ネットワークモニタ設定を割り当てるためには、そのネットワークセグメントにネットワークモニタ機能を導入する必要があります。

ネットワークモニタ設定を割り当てるには：

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を割り当てるネットワークセグメントを選択して、インフォメーションエリアの下部でネットワークモニタを有効にするコンピュータを選択して、[ネットワークモニタを有効にする] 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。

ネットワークセグメントにネットワークモニタ設定が割り当てられ、ネットワークモニタ設定の割り当て一覧に表示されます。

8.6.5 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。

8.7 ネットワーク制御リストを管理する

8.7.1 ネットワーク制御リストに機器を追加する手順

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に機器を追加できます。ネットワーク制御リストに機器を追加すると、特定の機器だけネットワーク接続を許可したり、遮断したりできます。また、ネットワーク接続する期間を設定することもできます。

ネットワーク制御リストに機器を追加するには：

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［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、ネットワーク接続可否の設定を入力して、[OK] ボタンをクリックします。

ネットワーク制御リストに機器が追加されます。

関連リンク

- [8.7.2 ネットワーク制御リストの機器を編集する手順](#)
- [8.7.3 ネットワーク制御リストから機器を削除する手順](#)
- [6.9 機器を削除する手順](#)

8.7.2 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。

8.7.3 ネットワーク制御リストから機器を削除する手順

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手動で登録されている機器を削除できます。

ネットワーク制御リストから機器を削除するには：

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、削除したい機器を選択して［削除］ボタンをクリックします。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

ネットワーク制御リストから、選択した機器が削除されます。

注意事項

ネットワーク制御リストの情報は、手動で追加したものは削除できますが、ネットワークモニタが検出した機器や、ネットワーク探索などによって自動で追加された情報はネットワーク制御リストの設定画面から削除できません。自動で追加された情報を削除する場合は、機器情報を削除することでネットワーク制御リストから削除できます。なお、自動で追加された設定情報かどうかは、ネットワーク制御リストの「ホスト名」に情報が表示されているかどうかで判別できます。

関連リンク

- ・ [8.7.1 ネットワーク制御リストに機器を追加する手順](#)
- ・ [8.7.2 ネットワーク制御リストの機器を編集する手順](#)

8.7.4 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。

8.8 特例接続を管理する

8.8.1 特例接続の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] 画面で、特例接続の設定を [ネットワークへの接続を許可しない機器の特例接続] に追加できます。これによって、ネットワーク接続が遮断されている機器に対して、特定の通信だけネットワーク接続を許可するようにネットワーク接続を制御できます。

特例接続の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 [ネットワークへの接続を許可しない機器の特例接続] 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特例接続の設定を入力して、[OK] ボタンをクリックします。

特例接続の設定が追加され、[ネットワークへの接続を許可しない機器の特例接続] の一覧に表示されます。

関連リンク

- [8.8.2 特例接続の設定を編集する手順](#)
- [8.8.3 特例接続の設定を削除する手順](#)

8.8.2 特例接続の設定を編集する手順

設定画面の [ネットワーク制御の設定] 画面の [ネットワークへの接続を許可しない機器の特例接続] にある特例接続の設定の内容を編集できます。

特例接続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、編集したい特例接続の設定の [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。

選択した特例接続の設定が更新されます。

関連リンク

- [8.8.1 特例接続の設定を追加する手順](#)
- [8.8.3 特例接続の設定を削除する手順](#)

8.8.3 特例接続の設定を削除する手順

設定画面の [ネットワーク制御の設定] 画面の [ネットワークへの接続を許可しない機器の特例接続] にある特例接続の設定を削除できます。

特例接続の設定を削除するには：

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、削除したい特例接続の設定を選択して [削除] ボタンをクリックします。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

[ネットワークへの接続を許可しない機器の特例接続] の一覧から、選択した特例接続の設定が削除されます。

関連リンク

- [8.8.1 特例接続の設定を追加する手順](#)
- [8.8.2 特例接続の設定を編集する手順](#)

8.9 JP1/NETM/NM - Manager 連携の設定を有効にする手順

JP1/NETM/NM - Manager 連携を有効にすると、JP1/NETM/NM - Manager で管理しているネットワークセグメントを JP1/IT Desktop Management 2 でネットワーク接続制御できます。

JP1/NETM/NM - Manager 連携の設定を有効にするには：

1. 設定画面を表示します。
2. メニューエリアで [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、[JP1/NETM/NM - Manager 連携の設定] 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、[操作を続行する] が表示された場合、表示されたメッセージの内容を確認した上でチェックします。
5. [JP1/NETM/NM - Manager と連携する] をチェックします。
6. [OK] ボタンをクリックします。

JP1/NETM/NM - Manager 連携の設定が有効になります。

9

セキュリティ状況を管理する

ここでは、組織内のセキュリティ管理およびセキュリティ状況の把握について説明します。

9.1 セキュリティ状況を確認する

管理対象のコンピュータには、デフォルトで「デフォルトポリシー」が適用されます。JP1/IT Desktop Management 2 でコンピュータを管理対象にした直後は、管理者がセキュリティポリシーを設定しなくても、デフォルトポリシーによって判定されたセキュリティ状況を確認できます。

ポイント

運用を開始した直後は、デフォルトポリシーによって判定されたセキュリティ状況を確認して問題点を対策することをお勧めします。これによって基本的なセキュリティを確保したあとで、組織のセキュリティ方針に沿ってセキュリティポリシーを設定し、セキュリティ状況を管理していきます。

セキュリティ状況は、ホーム画面に表示されるパネルや、セキュリティ画面、レポートおよびイベント画面で確認できます。

ホーム画面のパネルで確認する

ホーム画面では「システムサマリ」パネルの「危険と判定された機器」から、判定結果が「安全」以外のコンピュータの台数を確認できます。台数のリンクをクリックすると、セキュリティ画面の「機器のセキュリティ状態」画面が表示され、各コンピュータのセキュリティ状況を確認できます。

「カテゴリごとのセキュリティ評価」パネルでは、コンピュータの総合的なセキュリティ評価と、セキュリティ対策が不足している点を確認できます。

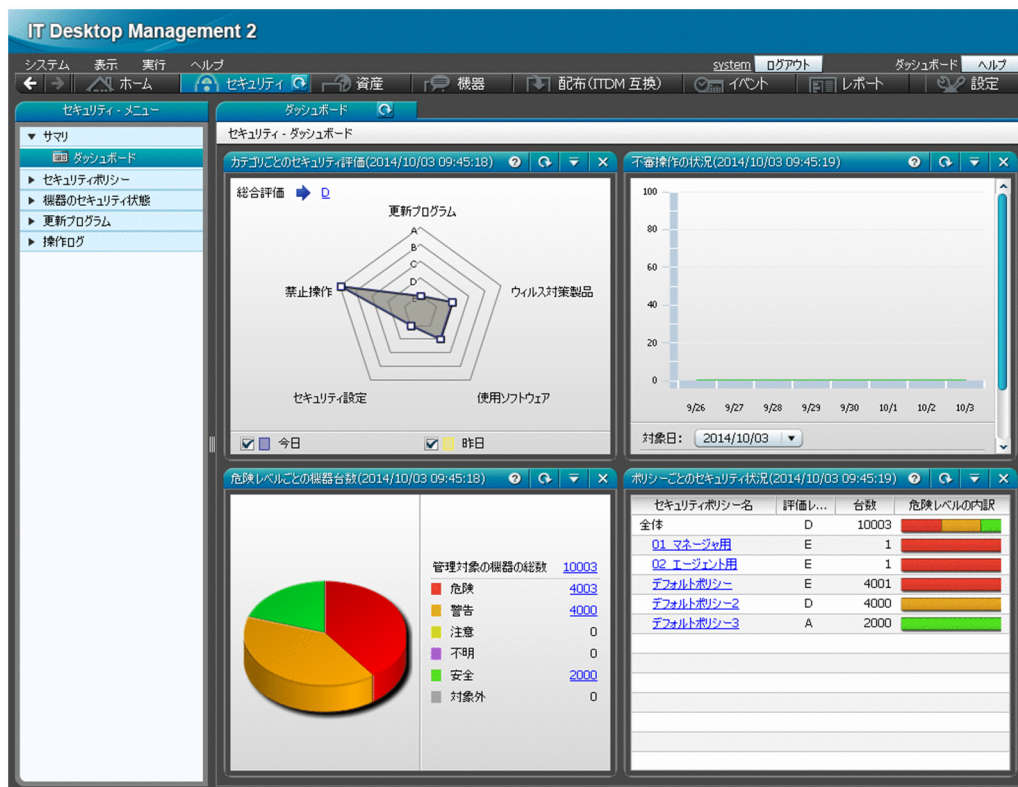


セキュリティ画面で確認する

セキュリティ画面では、[サマリ] 画面、[セキュリティポリシー] 画面、[機器のセキュリティ状態] 画面からセキュリティ状況を確認できます。

[サマリ] 画面で確認する

セキュリティ状況の概況を確認できます。各パネルのリンクをクリックすることで、詳細を確認できる画面が表示されるので、具体的な問題点を調査する入口として利用できます。



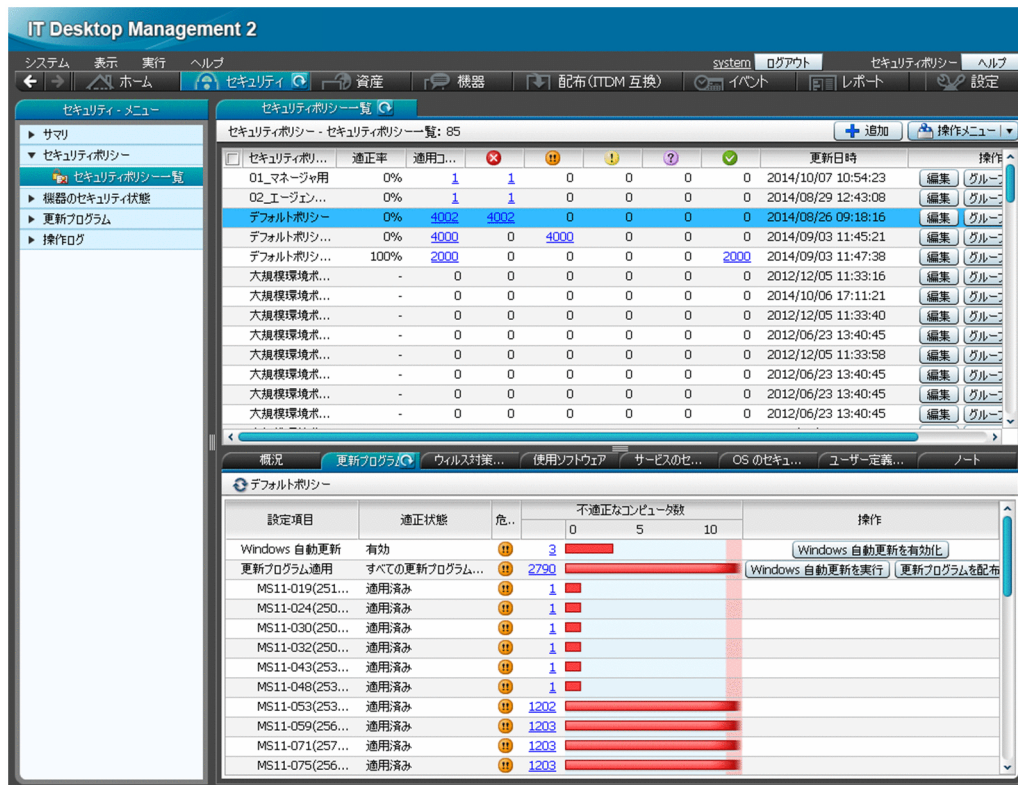
[セキュリティポリシー] 画面で確認する

セキュリティポリシーごとに、セキュリティポリシーに対する適正率や、セキュリティ項目の設定が不適正なコンピュータ数を確認できます。

表示項目の危険 (❌)、警告 (⚠️)、注意 (⚡) が 0 でない場合は、セキュリティポリシーが遵守されていないおそれがあります。

コンピュータ数のリンクをクリックして、[機器のセキュリティ状態] 画面を表示し、該当するコンピュータのセキュリティ状況を確認してください。

また、この画面からセキュリティポリシーを適用しているコンピュータに対して、自動対策を実行できます。

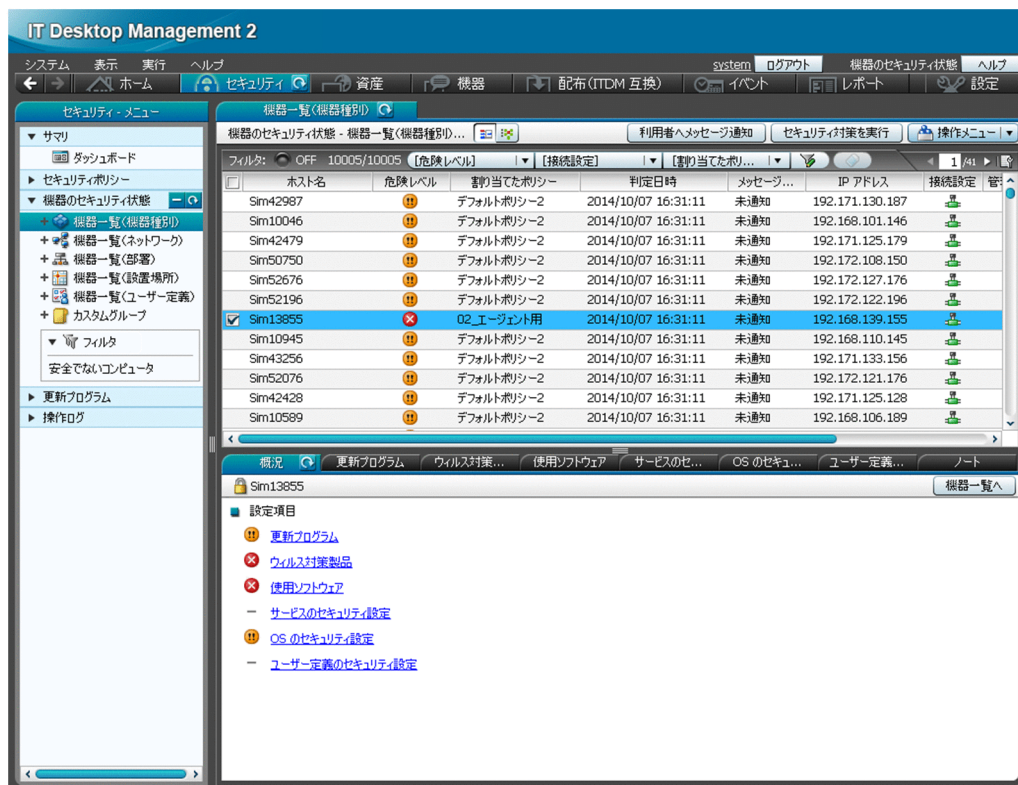


[機器のセキュリティ状態] 画面で確認する

コンピュータごとに、セキュリティ状況を確認できます。

各コンピュータの総合またはカテゴリ別の危険レベルや、セキュリティ設定の状況をピンポイントで確認できます。この画面から、個々のコンピュータに対して自動対策を実行できます。

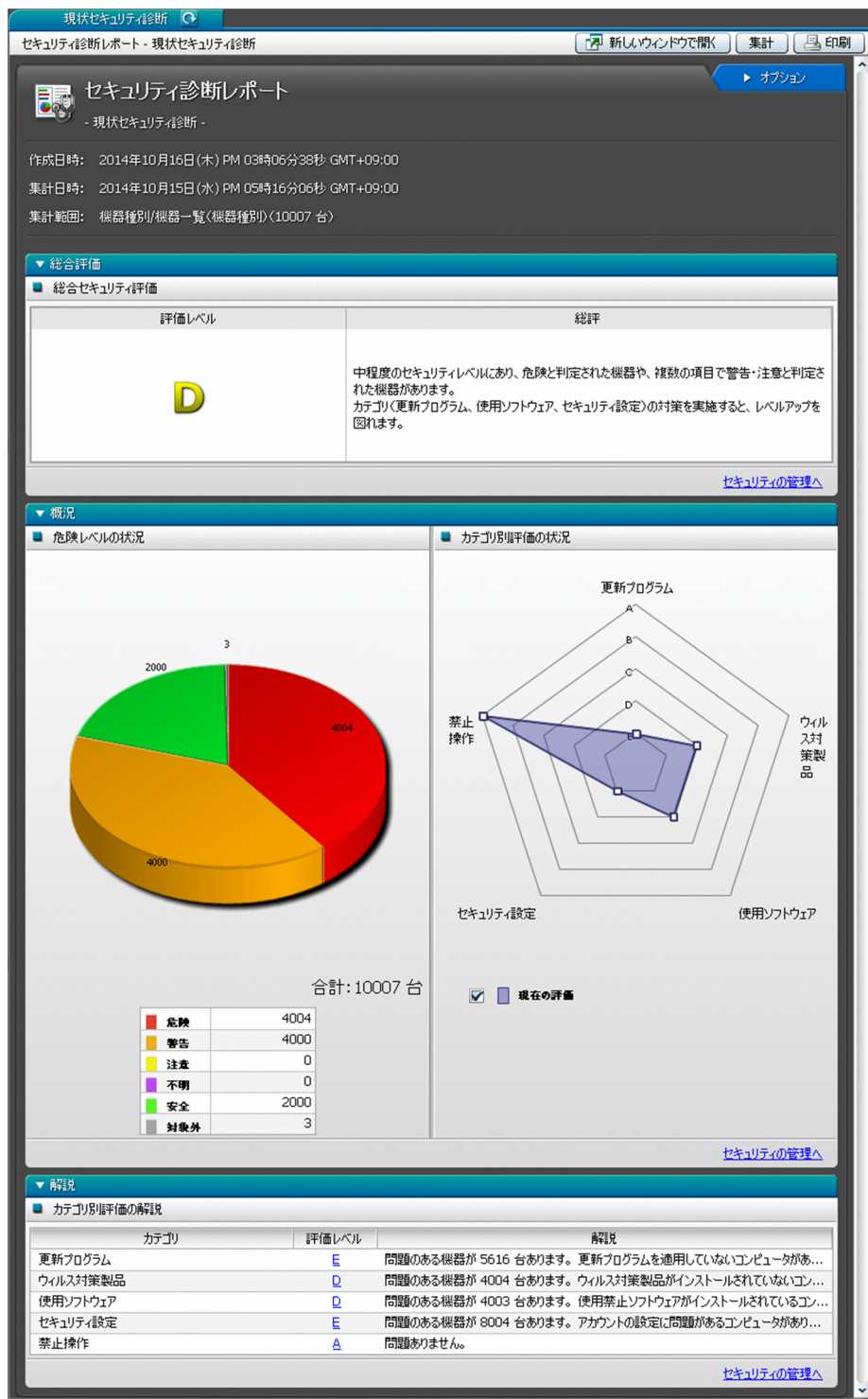
危険レベルが危険 (❌)、警告 (!!)、注意 (!) の場合は、セキュリティポリシーが遵守されていないおそれがあります。セキュリティ項目ごとに判定結果を確認して、問題があるセキュリティ項目を対策してください。



レポートで確認する

[ダイジェストレポート]、[セキュリティ診断レポート]、[セキュリティ詳細レポート] でセキュリティ状況を確認できます。

[ダイジェストレポート] では、セキュリティ評価を確認できます。[セキュリティ診断レポート] では、セキュリティの総合評価や現在の状況など、セキュリティ状況全体の概況を確認できます。[セキュリティ詳細レポート] では、セキュリティのカテゴリごとに、危険レベルの内訳や割合など詳細な状況を確認できます。



イベント画面で確認する

イベント画面でセキュリティ関連のイベントを確認できます。セキュリティポリシー違反とならないような軽微なイベントも確認できます。

IT Desktop Management 2

システム 表示 実行 ヘルプ

セキュリティ 資産 機器 配布 (ITDM 互換) イベント レポート 設定

system ログアウト イベント ヘルプ

イベント - メニュー

イベント

イベント一覧

イベント - イベント一覧: 31392... 2823742 176110 139355 確認済み: 0 未確認: 3139207

フィルタ: ON 3139207/7832055 [確認状態] [登録日時] セキュリティ 1/12557

確認状態	重大度	内容	登録日時	種類	発生元
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:16:03	セキュリティ	Sim11746
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:16:03	セキュリティ	Sim12047
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:16:03	セキュリティ	Sim13472
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:16:03	セキュリティ	Sim52464
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim43152
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim12694
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim43253
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim10131
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim50935
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim50929
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim50388
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim51072
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim44097
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:53	セキュリティ	Sim10381
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim50363
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim10231
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim11712
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim52985
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim10348
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim51507
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim50524
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim43977
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim51839
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim42552
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim10581
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim43449
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim50367
未確認	×	機器のセキュリティ状態を判定しまし...	2014/10/15 17:15:52	セキュリティ	Sim13678

9.2 判定対象から除外するユーザーを設定する手順

ユーザーアカウントごとにセキュリティ状況が判定される項目に対して、特定のユーザーアカウントが判定されないように設定できます。

判定対象から除外するユーザーを設定するには：

1. 判定除外ユーザー設定ファイルを作成します。
2. 判定除外ユーザー設定ファイルを次のフォルダに格納します。
JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf

判定除外ユーザー設定ファイルに指定したユーザーアカウントのセキュリティ状況が判定されなくなります。

関連リンク

- [付録 A.3 セキュリティ状況の判定除外ユーザー設定ファイルの形式](#)

9.3 セキュリティポリシーを利用する

9.3.1 セキュリティポリシーを追加する手順

セキュリティ画面の「セキュリティポリシー」画面の一覧に、セキュリティポリシーを追加できます。追加したセキュリティポリシーは、コンピュータやグループに割り当ててください。セキュリティポリシーを割り当てると、対象のコンピュータやグループのセキュリティ状況を管理できるようになります。

セキュリティポリシーを追加するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「セキュリティポリシー」－「セキュリティポリシー一覧」を選択します。
3. インフォメーションエリアで「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セキュリティに関するルールを設定して、「OK」ボタンをクリックします。

セキュリティポリシーが追加され、セキュリティポリシーの一覧に表示されます。

ポイント

セキュリティポリシーを新規に作成する場合、デフォルトの設定はデフォルトポリシーと同じです。

関連リンク

- [9.3.2 セキュリティポリシーを編集する手順](#)
- [9.3.3 セキュリティポリシーをコピーする手順](#)
- [9.3.4 セキュリティポリシーを削除する手順](#)
- [9.3.5 セキュリティポリシーを割り当てる手順](#)
- [9.3.6 セキュリティポリシーの割り当てを解除する手順](#)

9.3.2 セキュリティポリシーを編集する手順

組織のセキュリティ方針が変更された場合やセキュリティトレンドを取り入れる場合に、セキュリティポリシーを編集できます。

セキュリティポリシーを編集するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「セキュリティポリシー」－「セキュリティポリシー一覧」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セキュリティポリシーの[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セキュリティに関するルールを編集して、[OK] ボタンをクリックします。

ポイント

ダイアログで[初期値に戻す] ボタンをクリックすると、すべての設定項目をデフォルトに戻せます。

選択したセキュリティポリシーが更新されます。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.3 セキュリティポリシーをコピーする手順](#)
- [9.3.4 セキュリティポリシーを削除する手順](#)
- [9.3.5 セキュリティポリシーを割り当てる手順](#)
- [9.3.6 セキュリティポリシーの割り当てを解除する手順](#)

9.3.3 セキュリティポリシーをコピーする手順

類似したセキュリティポリシーを追加したい場合は、セキュリティポリシーをコピーして、一部だけ変更できます。

セキュリティポリシーをコピーするには：

1. セキュリティ画面を表示します。
2. メニューエリアで[セキュリティポリシー] - [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアでコピーしたいセキュリティポリシーを選択し、[操作メニュー] の[ポリシーをコピーする] を選択します。
4. 表示されるダイアログでセキュリティに関するルールを設定して、[OK] ボタンをクリックします。

コピーしたセキュリティポリシーが一覧に追加されます。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.2 セキュリティポリシーを編集する手順](#)
- [9.3.5 セキュリティポリシーを割り当てる手順](#)

9.3.4 セキュリティポリシーを削除する手順

組織のセキュリティ方針の変更や管理対象のコンピュータの削減に伴って、不要になったセキュリティポリシーを削除できます。

ポイント

コンピュータまたはグループに割り当てられているセキュリティポリシーは削除できません。セキュリティポリシーの割り当てを解除してから削除してください。なお、デフォルトポリシーは削除できません。

セキュリティポリシーを削除するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] - [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアで削除したいセキュリティポリシーを選択し、[操作メニュー] の [ポリシーを削除する] を選択します。
4. 表示されるダイアログで [OK] ボタンをクリックします。

選択したセキュリティポリシーが削除されます。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.6 セキュリティポリシーの割り当てを解除する手順](#)

9.3.5 セキュリティポリシーを割り当てる手順

コンピュータを管理対象にすると、デフォルトポリシーが自動的に割り当てられます。そのため、すぐにデフォルトポリシーに基づいてセキュリティ状況を把握できます。コンピュータおよびグループごとに異なるルールで管理したい場合は、新しいセキュリティポリシーを作成して割り当ててください。割り当てたセキュリティポリシーに基づいて、セキュリティ状況を把握できるようになります。

コンピュータにセキュリティポリシーを割り当てるには：

1. セキュリティ画面を表示します。
2. メニューエリアの [機器のセキュリティ状態] で、セキュリティポリシーを割り当てたいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアでセキュリティポリシーを割り当てたいコンピュータを選択し、[操作メニュー] の [ポリシーを割り当てる] を選択します。

4. 表示されるダイアログで、セキュリティポリシーを選択し [OK] ボタンをクリックします。

対象のコンピュータにセキュリティポリシーが割り当たります。

グループにセキュリティポリシーを割り当てるには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] - [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアでグループに割り当てたいセキュリティポリシーの [グループに割り当て] ボタンをクリックします。
4. 表示されるダイアログで、セキュリティポリシーを割り当てるグループを選択して [OK] ボタンをクリックします。

対象のグループにセキュリティポリシーが割り当たります。

ポイント

セキュリティポリシー設定時にもグループへの割り当てを設定できます。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.6 セキュリティポリシーの割り当てを解除する手順](#)

9.3.6 セキュリティポリシーの割り当てを解除する手順

組織内のセキュリティルールの変更や、セキュリティ管理対象の変更などに応じて、コンピュータおよびグループへのセキュリティポリシーの割り当てを解除できます。

コンピュータのセキュリティポリシーの割り当てを解除するには：

1. セキュリティ画面を表示します。
2. メニューエリアの [機器のセキュリティ状態] で、セキュリティポリシーの割り当てを解除したいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアでセキュリティポリシーの割り当てを解除したいコンピュータを選択し、[操作メニュー] の [ポリシーの割り当てを解除する] を選択します。

セキュリティポリシーの割り当てが解除されます。ほかのセキュリティポリシーが間接的に割り当たっていない場合は、デフォルトポリシーが適用されます。

グループのセキュリティポリシーの割り当てを解除するには：

1. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
2. インフォメーションエリアで割り当てを解除したいセキュリティポリシーの [グループに割り当て] ボタンをクリックします。
3. 表示されるダイアログで、セキュリティポリシーの割り当てを解除したいグループのチェックを外して [OK] ボタンをクリックします。

セキュリティポリシーの割り当てが解除されます。ほかのセキュリティポリシーが間接的に割り当たっていない場合は、デフォルトポリシーが適用されます。

関連リンク

- [9.3.5 セキュリティポリシーを割り当てる手順](#)
- [9.3.4 セキュリティポリシーを削除する手順](#)

9.3.7 セキュリティポリシーにユーザー定義のセキュリティ設定を追加する手順

セキュリティポリシーには、ユーザー定義のセキュリティ設定として、コンピュータのセキュリティ設定に関する任意のポリシーを追加できます。ユーザー定義のセキュリティ設定を追加すると、コンピュータのセキュリティ設定状況が任意の判定条件で判定されます。

ユーザー定義のセキュリティ設定を追加するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアで、[追加] ボタンをクリック、またはユーザー定義のセキュリティ設定を追加したいセキュリティポリシーを選択して [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、[セキュリティ設定項目] – [ユーザー定義のセキュリティ設定] を選択します。
5. [有効にする] ボタンをクリックします。
6. [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、ユーザー定義項目名、定義内容、および不適正時の危険レベルを設定して、[OK] ボタンをクリックします。
8. [OK] ボタンをクリックします。

セキュリティポリシーにユーザー定義のセキュリティ設定が追加されます。

関連リンク

- [9.3.1 セキュリティポリシーを追加する手順](#)
- [9.3.2 セキュリティポリシーを編集する手順](#)

9.3.8 セキュリティの判定結果に応じて機器のネットワーク接続を制御する手順

セキュリティポリシーのアクション項目では、セキュリティの判定結果に応じて、対象のコンピュータのネットワーク接続を制御できます。

なお、ネットワーク接続を制御するためには、対象のコンピュータが所属するネットワークセグメントが監視されている必要があります。ネットワーク接続を監視するための方法については、「[8. 機器のネットワーク接続を管理する](#)」を参照してください。

ポイント

機器画面の「機器情報」－「機器一覧」画面で対象のコンピュータを選択して、「操作メニュー」からネットワーク接続を遮断または許可することもできます。

セキュリティの判定結果に応じて機器のネットワーク接続を遮断および許可するには：

セキュリティポリシーの判定結果によって、ネットワーク接続を遮断および許可するときに必要な設定を次に示します。

1. セキュリティ画面を表示します。
2. 「セキュリティポリシー」－「セキュリティポリシー一覧」画面で、メッセージを通知したいコンピュータに割り当てているセキュリティポリシーの「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「アクション項目」－「ネットワーク接続制御」を選択します。
4. 「有効にする」ボタンをクリックします。
5. ネットワーク接続を遮断する危険レベルや接続拒否の条件を設定して、「OK」ボタンをクリックします。

セキュリティポリシーの判定結果が設定した危険レベルを超えると、対象のコンピュータのネットワーク接続が遮断されます。ネットワーク接続が遮断された場合、対象のコンピュータの利用者にセキュリティ対策を実施するように連絡してください。セキュリティ状態が適正になり設定した危険レベルを下回ると、ネットワーク接続が自動的に許可されます。

9.4 セキュリティポリシー違反を強制対策する手順

セキュリティポリシーに違反したコンピュータは、管理用サーバからリモートで強制対策できます。強制対策できる項目は、セキュリティの設定項目で自動対策できる項目だけです。

なお、セキュリティポリシーに違反したコンピュータを強制対策するには、対象のコンピュータにオンライン管理用のエージェントがインストールされている必要があります。

セキュリティポリシー違反を強制対策するには：

1. セキュリティ画面を表示します。
2. メニューエリアの「機器のセキュリティ状態」で、セキュリティポリシー違反を強制対策したいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアで、セキュリティポリシー違反を強制対策したいコンピュータを選択し、[セキュリティ対策を実行] ボタンをクリックします。
複数のコンピュータを選択して一括対策することもできます。
4. 表示されるダイアログで、セキュリティ対策を実行する対策項目にチェックして、[OK] ボタンをクリックします。

セキュリティ対策が実行され、対象のコンピュータが適正状態になります。

ポイント

強制対策は、[セキュリティポリシー] - [セキュリティポリシー一覧] 画面のインフォメーションエリア下部に表示されるタブからも実施できます。

9.5 利用者にメッセージを通知する手順

コンピュータの利用者に通知したいメッセージがある場合は、メッセージを作成して個別に通知できます。また、セキュリティの判定結果に応じて、自動的にメッセージを通知することもできます。

なお、メッセージを通知できるのは、オンライン管理のコンピュータだけです。

ポイント

機器画面の「機器情報」－「機器一覧」画面からメッセージを通知することもできます。詳細については、「[6.22 利用者にメッセージを通知する手順](#)」を参照してください。

利用者にメッセージを通知するには：

1. セキュリティ画面を表示します。
2. メニューエリアの「機器のセキュリティ状態」でメッセージを通知したいコンピュータが含まれるグループを選択します。
3. インフォメーションエリアで、メッセージを通知したいコンピュータを選択して、「利用者へメッセージ通知」ボタンをクリックします。
複数のコンピュータを選択して、同じ内容のメッセージを一斉に通知することもできます。
4. 表示されるダイアログで、通知するメッセージを設定して、「OK」ボタンをクリックします。
「ノートに追記する」をチェックすると、メッセージを通知した履歴や理由などを記録できます。ここで入力した情報は「ノート」タブに追記されます。

コンピュータの利用者にメッセージが通知されます。

自動でメッセージを通知するには：

1. セキュリティ画面を表示します。
2. 「セキュリティポリシー」－「セキュリティポリシー一覧」画面で、メッセージを通知したいコンピュータに割り当てているセキュリティポリシーの「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「アクション項目」－「利用者へのメッセージ通知」を選択します。
4. 通知する危険レベルやメッセージを設定して、「OK」ボタンをクリックします。

セキュリティポリシーの判定結果が設定した危険レベルを超えると、対象のコンピュータにメッセージが通知されます。

9.6 デバイスの使用を抑止する手順

禁止操作のポリシーを設定して、デバイスに対しての書き込み、または読み取りを抑止できます。

デバイスの使用を抑止するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアで編集するセキュリティポリシーを選択して、[編集] ボタンをクリックします。
新しくセキュリティポリシーを追加する場合は、[追加] ボタンをクリックします。
4. セキュリティ設定項目の [禁止操作] をクリックします。
画面が非活性の場合は、機器の使用抑止の設定が無効になっています。左上の [有効にする] ボタンをクリックすると、設定が有効になります。
5. [機器の使用抑止] で、使用を抑止するデバイスを設定します。
6. 使用を抑止したことを示すメッセージを、利用者のコンピュータに表示したい場合は、[抑止メッセージ表示デバイスの一覧] で、メッセージを表示するデバイスを設定します。
メッセージが表示できるのは、機器の使用抑止の対象に設定されているデバイスだけです。
7. 書き込みだけを抑止したいデバイスがある場合は、[書き込み抑止デバイスの一覧] で、書き込みを抑止したいデバイスを設定します。
書き込みだけを抑止できるのは、使用を許可しているデバイスだけです。なお、書き込みだけを抑止できるデバイスはコンピュータの OS によって異なります。OS ごとの抑止できるデバイスについては、マニュアル「JP1 Version 10 JP1/IT Desktop Management 2 導入・設計ガイド」を参照してください。
8. [OK] ボタンをクリックします。

禁止操作のポリシーに設定した内容で、デバイスの使用が抑止されます。

USB デバイスの抑止を設定する場合に、[登録済みの USB デバイスは使用を許可する] を選択すると、ハードウェア資産情報が登録されている USB デバイスは抑止の対象外にできます。USB デバイスを登録する方法については、[9.7 USB デバイスを登録する手順] を参照してください。

ポイント

[書き込み抑止デバイスの一覧] で書き込み抑止を設定したセキュリティポリシーを割り当てると、対象のコンピュータに再起動を促すメッセージが表示されます。メッセージに従って対象のコンピュータが再起動されると、その時点で有効になります。

ポイント

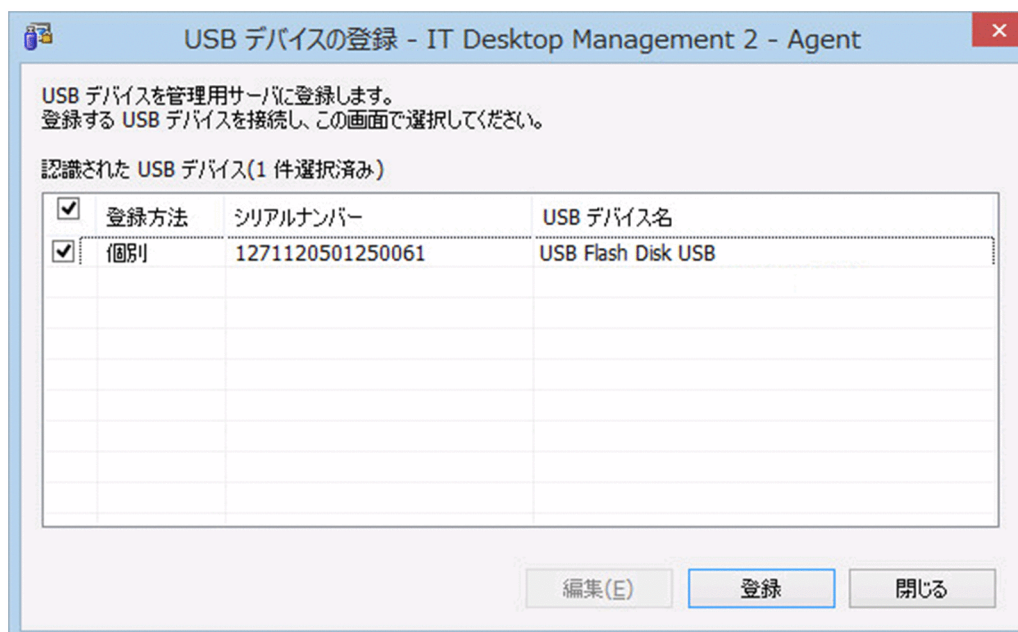
内蔵 CD/DVD ドライブ、または内蔵 FD ドライブの使用抑止を設定した場合、このデバイスを持つコンピュータでイベントが発生するため、ユーザーの操作に関わらず、一時的に禁止操作のセキュリティ評価が悪化する場合があります。

9.7 USB デバイスを登録する手順

オンライン管理用のエージェントをインストールしているコンピュータに USB デバイスを接続して、USB デバイスのハードウェア資産情報を登録できます。

USB デバイスを登録するには：

1. オンライン管理用の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] - [JP1_IT Desktop Management 2 - Agent] - [管理者ツール] - [USB デバイスの登録] を選択します。
[USB デバイスの登録] ダイアログが表示されます。



エージェントに USB デバイス登録時の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。デフォルトでは、JP1/IT Desktop Management 2 のデフォルトパスワードの「manager」が設定されています。

3. 登録する USB デバイスをコンピュータに接続します。

注意事項

USB デバイスには、個別に認識できるデバイスと、製品単位で認識されるデバイスがあります。製品単位で認識される USB デバイスを接続すると、確認のメッセージが表示されます。製品単位で認識される USB デバイスを登録すると、同じ製品の異なるデバイスを登録しても同じハードウェア資産として扱われます。このため、セキュリティポリシーで USB デバイスの使用抑止を設定している場合、製品単位で USB デバイスの使用が許可されます。

4. 製品単位で認識される USB デバイスを登録する場合は、[認識された USB デバイス] で登録する USB デバイスを選択して、[編集] ボタンをクリックしてください。

個別に認識される USB デバイスを登録する場合は、手順 7.に進んでください。

5. 表示されるダイアログで、[製品単位] を選択して [詳細設定] ボタンをクリックします。
6. 表示されるダイアログで、[登録条件] を編集して [OK] ボタンをクリックします。
[登録条件] には、USB デバイスを識別するために使われる、デバイスインスタンス ID の固定部分を指定します。例えば、デバイスインスタンス ID が「USB¥VID_xxxx&PID_003F」だった場合に、「PID_003F」の「3F」の部分が環境によって変化するときは、「USB¥VID_xxxx&PID_00」までを指定します。
7. [認識された USB デバイス] で登録する USB デバイスを選択して、[登録] ボタンをクリックします。
8. 表示されるダイアログで資産状態を確認するかどうかを設定して、[OK] ボタンをクリックします。
必要に応じて、USB デバイスのハードウェア資産情報に登録する登録者の情報を入力してください。
選択した USB デバイスの情報が収集されて、「未確認」のハードウェア資産として登録されます。
9. JP1/IT Desktop Management 2 にログインします。
10. 資産画面の [ハードウェア資産] 画面で、登録された USB デバイスの [資産状態] を「滅却」以外に変更します。

USB デバイスの登録が完了します。

注意事項

USB デバイスの使用を抑止している場合、コンピュータ上で [USB デバイスの登録] ダイアログが表示されている間は、そのコンピュータで一時的に USB デバイスの抑止機能が無効になります。

ポイント

- USB デバイスのデバイスインスタンス ID は、前方一致で判定します。
- 一部のセキュリティ機能付きの USB デバイスには、認証前後でデバイスインスタンス ID が変化するものがあります。そのようなデバイスを登録する場合は、認証前後のデバイスインスタンス ID をそれぞれ登録する必要があります。

ポイント

オンライン管理用のエージェントをインストールしているコンピュータに、登録済みの個別に認識される USB デバイスを接続すると、USB デバイスに格納されているファイルの情報が収集されます。収集された情報は、資産画面の [ハードウェア資産] 画面の [格納ファイル一覧] タブに表示されます。なお、[格納ファイル一覧] タブは [機器種別] が「USB デバイス」の場合だけ表示されます。製品単位で認識される USB デバイスの場合、ファイルの情報は収集されません。

9.8 更新プログラムを管理する

9.8.1 更新プログラムを自動配布する手順

管理者が設定したセキュリティポリシーに従って、自動的に更新プログラムをダウンロードして、管理対象のコンピュータに配布できます。

例えば、セキュリティ対策の一環として、更新プログラムが適用されていないコンピュータに対して、更新プログラムを自動配布するようセキュリティポリシーに設定します。すると、日本マイクロソフト社から更新プログラムがダウンロードされて、自動で更新プログラムファイルが登録されます。そして、セキュリティの判定結果に従って、更新プログラムファイルがコンピュータに自動で配布されます。

更新プログラムを自動で配布するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリア上部の [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、[更新プログラム] をクリックします。
5. 表示されるダイアログで、[更新プログラム適用] の [有効] をチェックして [設定項目]、[適正状態]、および [不適正時の危険レベル] を指定します。さらに、[自動対策] にチェックしたあと、[更新プログラムを配布 (ITDM 互換配布)] を選択して、[OK] ボタンをクリックします。
6. メニューエリアの [機器のセキュリティ状態] で、更新プログラムを自動配布したいコンピュータが含まれるグループを選択します。
7. インフォメーションエリア上部で、更新プログラムを自動配布したいコンピュータを選択して、[操作メニュー] の [ポリシーを割り当てる] を選択します。
8. 表示されるダイアログで、割り当てるセキュリティポリシーを選択して、[OK] ボタンをクリックします。

更新プログラムが適用されていないコンピュータに、自動で更新プログラムが適用されます。

関連リンク

- [9.8.2 更新プログラムを手動で登録して配布する手順](#)

9.8.2 更新プログラムを手動で登録して配布する手順

更新プログラムは自動で配布するほかに、管理者が手動で登録してから配布することもできます。セキュリティに関する重要な更新プログラムを、JP1/IT Desktop Management 2 の自動配布を待たないで至急配布したいときなどに手動で登録してから配布します。

更新プログラムを手動で登録してから配布する場合、更新プログラムのダウンロードおよび更新プログラムファイルの登録をすべて管理者自身で行ってください。

更新プログラムを手動で登録してから配布するには：

1. 更新プログラムをダウンロードします。

更新プログラムは、日本マイクロソフト社の Web サイトからダウンロードできます。

2. セキュリティ画面を表示します。

3. メニューエリアで [更新プログラム] - [更新プログラム一覧] を選択します。

4. インフォメーションエリアの [操作メニュー] から [更新プログラムを追加する] を選択します。

5. 表示されるダイアログで、追加する更新プログラムの情報を入力します。また、[更新プログラムファイルを登録する] をチェックして、登録に必要な情報も入力します。入力が完了したら、[OK] ボタンをクリックします。

[更新プログラム一覧] に、更新プログラムが追加されて、更新プログラムファイルが登録されます。

ポイント

特定の更新プログラムだけを適用させる運用にしている場合は、更新プログラムグループに更新プログラムを追加してください。更新プログラムグループが設定されているセキュリティポリシーの自動対策の設定に従って、対象のコンピュータに更新プログラムが適用されます。

更新プログラムが、セキュリティポリシーの自動対策の設定に従って、対象のコンピュータに適用されます。

ポイント

管理者のコンピュータがインターネットに接続できない環境の場合、インターネットに接続できるコンピュータで日本マイクロソフト社の Web サイトから更新プログラムをダウンロードして、そのデータを使用することで、更新プログラムファイルを登録できます。

9.8.3 更新プログラム一覧へ更新プログラムを手動で追加する手順

管理用サーバがインターネットに接続できない環境のため、更新プログラム一覧を自動的に更新できない場合は、ほかにインターネット接続できるコンピュータを利用して、管理者が手動で更新プログラム情報を更新できます。

また、サポートサービスサイトから情報を取得するよりも早く、更新プログラムの情報を一覧へ追加したい（セキュリティの判定対象としたい）場合は、更新プログラムを手動で追加することもできます。

管理用サーバがインターネットに接続できない場合に更新プログラム一覧を手動で更新するには：

1. インターネット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ます。
2. サポートサービスサイトから「更新プログラム一覧のオフライン更新用サポート情報ファイル」をダウンロードします。
3. コンピュータから、セキュリティ画面を表示します。
4. メニューエリアで「更新プログラム」－「更新プログラム一覧」を選択します。
5. 「操作メニュー」の「サポートサービスからの情報をオフライン更新する」を選択します。
6. 表示されるダイアログでダウンロードしたファイルを指定して、「OK」ボタンをクリックします。

ダウンロードしたファイルがアップロードされ、更新プログラム一覧が更新されます。

サポートサービスサイトから情報を取得するよりも早く更新プログラム一覧へ更新プログラムを手動で追加するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「更新プログラム」－「更新プログラム一覧」を選択します。
3. 「操作メニュー」の「更新プログラムを追加する」を選択します。
4. 表示されるダイアログで追加する更新プログラムの情報を入力して、「OK」ボタンをクリックします。
追加する更新プログラムの情報は、日本マイクロソフト社の Web サイトで確認してください。

入力した更新プログラムの情報が、更新プログラム一覧に追加されます。

9.8.4 更新プログラムの手動登録手順

更新プログラムを手動で登録する場合、日本マイクロソフト社の Web サイトから更新プログラムの情報を確認して、更新プログラム登録時に情報を設定する必要があります。

必須更新プログラムを手動で登録するには：

1. セキュリティのページを表示します。

日本マイクロソフト社の Web サイトのトップページから、セキュリティのページ（セキュリティホーム）を表示します。

2. セキュリティのページから、更新プログラムの詳細情報を確認します。

セキュリティのページの更新プログラムへのリンクをクリックして表示される、更新プログラムの情報ページ（セキュリティ情報）で詳細情報を確認します。

ポイント

詳細情報は、登録時に作業しやすいように表示したままにしておくことをお勧めします。

3. JP1/IT Desktop Management 2 に更新プログラムを登録します。

セキュリティ画面の［更新プログラム一覧］画面で、［操作メニュー］の［更新プログラムを追加する］をクリックします。

4. 表示されるダイアログで、更新プログラムの情報を入力して［OK］ボタンをクリックします。

更新プログラム情報が登録されます。

日本マイクロソフト社の Web サイトで確認した更新プログラム情報と、各項目に設定する値の対応例を次の図に示します。

更新プログラム名 リリース日 セキュリティ情報番号 詳細情報URL

サポート技術情報番号

更新プログラム情報の表示例

マイクロソフト セキュリティ情報 **MSnn-nnn - 重要**

XXXの脆弱性により、XXXが実行される (999999)
 公開日: 2011年4月12日 最終更新日: 2011年6月13日

概説

要点
 . . .

USマイクロソフトセキュリティ情報: <http://www.xxxxx/xxx/xxxx.xxx>

. . .

影響を受けるソフトウェアおよびそのダウンロード先:
 . . .

オペレーティング システム/ソフトウェア	コンポーネント	. . .
Windows Vista		
Microsoft Windows Vista	Microsoft XML コア サービス 3.0 (KB955xxx)	. . .
Microsoft Windows Vista	Microsoft XML コア サービス 4.0 (KB954xxx)	. . .
Internet Explorer 8		
Microsoft Windows Vista	Microsoft Internet Explorer 8 Service Pack 1	. . .
. . .	. . .	. . .

更新プログラムの適用対象: 「Windows」

更新プログラムの適用対象: 「製品」
 製品名: 「Microsoft Internet Explorer」
 バージョン: 「8」
 サービスパック: 「Service Pack 1」

9.8.5 更新プログラムファイルを登録する手順

更新プログラムを手動で登録してから配布する際に、更新プログラムファイルを登録する必要があります。

ポイント

管理用サーバがサポートサービスサイトおよび日本マイクロソフト社のサイトと接続できる場合、セキュリティポリシーの自動対策で更新プログラムの配布を設定しているときは、自動対策が実行されるタイミングで、配布される更新プログラムファイルが自動的に登録されます。

ポイント

[更新プログラム一覧] 画面に表示されていない更新プログラムファイルを登録する場合、あらかじめ更新プログラム情報を登録しておく必要があります。更新プログラム情報の登録方法については、「[9.8.3 更新プログラム一覧へ更新プログラムを手動で追加する手順](#)」を参照してください。

ポイント

手動で登録した更新プログラム情報の更新プログラムファイルを登録する場合、または管理用サーバがインターネット接続できない場合は、登録する更新プログラムの実行ファイルを、あらかじめ日本マイクロソフト社のサイトからダウンロードしておく必要があります。

更新プログラム一覧をオフラインで更新している場合、[更新プログラム] 画面の [更新プログラムの情報] タブに表示される [更新プログラムのダウンロード URL] から、更新プログラムをダウンロードできます。

更新プログラムファイルを登録するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [更新プログラム] - [更新プログラム一覧] を選択します。
3. インフォメーションエリアで更新プログラムファイルを登録したい更新プログラムを選択して、[操作メニュー] の [更新プログラムファイルを登録する] を選択します。
4. 表示されるダイアログで更新プログラムファイルの登録情報を設定し、[OK] ボタンをクリックします。

更新プログラムファイルが登録されて、一覧の [登録状態] 欄に  が表示されます。

なお、登録された更新プログラムファイルは、配布 (ITDM 互換) 画面の [パッケージ一覧] 画面には追加されません。更新プログラムファイルは、セキュリティポリシーの自動対策だけで配布できます。手動で更新プログラムを配布するタスクを作成することはできません。実行されたタスクは配布 (ITDM 互換) 画面で確認できます。

9.8.6 更新プログラムグループを作成する手順

更新プログラムをメニューエリアで任意のグループに振り分けて管理できます。このグループのことを更新プログラムグループと呼びます。

更新プログラムグループを作成することで、更新プログラムの管理に次のように活用できます。

- 異なるセキュリティポリシー間で、更新プログラムの判定条件に同じ更新プログラムグループを指定することで、判定対象とする更新プログラムを一元管理できる。

- 適用しても問題ないかテストしてからコンピュータに適用する場合に、テストが完了した更新プログラムを更新プログラムグループに登録して自動配布できる。

更新プログラムグループを作成するには：

1. セキュリティ画面を表示します。
2. メニューエリアの [更新プログラム] – [更新プログラムグループ] にマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるテキストエリアにグループの名称を入力します。

メニューエリアに更新プログラムグループが追加されます。

ポイント

更新プログラムグループは、メニューエリアの [更新プログラムグループ] を右クリックして表示されるメニューから作成することもできます。

関連リンク

- [9.8.8 更新プログラムグループを削除する手順](#)
- [9.8.7 更新プログラムグループ名を変更する手順](#)
- [9.8.9 更新プログラムグループに更新プログラムを追加する 手順](#)
- [9.8.10 更新プログラムグループから更新プログラムを削除する手順](#)

9.8.7 更新プログラムグループ名を変更する手順

グルーピングしていた情報の観点が変更になった場合などに、更新プログラムグループ名を変更できます。

更新プログラムグループ名を変更するには：

1. セキュリティ画面を表示します。
2. メニューエリアの [更新プログラム] – [更新プログラムグループ] で変更したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。

5. 表示されるテキストエリアに更新プログラムグループの名称を入力します。

更新プログラムグループ名が変更されます。

ポイント

メニューエリアの更新プログラムグループを右クリックして表示されるメニューから変更することもできます。

関連リンク

- [9.8.6 更新プログラムグループを作成する手順](#)
- [9.8.8 更新プログラムグループを削除する手順](#)
- [9.8.9 更新プログラムグループに更新プログラムを追加する 手順](#)
- [9.8.10 更新プログラムグループから更新プログラムを削除する手順](#)

9.8.8 更新プログラムグループを削除する手順

不要になった更新プログラムグループを削除できます。

更新プログラムグループを削除するには：

1. セキュリティ画面を表示します。
2. メニューエリアの [更新プログラム] - [更新プログラムグループ] で削除したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるダイアログで [OK] ボタンをクリックします。

更新プログラムグループが削除されます。

ポイント

メニューエリアの更新プログラムグループを右クリックして表示されるメニューから削除することもできます。

関連リンク

- [9.8.6 更新プログラムグループを作成する手順](#)

- 9.8.7 更新プログラムグループ名を変更する手順
- 9.8.9 更新プログラムグループに更新プログラムを追加する 手順
- 9.8.10 更新プログラムグループから更新プログラムを削除する手順

9.8.9 更新プログラムグループに更新プログラムを追加する 手順

判定対象とする更新プログラムをグルーピングするには、作成した更新プログラムグループに更新プログラム情報を追加します。

更新プログラムグループに更新プログラムを追加するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [更新プログラム] – [更新プログラム一覧] をクリックします。
3. 更新プログラムグループに追加したい情報をインフォメーションエリアに表示します。
4. 追加したい情報を選択して、[操作メニュー] の [更新プログラムグループに追加する] を選択します。
5. 表示されるダイアログで、追加する更新プログラムグループを選択して [OK] ボタンをクリックします。

選択した更新プログラムグループに、情報が追加されます。

ポイント

インフォメーションエリアの情報を右クリックして、[更新プログラムグループに追加する] を選択して追加することもできます。

ポイント

インフォメーションエリアの情報を、メニューエリアの任意の更新プログラムグループにドラッグ & ドロップして追加することもできます。

関連リンク

- 9.8.6 更新プログラムグループを作成する手順
- 9.8.8 更新プログラムグループを削除する手順
- 9.8.7 更新プログラムグループ名を変更する手順
- 9.8.10 更新プログラムグループから更新プログラムを削除する手順

9.8.10 更新プログラムグループから更新プログラムを削除する手順

更新プログラムグループに追加した更新プログラムを、セキュリティの判定対象から外したい場合、更新プログラムグループに追加した情報を削除できます。

更新プログラムグループから更新プログラムを削除するには：

1. セキュリティ画面を表示します。
2. メニューエリアの[更新プログラム]－[更新プログラムグループ]で、情報を削除したい更新プログラムグループを選択します。
3. インフォメーションエリアで削除したい情報を選択して、[操作メニュー]の[更新プログラムグループから削除する]を選択します。
4. 表示されるダイアログで[OK]ボタンをクリックします。

選択した更新プログラムグループから、情報が削除されます。

ポイント

インフォメーションエリアの情報を右クリックして、[更新プログラムグループから削除する]を選択して削除することもできます。

関連リンク

- [9.8.6 更新プログラムグループを作成する手順](#)
- [9.8.8 更新プログラムグループを削除する手順](#)
- [9.8.7 更新プログラムグループ名を変更する手順](#)
- [9.8.9 更新プログラムグループに更新プログラムを追加する 手順](#)

9.9 禁止操作の抑止イベントと操作ログを上位システムに通知する間隔を設定する手順

禁止操作の抑止イベントと操作ログを、利用者のコンピュータから上位システムに通知する間隔を設定できます。分単位または日単位で設定できます。

禁止操作の抑止イベントと操作ログを上位システムに通知する間隔を設定するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアで編集するセキュリティポリシーを選択して、[編集] ボタンをクリックします。
新しくセキュリティポリシーを追加する場合は、[追加] ボタンをクリックします。
4. セキュリティ設定項目の [禁止操作と操作ログの共通設定] をクリックします。
5. [禁止操作／操作ログの、上位システムへの通知間隔] で、禁止操作の抑止イベントと操作ログを、利用者のコンピュータから上位システムに通知する間隔を設定します。
6. [OK] ボタンをクリックします。

禁止操作と操作ログの共通設定のポリシーに設定した内容で、禁止操作の抑止イベントと操作ログを上位システムに通知する間隔が設定されます。

9.10 禁止操作の抑止イベントと操作ログを保持する期間を設定する手順

禁止操作の抑止イベントと操作ログを上位システムに通知するまでの間、利用者のコンピュータ側で保持する期間の最大日数を設定できます。

禁止操作の抑止イベントと操作ログを保持する期間を設定するには：

1. セキュリティ画面を表示します。
2. メニューエリアで [セキュリティポリシー] – [セキュリティポリシー一覧] を選択します。
3. インフォメーションエリアで編集するセキュリティポリシーを選択して、[編集] ボタンをクリックします。
新しくセキュリティポリシーを追加する場合は、[追加] ボタンをクリックします。
4. セキュリティ設定項目の [禁止操作と操作ログの共通設定] をクリックします。
5. [禁止操作／操作ログの、利用者のコンピュータでの保持期間] で、禁止操作の抑止イベントと操作ログを保持する期間を設定します。
6. [OK] ボタンをクリックします。

禁止操作と操作ログの共通設定のポリシーに設定した内容で、禁止操作の抑止イベントと操作ログを保持する期間が設定されます。

10

操作ログを管理する

ここでは、利用者の操作を把握および追跡する方法について説明します。

10.1 管理用サーバへの操作ログの収集を設定する手順

コンピュータから操作ログを収集して、管理用サーバに格納するための設定方法について説明します。

■ 注意事項

操作ログを取得するためには、対象のコンピュータにエージェントが導入されている必要があります。

管理用サーバへの操作ログの収集を設定するには：

1. セットアップで操作ログの取得を有効にします。

操作ログで使用するフォルダやディスク所要量などを設定します。

2. セキュリティポリシーで操作ログの取得を設定します。

取得する操作ログの種類を選択できます。不審操作を検知する場合は、検知の条件も設定できます。

3. セキュリティポリシーをグループまたはコンピュータに割り当てます。

セキュリティポリシーが割り当てられたコンピュータの操作ログが、管理用サーバに収集されます。

関連リンク

- [\(2\) セキュリティポリシーの管理](#)
- [10.2 操作ログを確認する手順](#)

10.2 操作ログを確認する手順

管理用サーバに保管された利用者の操作ログを一覧で確認できます。ファイルの持ち込みまたは持ち出しを追跡したり、操作を行ったコンピュータを特定したりすることで、情報漏えいの早期発見および対策ができます。

ポイント

操作ログを取得するには、セットアップ時に操作ログの設定が必要です。また、操作ログのポリシーを有効にしている必要があります。

操作ログを確認するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「操作ログ」－「操作ログ一覧」を選択します。

インフォメーションエリアに操作ログが表示されます。表示された操作ログは、スクロールバーの   をクリックすると1日単位、  をクリックすると1か月単位でスクロールできます。

画面の上部には、タイムチャートが表示され、画面上に表示されている日付が青色の枠で囲まれます。日付のボタンをクリックすると、その日付の操作ログが先頭に表示されます。なお、マウスカーソルを合わせたときに「操作ログなし」と表示される日付はクリックできません。タイムチャートの幅が長い場合は、 または  をクリックしてスライドできます。

フィルタを使って情報を絞り込むと、対象の日付が緑色の枠で囲まれます。

セキュリティポリシーで、ファイル持ち出しによる不審と見なす操作を設定している場合、ファイル持ち出しによる不審と見なす操作として検知された操作ログには、「不審操作」欄に  が表示されます。一覧からファイル持ち出しによる不審と見なす操作の操作ログを探す場合、この項目でフィルタすると便利です。

ポイント

セットアップ時に、操作ログの保管先フォルダを設定しておく、と、操作ログがバックアップされます。設定画面の「操作ログの設定」－「操作ログの自動取り込み」－「自動取り込みされる操作ログの格納期間」で指定した期間より前の操作ログはデータベースから削除されるため、過去の操作ログを参照したい場合は、バックアップした操作ログを取り込んでください。

ポイント

操作ログの表示に時間が掛かる場合は、[操作日時（Web ブラウザのロケール）] で検索範囲を絞り込み、[部署]、[設置場所]、[発生元]、[ユーザ名]などで検索対象の機器を絞り込んでください。

注意事項

管理用サーバに操作ログが取得されていない場合、[操作ログ] 画面は表示されません。

ポイント

操作ログは、`ioutils exportoplog` コマンドを実行してエクスポートすることもできます。操作ログの内容を資料に使用したい場合などは、エクスポートすることをお勧めします。

ポイント

機器画面で選択した機器の操作ログを確認することもできます。

機器画面の[機器情報]－[機器一覧]画面で、[操作メニュー]の[操作ログへ]を選択すると、セキュリティ画面に切り替わり、機器の操作ログを確認できます。

関連リンク

- [10.4 不審操作のログを確認する手順](#)
- [10.6 操作ログを追跡調査する手順](#)
- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [17.16 ioutils exportoplog（操作ログのエクスポート）](#)

10.3 不審と見なす操作を検知するための設定手順

不審と見なす操作を検知するには、操作ログのポリシーで「不審と見なす操作」を設定する必要があります。

不審と見なす操作を設定するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「セキュリティポリシー」－「セキュリティポリシー一覧」を選択します。
3. インフォメーションエリアで編集するセキュリティポリシーを選択して、「編集」ボタンをクリックします。
新しくセキュリティポリシーを追加する場合は、「追加」ボタンをクリックします。
4. セキュリティ設定項目の「操作ログ」をクリックします。
画面が非活性の場合は、操作ログのポリシーが無効になっています。左上の「有効にする」ボタンをクリックすると、ポリシーが有効になります。
5. 「不審と見なす操作」で、不審と見なす操作を設定します。
6. 「OK」ボタンをクリックします。

不審と見なす操作が検知されると、セキュリティ画面にはファイル持ち出しによる不審操作のログが、イベント画面にはすべての不審操作のイベントが表示されます。

関連リンク

- [10.4 不審操作のログを確認する手順](#)
- [10.5 不審操作のイベントを確認する手順](#)

10.4 不審操作のログを確認する手順

操作ログのポリシーの「不審と見なす操作」で次に示す項目を1つ以上チェックした場合、不審と見なす操作が検知されると、セキュリティ画面にファイル持ち出しによる不審操作のログが表示されます。

- 「添付ファイル付きメールの送受信」
- 「Web/FTP サーバの使用」
- 「外部メディア（リムーバブルディスク）へのファイルコピーと移動」

不審操作のログを確認するには：

1. セキュリティ画面を表示します。
2. メニューエリアで「操作ログ」－「操作ログ一覧」を選択します。
3. フィルタを利用して、「不審操作」が警戒のアイコン（) の操作ログを表示します。

不審操作のログが表示されます。操作ログの詳細を確認して、必要に応じて対処してください。

関連リンク

- [10.5 不審操作のイベントを確認する手順](#)
- [10.2 操作ログを確認する手順](#)
- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [10.6 操作ログを追跡調査する手順](#)

10.5 不審操作のイベントを確認する手順

操作ログのポリシーで「不審と見なす操作」を設定すると、不審と見なす操作が検知された場合、イベント画面に不審操作のイベントが表示されます。

不審操作のイベントを確認するには：

1. イベント画面を表示します。
2. フィルタを利用して、「種類」が「不審操作」のイベントを表示します。

不審操作のイベントが表示されます。イベントの詳細を確認して、必要に応じて対処してください。

ポイント

不審操作のイベントが発生したときに自動的にメールで通知するように設定できます。

関連リンク

- [10.4 不審操作のログを確認する手順](#)
- [15.7.1 イベント通知の設定をする手順](#)

10.6 操作ログを追跡調査する手順

利用者が操作したファイルについて、そのファイルがいつ作成されたか、どこから持ち込まれたか、およびどこに持ち出されたかを追跡調査できます。追跡結果を確認して、情報漏えいなどの問題が発生していないか調査してください。

操作ログをトレースするには：

1. セキュリティ画面を表示します。
2. メニューエリアで [操作ログ] – [操作ログ一覧] を選択します。
3. インフォメーションエリアで、追跡したい操作ログの [追跡] ボタンをクリックします。

[操作の追跡] ダイアログに、選択した操作ログを基点とした追跡結果が表示されます。

[操作内容] のリンクをクリックすると、操作ログの詳細を確認できます。

ポイント

バックアップされた過去の操作ログを含めて追跡調査する場合は、あらかじめ過去の操作ログを取り込んでください。過去の操作ログを取り込む方法については、「[10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)」を参照してください。

ポイント

操作ログは、`ioutils exportoplog` コマンドを実行してエクスポートすることもできます。操作ログの内容を資料に使用したい場合などは、エクスポートすることをお勧めします。

関連リンク

- [10.2 操作ログを確認する手順](#)
- [10.4 不審操作のログを確認する手順](#)
- [17.16 ioutils exportoplog（操作ログのエクスポート）](#)

10.7 過去の操作ログを取り込む

10.7.1 管理用サーバに過去の操作ログを取り込む手順

操作ログのデータベースに操作ログがすでに存在しない場合に、操作ログのバックアップから過去の操作ログを取り込みます。JP1/IT Desktop Management の操作ログを取り込むこともできます。

注意事項

該当する範囲の操作ログが操作ログの保管先フォルダから削除されている場合は、取り込みません。

ポイント

過去の操作ログを取り込むには、セットアップの［操作ログの設定］画面で操作ログの保管先などを設定する必要があります。なお、取り込める操作ログのデータ量は、セットアップの［操作ログの設定］画面の［必要なディスク容量］に応じて決まっています。より長い範囲の操作ログを取り込みたい場合は、［操作ログのデータベース格納最大日数］を長く設定するか、設定画面の［操作ログの設定］画面の［自動取り込みされる操作ログの格納期間］を短く設定してください。

過去の操作ログを取り込むには：

1. セキュリティ画面を表示します。
2. メニューエリアで［操作ログ］－［操作ログ一覧］を選択します。
3. ［操作メニュー］の［保管した操作ログを手動で取り込む］を選択します。

注意事項

操作ログのバックアップファイルが存在しない場合は選択できません。

4. 表示されるダイアログで操作ログを取り込む範囲を設定して、[OK] ボタンをクリックします。

操作ログの取り込みが開始され、取り込み状況が表示されます。

5. [閉じる] ボタンをクリックします。

設定した範囲の操作ログが取り込まれます。取り込み済みのデータに設定した範囲の一部が含まれている場合は、それ以外の範囲が取り込まれます。

［保管した操作ログを手動で取り込む］では、取り込み対象のコンピュータを指定できます。取り込み範囲が長い場合や取り込み対象のコンピュータが多い場合は操作ログの量が膨大になるため、取り込みに時間が掛かるおそれがあります。取り込み対象のコンピュータを指定して、取得する操作ログを絞り込むこと

をお勧めします。操作ログの取り込み対象のコンピュータを指定する手順については、「[10.7.2 コンピュータを選択して操作ログを取り込む手順](#)」を参照してください。

ポイント

以前に取り込んだデータ量が多くて取り込める範囲が不足する場合は、[操作メニュー] の [手動取り込み済みの操作ログを削除する] で不要な期間を削除してから、操作ログを取り込んでください。

ポイント

操作ログは、`ioutils exportoplog` コマンドを実行してエクスポートすることもできます。操作ログの内容を資料に使用したい場合などは、エクスポートすることをお勧めします。

関連リンク

- [10.2 操作ログを確認する手順](#)
- [10.6 操作ログを追跡調査する手順](#)
- [10.4 不審操作のログを確認する手順](#)
- [15.3.2 操作ログを自動的に取り込む手順](#)
- [17.16 ioutils exportoplog \(操作ログのエクスポート\)](#)

10.7.2 コンピュータを選択して操作ログを取り込む手順

取り込み範囲が長い場合や取り込み対象のコンピュータが多い場合は、取り込む対象のコンピュータを選択して操作ログを取り込めます。JP1/IT Desktop Management の操作ログを取り込むこともできます。

注意事項

該当する範囲の操作ログが操作ログの保管先フォルダから削除されている場合は、取り込めません。

ポイント

過去の操作ログを取り込むには、セットアップの [操作ログの設定] 画面で操作ログの保管先などを設定する必要があります。なお、取り込める操作ログのデータ量は、セットアップの [操作ログの設定] 画面の [必要なディスク容量] に応じて決まっています。より長い範囲の操作ログを取り込みたい場合は、[操作ログのデータベース格納最大日数] を長く設定するか、設定画面の [操作ログの設定] 画面の [自動取り込みされる操作ログの格納期間] を短く設定してください。

対象のコンピュータを選択して操作ログを取り込むには：

1. セキュリティ画面を表示します。
2. メニューエリアで [操作ログ] – [操作ログ一覧] を選択します。
3. [操作メニュー] の [保管した操作ログを手動で取り込む] を選択します。

注意事項

操作ログのバックアップファイルが存在しない場合は選択できません。

4. 表示されたダイアログの [手動取り込みの範囲] で、操作ログを取り込む範囲を設定します。
5. [手動取り込み対象のコンピュータ] で、[コンピュータを選択して操作ログを取り込む] を選択し、[変更] ボタンをクリックします。
6. 表示されたダイアログで、取り込み対象のコンピュータを選択し、[対象にする] ボタンをクリックします。
[対象にしている項目だけを表示する] をチェックすると、取り込み対象にしたコンピュータだけが一覧に表示されます。一度取り込み対象にしたコンピュータを対象から外したいときは、対象にしたコンピュータを選択して [対象外にする] ボタンをクリックしてください。
7. [OK] ボタンをクリックします。
[保管した操作ログの手動取り込み] ダイアログに戻ります。
8. [OK] ボタンをクリックします。
9. 操作ログの取り込みが開始され、取り込み状況が表示されます。
10. [閉じる] ボタンをクリックします。

設定した範囲で対象のコンピュータの操作ログが取り込まれます。取り込み済みのデータに設定した範囲の一部が含まれている場合は、それ以外の範囲が取り込まれます。

注意事項

環境に依存しますが、200 台のコンピュータの操作ログを 3 ヶ月分取り込む場合、2 時間以上掛かるおそれがあります。取り込み時間を短縮するには、手動取り込みをする範囲を短く設定してください。

ポイント

以前に取り込んだデータ量が多くて取り込める範囲が不足する場合は、[操作メニュー] の [手動取り込み済みの操作ログを削除する] で不要な期間を削除してから、操作ログを取り込んでください。

ポイント

操作ログは、`ioutils exportoplog` コマンドを実行してエクスポートすることもできます。操作ログの内容を資料に使用したい場合などは、エクスポートすることをお勧めします。

関連リンク

- [10.2 操作ログを確認する手順](#)
- [10.6 操作ログを追跡調査する手順](#)
- [10.4 不審操作のログを確認する手順](#)
- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [17.16 ioutils exportoplog（操作ログのエクスポート）](#)

10.8 操作ログのバックアップファイルを管理する

10.8.1 操作ログの保管先フォルダからバックアップファイルを削除する手順

操作ログの保管先フォルダから不要な操作ログのバックアップファイルを削除して、保管できる領域を確保します。

注意事項

保管先フォルダから操作ログのバックアップファイルを削除するためには、管理用サーバのサービスを停止する必要があります。このため、管理用サーバを使用しない曜日、時間などを考慮して実施してください。

操作ログの保管先フォルダからバックアップファイルを削除するには：

1. 操作ログの保管先フォルダを開きます。

2. 不要なバックアップファイルを削除します。

操作ログのバックアップファイルは日付単位で格納されています。不要な日付のフォルダを削除してください。

操作ログのバックアップファイルが削除され、操作ログを保管する領域が確保できます。

10.8.2 操作ログをバックアップする手順

操作ログはデータ量が膨大になりやすいため、定期的に別のディスクなどに保存して、バックアップすることをお勧めします。管理用サーバのサービスは起動した状態でバックアップできます。

操作ログをバックアップするには：

1. 操作ログの保管先フォルダを開きます。

2. 操作ログのバックアップファイルをバックアップ用のディスクなどにコピーします。

操作ログのバックアップファイルは日付単位で格納されています。

操作ログのバックアップファイルがバックアップ用のディスクに保存されます。

注意事項

拡張子が「.copying」のファイルは、コピー中、またはコピーに失敗したファイルのため、バックアップしないでください。

ポイント

バックアップしたファイルを保管先フォルダに戻すと、操作ログが復元できます。復元後は、管理用サーバの再起動が必要です。

10.8.3 操作ログの保管先フォルダを一時的に変更する手順

障害やメンテナンスなどに対応するため、一時的に操作ログの保管先フォルダを変更できます。

ポイント

操作ログを一時的に保存するディスク（一時ディスク）を用意してください。

操作ログの保管先フォルダを変更するには：

1. Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Manager] - [セットアップ] を選択します。
2. [次へ] ボタンをクリックし、[操作ログの設定] 画面で [操作ログの保管先フォルダ] に一時ディスクを設定します。
3. [次へ] ボタンをクリックし、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。
4. 障害やメンテナンスなどの対応が終了したあと、再度手順 1～手順 3 の操作を実施し、操作ログの保管先フォルダを元の設定に戻します。
5. 一時ディスクに格納された操作ログのバックアップファイルを、元の保管先フォルダに格納します。
6. 管理用サーバのサービスを再起動します。

元の保管先フォルダに操作ログのバックアップファイルが格納されます。

注意事項

拡張子が「.copying」のファイルは、コピー中、またはコピーに失敗したファイルのため、バックアップしないでください。

10.8.4 操作ログの保管先のディスクを変更する手順

操作ログの保管先のディスク容量が足りない場合、操作ログの保管先のディスクを変更してください。

ポイント

新しい操作ログの保管先のディスクを用意してください。

注意事項

保管先フォルダから操作ログのバックアップファイルを削除するためには、管理用サーバのサービスを停止する必要があります。このため、管理用サーバを使用しない曜日、時間などを考慮して実施してください。

操作ログの保管先のディスクを変更するには：

1. 操作ログの保管先のデータを新しい保管先のディスクにコピーします。
2. Windows の [スタート] メニューから [すべてのプログラム] - [JP1_IT Desktop Management 2 - Manager] - [セットアップ] を選択します。
3. [次へ] ボタンをクリックし、[操作ログの設定] 画面で [操作ログの保管先フォルダ] に新しい保管先のディスクを設定します。
4. [次へ] ボタンをクリックし、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。

操作ログが新しい保管先に保存されます。

10.8.5 操作ログのディスクの空き容量のしきい値を変更する手順

操作ログのディスクの空き容量が不足すると、イベント画面にイベントが表示されます。このイベントを通知するタイミングとなる空き容量のしきい値を設定できます。

操作ログのディスクの空き容量のしきい値を変更するには：

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。
JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥conf
2. JP1/IT Desktop Management 2 のサービスを再起動します。

コンフィグレーションファイルに設定した内容で、イベントが通知されます。

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	設定値の計算式
Capacity_OplogDBPathWarningThreshold	操作ログのデータベースフォルダの空き容量の警戒しきい値	1.52 メガバイト×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 ×0.1
Capacity_OplogDBPathErrorThreshold	操作ログのデータベースフォルダの空き容量の緊急しきい値	1.52 メガバイト×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 ×0.03
Capacity_OplogBKPathWarningThreshold	操作ログの保管先フォルダの空き容量の警戒しきい値 (定期エクスポート無効時)	70 キロバイト×管理対象の機器の台数× 7
Capacity_OplogBKPathErrorThreshold	操作ログの保管先フォルダの空き容量の緊急しきい値 (定期エクスポート無効時)	70 キロバイト×管理対象の機器の台数× 3
Capacity_OplogBKPathWarningThreshold_ExportEnabled	操作ログの保管先フォルダの空き容量の警戒しきい値 (定期エクスポート有効時)	730 キロバイト×管理対象の機器の台 数×7
Capacity_OplogBKPathErrorThreshold_ExportEnabled	操作ログの保管先フォルダの空き容量の緊急しきい 値 (定期エクスポート有効時)	730 キロバイト×管理対象の機器の台 数×3
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportDisabled	データフォルダの空き容量の警戒しきい値 (操作ログ 有効時・定期エクスポート無効時)	15.3 メガバイト×管理対象の機器の台数 ×0.5 + 3 ギガバイト
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportDisabled	データフォルダの空き容量の緊急しきい値 (操作ログ 有効時・定期エクスポート無効時)	15.3 メガバイト×管理対象の機器の台数 ×0.3 + 500 メガバイト
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportEnabled	データフォルダの空き容量の警戒しきい値 (操作ログ 有効時・定期エクスポート有効時)	21.4 メガバイト×管理対象の機器の台数 ×0.5 + 3 ギガバイト
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportEnabled	データフォルダの空き容量の緊急しきい値 (操作ログ 有効時・定期エクスポート有効時)	21.4 メガバイト×管理対象の機器の台数 ×0.3 + 500 メガバイト

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
#
# 操作ログのデータベースフォルダの空き容量の警戒しきい値
Capacity_OplogDBPathWarningThreshold=10000
```

11

資産を管理する

ここでは、ハードウェア資産、ソフトウェアライセンス、契約の管理について説明します。

11.1 ハードウェア資産情報を利用する

11.1.1 ハードウェア資産情報を追加する手順

管理対象の機器の棚卸日や資産状態などを管理するために、資産画面の［ハードウェア資産］画面の一覧に、ハードウェア資産情報を追加できます。また、ハードウェア資産に対応する契約情報を関連づけると、［ハードウェア資産の費用］レポートで資産運用に掛かっているコストを確認できるようになります。

ハードウェア資産情報を追加するには：

1. 資産画面を表示します。
2. メニューエリアの［ハードウェア資産］で任意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［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資産情報を入力し、［OK］ボタンをクリックします。

ポイント

複数のハードウェア資産情報を追加したい場合は、［連続して追加］ボタンをクリックしてください。

追加したハードウェア資産情報が、ハードウェア資産の一覧に表示されます。

ポイント

機器を管理対象にすると、ハードウェア資産情報が自動的に登録されます。自動的に登録されたハードウェア資産情報には、機器情報が関連づけられています。ハードウェア資産情報を編集すると、機器情報もあわせて管理できます。機器情報とハードウェア資産情報をあわせて管理する場合は、この方法でハードウェア資産情報を追加することをお勧めします。

注意事項

ハードウェア資産情報に関連づけている機器情報の［ホスト名］を変更しても、ハードウェア資産情報の［機器名称］は自動で変更されません。ハードウェア資産情報の［機器名称］と機器情報の［ホスト名］を統一している場合に、機器情報の［ホスト名］を変更したときは、ハードウェア資産情報の［機器名称］を手動で変更してください。

ポイント

ハードウェア資産情報は、CSV ファイルをインポートして一括で追加することもできます。追加するハードウェア資産情報が多い場合は、CSV ファイルを作成してインポートすることをお勧めします。

ポイント

セキュリティポリシーに USB デバイスの使用を許可するよう設定したい場合は、オンライン管理のコンピュータに USB デバイスを接続して、ハードウェア資産情報を登録してください。

関連リンク

- 11.1.2 ハードウェア資産情報を編集する手順
- 11.1.3 ハードウェア資産情報を削除する手順
- 11.1.6 資産状態を変更する手順
- 11.1.7 予定資産状態を変更する手順
- 11.4.1 ハードウェア資産情報をインポートする手順
- 11.5 資産情報をエクスポートする手順
- 9.7 USB デバイスを登録する手順

11.1.2 ハードウェア資産情報を編集する手順

ハードウェア資産の利用者情報に変更があった場合や、関連するほかのハードウェア資産が変わった場合などに、ハードウェア資産情報を編集できます。

ハードウェア資産情報を編集するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で編集したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで編集したいハードウェア資産情報を選択して、[編集] ボタンをクリックします。
複数のハードウェア資産情報を選択して一括編集することもできます。
4. 表示されるダイアログでハードウェア資産情報を編集し、[OK] ボタンをクリックします。

選択したハードウェア資産情報が更新されます。

注意事項

ハードウェア資産情報が機器情報と関連づけられている場合、[機器情報] を編集しても、収集された機器情報で自動的に上書きされます。

ポイント

ハードウェア資産情報は、CSV ファイルをインポートして一括で編集することもできます。編集するハードウェア資産情報が多い場合は、ハードウェア資産情報を CSV ファイルにエクスポートして編集したあと、インポートすることをお勧めします。

ポイント

[資産状態] と基本的なハードウェア資産情報だけ変更したい場合は、[状態を変更] ボタンをクリックして表示されるダイアログでも編集できます。

ポイント

[予定資産状態] と [変更予定日] だけ変更したい場合は、[操作メニュー] の [予定資産状態を変更する] を選択して表示されるダイアログでも編集できます。

関連リンク

- 11.1.1 ハードウェア資産情報を追加する手順
- 11.1.3 ハードウェア資産情報を削除する手順
- 11.1.6 資産状態を変更する手順
- 11.1.7 予定資産状態を変更する手順
- 11.4.1 ハードウェア資産情報をインポートする手順
- 11.5 資産情報をエクスポートする手順

11.1.3 ハードウェア資産情報を削除する手順

管理する必要がなくなったハードウェア資産情報を削除できます。ハードウェア資産情報は、[資産状態] が [未確認] または [滅却] の場合だけ削除できます。

なお、ハードウェア資産情報を削除すると、契約情報やほかのハードウェア資産情報との関連づけも削除されます。

ハードウェア資産情報を削除するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で削除したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで削除したいハードウェア資産情報を選択して、[操作メニュー] の [ハードウェア資産を削除する] を選択します。
複数のハードウェア資産情報を選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したハードウェア資産情報が削除されます。

関連リンク

- [11.1.1 ハードウェア資産情報を追加する手順](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [11.1.6 資産状態を変更する手順](#)
- [11.1.7 予定資産状態を変更する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.1.4 資産画面で [利用者情報の入力] 画面の表示間隔を設定する手順

ハードウェア資産情報が管理対象のコンピュータの機器情報と関連づいている場合は、オンライン管理のコンピュータに [利用者情報の入力] 画面を表示させる間隔を設定できます。定期的に利用者に情報を入力してもらうことで、管理業務の負担を軽減できます。

なお、[利用者情報の入力] 画面を表示させるには、利用者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必要があります。

[利用者情報の入力] 画面の表示間隔を設定するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で任意のグループを選択します。
3. [操作メニュー] の [[利用者情報の入力] 画面を定期的に表示させる] を選択します。
4. 表示されるダイアログで、表示間隔を設定して [OK] ボタンをクリックします。

[利用者情報の入力] 画面の表示間隔が設定されます。

ポイント

〔利用者情報の入力〕画面の表示項目は、設定画面の〔資産管理〕－〔資産管理項目の設定〕画面で設定できます。

関連リンク

- 15.4.1 資産管理項目を追加する手順

11.1.5 資産状態を追加する手順

〔資産状態〕に任意の項目を追加できます。これによって、運用に合わせた資産状態の管理を実現できます。

資産状態を追加するには：

1. 設定画面の〔資産管理項目の設定〕画面を表示します。
2. 〔ハードウェア資産情報の追加管理項目〕で〔資産状態〕の〔編集〕ボタンをクリックします。
3. 〔管理項目の編集〕ダイアログで〔追加〕ボタンをクリックします。
4. 〔項目の追加〕ダイアログで項目名を入力して〔OK〕ボタンをクリックします。
例えば、「障害対応中」と入力します。
5. 〔管理項目の編集〕ダイアログで〔OK〕ボタンをクリックします。

資産状態の項目が追加されます。なお、追加できる項目は、デフォルトの項目とは別に 100 種類までです。

〔管理項目の編集〕ダイアログでは、既存の項目を編集・削除したり、項目の並び順を変更したりできます。

ポイント

デフォルトの項目（未確認、在庫、運用中、滅却）は、編集および削除できません。また、システム管理者が追加した資産状態のうち、フィルタの条件として保存している資産状態も削除できません。

ポイント

資産状態は、ハードウェア資産情報を設定するときに、〔(新規追加)〕を選択して追加することもできます。

11.1.6 資産状態を変更する手順

〔資産状態〕 および基本的な資産情報（部署や設置場所など）を変更する場合は、〔ハードウェア資産情報の編集〕 ダイアログ以外に、〔資産状態の変更〕 ダイアログでも変更できます。

資産状態を変更するには：

1. 資産画面を表示します。
2. メニューエリアの〔ハードウェア資産〕で〔資産状態〕を変更したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで〔資産状態〕を変更したいハードウェア資産情報を選択して、〔状態を変更〕 ボタンをクリックします。
複数のハードウェア資産情報を選択して一括変更することもできます。
4. 表示されるダイアログで、〔資産状態〕を変更して、〔OK〕 ボタンをクリックします。
〔ノートに追記する〕 をチェックすると、変更前と変更後の資産状態、変更した日、変更した理由などを記録できます。ここで入力した情報は〔ノート〕 タブに追記されます。

選択したハードウェア資産情報の〔資産状態〕が更新されます。

ポイント

ほかの項目を変更したい場合は、〔編集〕 ボタンをクリックして表示されるダイアログで編集できます。

関連リンク

- [11.1.1 ハードウェア資産情報を追加する手順](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [11.1.3 ハードウェア資産情報を削除する手順](#)
- [11.1.7 予定資産状態を変更する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.1.7 予定資産状態を変更する手順

〔予定資産状態〕 および〔変更予定日〕を変更する場合は、〔ハードウェア資産情報の編集〕 ダイアログ以外に、〔予定資産状態の変更〕 ダイアログでも変更できます。

〔予定資産状態〕を設定すると、ダイジェストレポートやメール通知によって変更予定のハードウェア資産を確認できます。例えば、「運用中」から「在庫」に変更予定のハードウェア資産について、変更の通知を受けて回収するなどの使い方ができます。

予定資産状態を変更するには：

1. 資産画面を表示します。
2. メニューエリアの〔ハードウェア資産〕で〔予定資産状態〕を変更したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで〔予定資産状態〕を変更したいハードウェア資産情報を選択して、〔操作メニュー〕の〔予定資産状態を変更する〕を選択します。
複数のハードウェア資産情報を選択して一括変更することもできます。
4. 表示されるダイアログで、〔予定資産状態〕と〔変更予定日〕を変更して、〔OK〕ボタンをクリックします。
〔ノートに追記する〕をチェックすると、変更前と変更後の予定資産状態、変更した日、変更した理由などを記録できます。ここで入力した情報は〔ノート〕タブに追記されます。

選択したハードウェア資産情報の〔予定資産状態〕と〔変更予定日〕が更新されます。

ポイント

ほかの項目を変更したい場合は、〔編集〕ボタンをクリックして表示されるダイアログで編集できます。

関連リンク

- [11.1.1 ハードウェア資産情報を追加する手順](#)
- [11.1.2 ハードウェア資産情報を編集する手順](#)
- [11.1.3 ハードウェア資産情報を削除する手順](#)
- [11.1.6 資産状態を変更する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.1.8 手動で棚卸日を更新する手順

ハードウェア資産情報およびソフトウェアライセンス情報の〔棚卸日〕を手動で更新できます。手もとにある少数の資産を、個別に棚卸する場合にお勧めします。

手動で棚卸日を更新するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] または [ソフトウェアライセンス] で [棚卸日] を更新したい資産情報が含まれるグループを選択します。
3. インフォメーションエリアで [棚卸日] を更新したい資産情報を選択して、[操作メニュー] の [棚卸日を更新する] を選択します。
複数の資産情報を選択して一括更新することもできます。
4. 表示されるダイアログで、棚卸日を入力して、[OK] ボタンをクリックします。
[ノートに追記する] をチェックすると、棚卸日、棚卸の方法、棚卸の理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

選択した資産情報の [棚卸日] が更新されます。

ポイント

[資産管理番号] または [ライセンス管理番号] が記載された CSV ファイルを利用して、[棚卸日] を一括更新することもできます。

ポイント

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2 は機器のネットワーク接続または機器の利用者の入力で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。

ポイント

ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、[棚卸日] を一括更新することもできます。

関連リンク

- [11.1.9 CSV ファイルを基に棚卸日を一括更新する手順](#)
- [11.1.10 棚卸日の自動更新を設定する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.1.9 CSV ファイルを基に棚卸日を一括更新する手順

CSV ファイルを利用して、ハードウェア資産情報およびソフトウェアライセンス情報の [棚卸日] を一括更新できます。

JP1/IT Desktop Management 2 とは別に、バーコードを利用して資産管理番号を管理している場合にお勧めします。バーコードリーダーで読み取った情報を、CSV ファイルで出力してください。CSV ファイルは次の形式になっている必要があります。

ハードウェア資産情報の場合

[棚卸日] を更新するハードウェア資産情報の [資産管理番号] の一覧

ソフトウェアライセンス情報の場合

[棚卸日] を更新するソフトウェアライセンス情報の [ライセンス管理番号] の一覧

CSV ファイルを基に棚卸日を一括更新するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] または [ソフトウェアライセンス] で [棚卸日] を更新したい資産情報が含まれるグループを選択します。
3. [操作メニュー] の [棚卸日を更新する (CSV)] を選択します。
4. 表示されるダイアログで [選択] ボタンをクリックして、事前に作成した CSV ファイルを指定します。
[CSV ファイル(サンプル)のダウンロード] のリンクをクリックすると、CSV ファイルのサンプルをダウンロードできます。
5. 棚卸日を入力して、[OK] ボタンをクリックします。
[ノートに追記する] をチェックすると、棚卸日、棚卸の方法、棚卸の理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

CSV ファイルに記載された [資産管理番号] または [ライセンス管理番号] に該当する資産情報の [棚卸日] が、一括で更新されます。

注意事項

棚卸日の更新でエラーになった場合、JP1/IT Desktop Management 2 で管理されていない資産があります。資産管理番号またはライセンス管理番号を確認して、対象の資産を登録してください。

ポイント

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2 は機器のネットワーク接続または機器の利用者の入力で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。

ポイント

ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、[棚卸日]を一括更新することもできます。この場合は、各資産情報の[棚卸日]に異なった日付を設定できます。

関連リンク

- 11.1.11 バーコードリーダーを使用して棚卸する
- 11.1.8 手動で棚卸日を更新する手順
- 11.1.10 棚卸日の自動更新を設定する手順
- 11.4.1 ハードウェア資産情報をインポートする手順
- 11.4.2 ソフトウェアライセンス情報をインポートする手順
- 11.5 資産情報をエクスポートする手順

11.1.10 棚卸日の自動更新を設定する手順

ハードウェア資産情報の[棚卸日]を自動更新するように設定できます。自動更新を設定すると、次のタイミングで[棚卸日]が自動的に更新されるため、棚卸を実施する手間を省けます。

オンライン管理の場合

機器の最終接続確認日時が更新されたとき、または利用者情報が入力されたとき

オフライン管理の場合

機器情報が管理用サーバに通知されたとき

[棚卸日]の自動更新を設定するには：

1. 資産画面を表示します。
2. メニューエリアの[ハードウェア資産]で任意のグループを選択します。
3. [操作メニュー]の[棚卸日を自動更新する]を選択します。
4. 表示されるダイアログで、次のどちらかのタイミングを選択して[OK]ボタンをクリックします。

なお、オフライン管理の機器の場合は、機器情報が管理用サーバに通知された日時が「棚卸日」となります。

機器の最終接続確認日時を、「棚卸日」とする

ネットワークに接続していることを確認できたら、その機器の存在確認ができたと見なして棚卸日が自動的に更新されるようにします。なお、ネットワークに接続されていない機器は自動更新されません。

利用者による「利用者情報の入力」画面の入力が完了した日を、「棚卸日」とする

利用者のコンピュータに利用者入力画面を表示させて、利用者が情報を入力したことでコンピュータが存在していることとし、そのコンピュータの棚卸日が自動的に更新されるようにします。そのために、利用者入力画面が定期的に表示されるように設定します。「利用者情報の入力」画面の表示タイミングは、「操作メニュー」の「[[利用者情報の入力] 画面を定期的に表示させる」を選択すると設定できます。なお、「利用者情報の入力」画面を表示させるには、利用者のコンピュータにエージェントが導入されている必要があります。エージェントを導入していないコンピュータは、棚卸日が自動更新されません。

選択したタイミングで、「棚卸日」の自動更新が設定されます。

ポイント

「資産管理番号」または「ライセンス管理番号」が記載された CSV ファイルを利用して、「棚卸日」を一括更新することもできます。

ポイント

ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、「棚卸日」を一括更新することもできます。この場合は、各資産情報の「棚卸日」に異なった日付を設定できます。

関連リンク

- [11.1.8 手動で棚卸日を更新する手順](#)
- [11.1.9 CSV ファイルを基に棚卸日を一括更新する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.1.11 バーコードリーダーを使用して棚卸する

バーコードリーダーを使用することで、簡単に棚卸を実施できます。JP1/IT Desktop Management 2 とは別に、CSV ファイルをエクスポートできるバーコードリーダーを利用して資産を管理している場合は、こちらの方法で棚卸を実施することをお勧めします。

1. 機器を現品確認する

バーコードリーダーを利用して、組織内のすべての機器の現品を確認します。

2. 資産情報の一覧をエクスポートする

バーコードリーダーに読み込んだ現品確認の情報を、CSV ファイルにエクスポートします。

CSV ファイルは、1 行ごとに現品確認できた機器の「資産管理番号」だけが記入されるように編集してください。

3. 棚卸日を更新する

CSV ファイルを作成したら、ハードウェア資産情報の CSV ファイルを読み込んで、一括で棚卸日を更新します。棚卸日を更新する手順については、「[11.1.9 CSV ファイルを基に棚卸日を一括更新する手順](#)」を参照してください。

CSV ファイルに記入されていたハードウェア資産情報の「棚卸日」が更新されます。

注意事項

棚卸日の更新でエラーになった場合は、JP1/IT Desktop Management 2 で管理されていない資産があります。資産管理番号を確認して、対象の資産を登録してください。

4. 棚卸できなかった機器を確認する

資産画面の「ハードウェア資産」画面で、「棚卸日」が更新されていないハードウェア資産情報を表示します。現品を調査するために、「資産管理番号」、「部署」、「設置場所」、「利用者名」などの項目をエクスポートしてください。エクスポートの手順については、「[11.5 資産情報をエクスポートする手順](#)」を参照してください。

5. 該当機器の利用者に状況を確認する

ハードウェア資産情報の一覧を作成したら、現品がどこにあるか機器の利用者に確認します。

機器が見つかった場合

一覧に、機器を現品確認できたことと、修正があればその内容を記入します。

機器が見つからなかった場合

機器が紛失したおそれがあります。利用者に機器の紛失届けを提出するように指示し、必要に応じて資産画面の「ハードウェア資産」画面で該当資産の「資産状態」を「滅却」にします。また、紛失理由や紛失日時などを「ノート」タブにメモしておきます。

6. 棚卸結果を反映する

現品確認できた機器について、現品確認の結果を反映します。

現品確認時に見つからなかった機器のうち、発見できたものについて「棚卸日」が更新されます。

関連リンク

- [11.1.8 手動で棚卸日を更新する手順](#)
- [11.1.10 棚卸日の自動更新を設定する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)

11.1.12 ハードウェア資産に対する契約情報を関連づける手順

ハードウェア資産に対する契約情報を関連づけられます。契約情報を関連づけると、ハードウェア資産の契約費用の推移や契約種別などを管理できるようになります。

契約情報の作成方法については、「[11.3.1 契約情報を追加する手順](#)」を参照してください。

ハードウェア資産に対する契約情報を関連づけるには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」で契約情報を設定したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで契約情報を設定したいハードウェア資産情報を選択して、[操作メニュー]の「契約情報を追加する」を選択します。
4. 表示されるダイアログで契約情報を選択して、[OK] ボタンをクリックします。

ハードウェア資産に対する契約情報が関連づけられます。

ポイント

ハードウェア資産情報の「契約情報」タブで、契約情報を関連づけることもできます。

ポイント

ハードウェア資産情報を追加または編集するダイアログの「関連情報」で、契約情報を関連づけることもできます。

関連リンク

- [11.3.6 契約対象のハードウェア資産を関連づける手順](#)

11.1.13 複数のハードウェア資産情報を関連づける手順

コンピュータ、ディスプレイ、CD/DVD ドライブなどの複数のハードウェア資産情報をまとめて管理するために、ハードウェア資産情報同士を関連づけられます。

複数のハードウェア資産情報を関連づけるには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で関連づけたいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで関連づけたいハードウェア資産情報を選択して、[操作メニュー] の [ほかのハードウェア資産と関連づける] を選択します。
4. 表示されるダイアログでハードウェア資産情報を選択して、[OK] ボタンをクリックします。

複数のハードウェア資産情報が関連づけられます。

注意事項

複数の資産をまとめて管理する場合、コンピュータの [資産状態] を変更しても、関連するディスプレイ、CD/DVD ドライブなどの [資産状態] は変更されません。例えば、[棚卸日] を更新する場合は、関連するすべてのハードウェア資産情報について [棚卸日] を更新する必要があります。

ポイント

ハードウェア資産情報の [関連資産] タブで、複数の資産情報を関連づけることもできます。

ポイント

ハードウェア資産情報を追加または編集するダイアログの [関連情報] で、複数の資産情報を関連づけることもできます。

11.1.14 ハードウェア資産情報に対応する機器情報を変更する手順

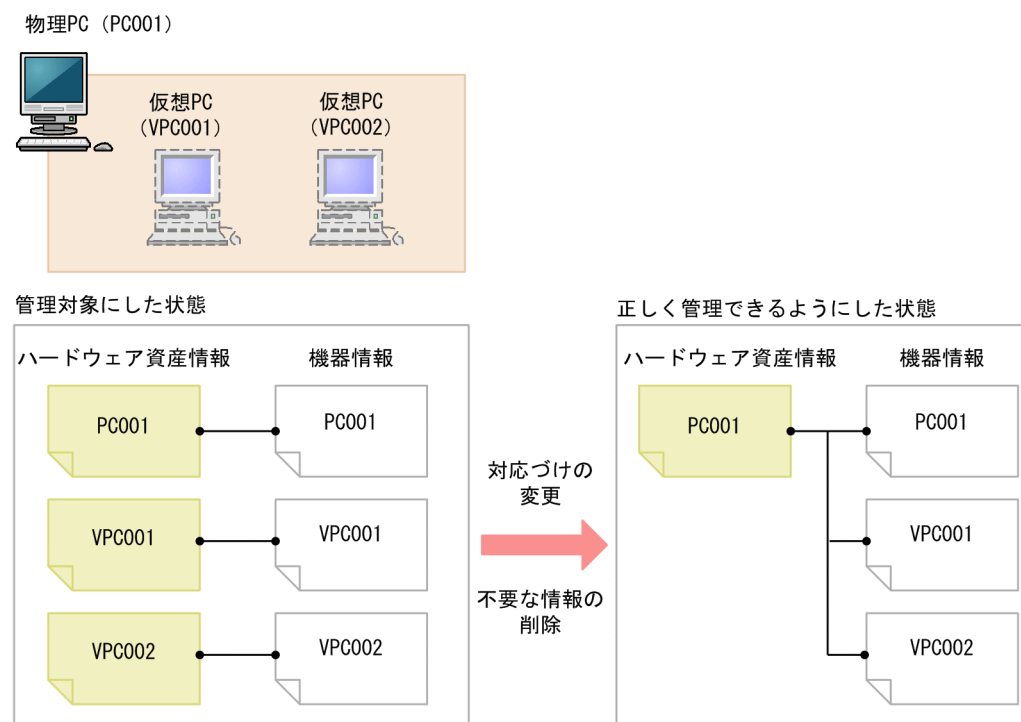
ハードウェア資産情報に対応する機器情報を手動で変更できます。

ハードウェア資産情報にほかの機器情報を対応づけたり、1 つのハードウェア資産情報に複数の機器情報を対応づけたりできます。

例えば、1 台の物理コンピュータ内に 2 つの仮想コンピュータが構築されている環境があった場合、それぞれを管理対象にすると 3 台分のハードウェア資産情報が登録されます。しかし、物理的に存在するコン

ピュータは1台なので、ハードウェア資産情報を正しく管理するためには、仮想コンピュータの機器情報が物理コンピュータのハードウェア資産情報に対応づくように変更して、さらに不要なハードウェア資産情報（仮想コンピュータの情報）を削除する必要があります。

ハードウェア資産情報を正しく管理するために、機器情報の対応づけを変更する例を次の図に示します。



ハードウェア資産情報に対応する機器情報を変更するには：

1. 資産画面を表示します。
2. メニューエリアの［ハードウェア資産］で、対応づけを変更したいハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで対応づけを変更したいハードウェア資産情報を選択して、［機器情報］タブを表示します。
4. タブ中で、対応づけを変更したい機器情報を選択します。
5. タブ中の［機器に関連するハードウェア資産を変更］ボタンをクリックします。
6. 表示されるダイアログで機器情報と対応づけたいハードウェア資産情報を選択して、［OK］ボタンをクリックします。

ハードウェア資産情報に対応する機器情報が変更されます。

関連リンク

- [11.1.15 ハードウェア資産情報に関連づいた機器情報の代表を設定する手順](#)

11.1.15 ハードウェア資産情報に関連づいた機器情報の代表を設定する手順

ハードウェア資産情報に複数の機器情報が関連づいている場合、その中で代表となる機器情報を設定できます。代表の機器を設定すると、その機器の機器情報がハードウェア資産情報に反映されるようになります。

機器情報の代表を設定するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、複数の機器情報が関連づけられたハードウェア資産情報が含まれるグループを選択します。
3. インフォメーションエリアで複数の機器情報が関連づけられたハードウェア資産情報を選択して、【機器情報】タブを表示します。
4. タブ中で、代表に設定したい機器情報を選択します。
複数の機器情報は選択できません。
5. タブ中の【代表の機器を変更】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。

ハードウェア資産情報に関連づいた機器情報の代表が設定されます。代表となった機器情報には、【代表の機器】の項目に  が表示されます。

関連リンク

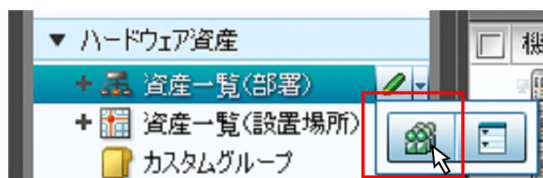
- [11.1.14 ハードウェア資産情報に対応する機器情報を変更する手順](#)

11.1.16 部署・設置場所の定義を追加する手順

管理する部署や設置場所が増えた場合、部署・設置場所の定義を追加できます。定義を追加すると、追加した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を追加するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の「資産管理」－「資産管理項目の設定」を選択して表示される画面で、「資産情報と機器情報の共通管理項目」の「部署」または「設置場所」の「編集」ボタンをクリックしても追加できます。

3. 表示されるダイアログで「データ型」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部署・設置場所を追加します。

5. [OK] ボタンをクリックします。

6. [OK] ボタンをクリックします。

部署・設置場所の定義が追加されて、資産画面や機器画面などのメニューエリアに追加したグループが表示されます。

関連リンク

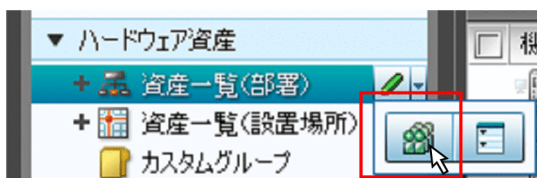
- [6.29 部署・設置場所の定義を編集する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)

11.1.17 部署・設置場所の定義を編集する手順

管理する部署が統合されたり設置場所の名称が変更になったりした場合、部署・設置場所の定義を編集できます。定義を編集すると、編集した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を編集するには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」で、「資産一覧（部署）」または「資産一覧（設置場所）」を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の「資産管理」－「資産管理項目の設定」を選択して表示される画面で、「資産情報と機器情報の共通管理項目」の「部署」または「設置場所」の「編集」ボタンをクリックしても編集できます。

3. 表示されるダイアログで「データ型」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部署・設置場所の名称や階層を編集します。

5. [OK] ボタンをクリックします。

6. [OK] ボタンをクリックします。

部署・設置場所の定義が編集されて、資産画面や機器画面などのメニューエリアに編集したグループが表示されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除します。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が変更されると、資産画面の「ソフトウェアライセンス」－「ソフトウェアライセンス一覧」、[ソフトウェアライセンス状況]－「ソフトウェアライセンス状況一覧」および資産画面の「契約」－「契約一覧」に表示される部署の情報も変更されます。

関連リンク

- ・ [6.28 部署・設置場所の定義を追加する手順](#)
- ・ [6.30 部署・設置場所の定義を削除する手順](#)

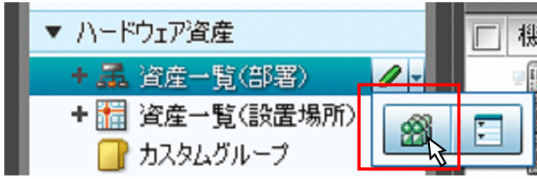
11.1.18 部署・設置場所の定義を削除する手順

管理していた部署や設置場所を管理しなくなった場合、部署・設置場所の定義を削除できます。定義を削除すると、削除した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を削除するには：

1. 資産画面を表示します。

2. メニューエリアの「ハードウェア資産」で、「資産一覧（部署）」または「資産一覧（設置場所）」を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで「データ型」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部署・設置場所の定義を削除します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が削除されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除します。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が削除されると、資産画面の次の画面に表示されていた該当する部署の情報は、「不明」と表示されます。

- [ソフトウェアライセンス] — [ソフトウェアライセンス一覧] 画面
- [ソフトウェアライセンス状況] — [ソフトウェアライセンス状況一覧] 画面
- [契約] — [契約一覧] 画面

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)

11.1.19 旧体制で使われていた階層だけを削除する手順

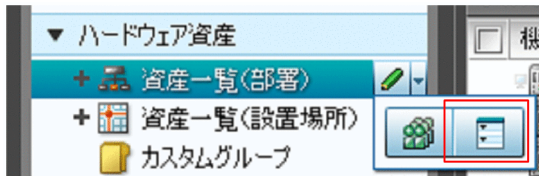
職制変更に伴い設定画面で部署・設置場所の階層（定義）を削除しても、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。メニューエリアの表示を定義に合わせる

ためには、旧体制で使われていた階層だけを削除する必要があります。メニューエリアの階層は、資産画面、機器画面およびセキュリティ画面のメニューエリアから表示できるダイアログで削除できます。

資産画面で削除する場合を例に、手順を次に示します。

旧体制で使われていた階層だけを削除するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで、削除したい階層を選択します。
4. [削除] ボタンをクリックします。
5. 表示されるダイアログで、[OK] ボタンをクリックします。
6. [閉じる] ボタンをクリックします。

旧体制で使われていた階層だけが削除されて、資産画面や機器画面のメニューエリアの表示が定義と一致します。

11.1.20 部署・設置場所の名称を変更する手順

管理する部署が統合されたり設置場所の名称が変更になったりした場合、部署・設置場所の名称を変更できます。

部署・設置場所の名称を変更するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】で名称を変更したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるテキストエリアに部署または設置場所の名称を入力します。

部署・設置場所のグループの名称が変更されます。また、機器の利用者情報も変更後のグループ名に変更されます。

ポイント

メニューエリアの部署または設置場所を右クリックして表示されるメニューから変更することもできます。

関連リンク

- 6.28 部署・設置場所の定義を追加する手順
- 6.29 部署・設置場所の定義を編集する手順
- 6.30 部署・設置場所の定義を削除する手順
- 6.33 部署・設置場所を削除する手順

11.1.21 部署・設置場所を削除する手順

不要になった部署・設置場所を削除できます。

部署・設置場所を削除するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] で、[資産一覧（部署）] または [資産一覧（設置場所）] で削除したいグループにマウスカーソルを合わせます。
3. 項目の右側に表示される  をクリックします。
4. 表示されるメニューで  をクリックします。
5. 表示されるダイアログで [OK] ボタンをクリックします。

部署・設置場所のグループが削除されます。また、機器の利用者情報の部署・設置場所も削除されます。

ポイント

メニューエリアの部署・設置場所を右クリックして表示されるメニューから削除することもできます。

関連リンク

- 6.28 部署・設置場所の定義を追加する手順

- 6.29 部署・設置場所の定義を編集する手順
- 6.30 部署・設置場所の定義を削除する手順
- 6.32 部署・設置場所の名称を変更する手順

11.2 ソフトウェアライセンス情報を利用する

11.2.1 管理ソフトウェア情報を追加する手順

資産画面の「管理ソフトウェア」－「管理ソフトウェア一覧」画面の一覧に、管理ソフトウェア情報を追加できます。管理ソフトウェア情報を追加すると、ソフトウェアのライセンス消費数を確認できます。

また、機器画面の「ソフトウェア情報」－「ソフトウェア一覧」画面や資産画面の「ソフトウェアライセンス」－「ソフトウェアライセンス一覧」画面からも、対応する管理ソフトウェア情報を確認できます。

管理ソフトウェア情報を追加するには：

1. 資産画面を表示します。
2. メニューエリアで「管理ソフトウェア」－「管理ソフトウェア一覧」を選択します。
3. インフォメーションエリアで「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情報を入力して、「OK」ボタンをクリックします。

管理ソフトウェア情報が追加され、一覧に表示されます。

ポイント

管理ソフトウェア情報は、CSV ファイルをインポートして一括で追加することもできます。追加する管理ソフトウェア情報が多い場合は、CSV ファイルを作成してインポートすることをお勧めします。

管理ソフトウェア情報に対応するソフトウェアを指定することで、収集されたソフトウェア情報を基にライセンス消費数がカウントされ、ライセンス消費の実態が確認できます。対応するソフトウェアは複数指定できます。例えば、バージョンの異なる同じソフトウェアを指定することで、バージョンに関係なくそのソフトウェアのライセンス消費数の累計を把握できます。

なお、ソフトウェアライセンスをコンピュータに割り当てて、対応するソフトウェアライセンス情報を追加すると、ソフトウェアライセンスの過不足と、許可なくソフトウェアを利用しているコンピュータを確認できるようになります。また、「サマリ」－「ダッシュボード」画面の「超過したソフトウェアライセンス」パネルにも、情報が表示されるようになります。

関連リンク

- [11.2.2 管理ソフトウェア情報を編集する手順](#)
- [11.2.3 管理ソフトウェア情報を削除する手順](#)
- [11.4.3 管理ソフトウェア情報をインポートする手順](#)

- [11.5 資産情報をエクスポートする手順](#)

11.2.2 管理ソフトウェア情報を編集する手順

管理ソフトウェアとして設定するインストールソフトウェアに変更があった場合や、対応するソフトウェアライセンスが増えた場合など、管理ソフトウェアの情報を編集して更新できます。

管理ソフトウェアを編集するには：

1. 資産画面を表示します。
2. メニューエリアで [管理ソフトウェア] – [管理ソフトウェア一覧] 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管理ソフトウェア情報を選択して、[編集] ボタンをクリックします。
複数の管理ソフトウェア情報を選択して一括編集することもできます。
4. 表示されるダイアログで管理ソフトウェア情報を編集して、[OK] ボタンをクリックします。

選択した管理ソフトウェア情報が更新されます。

ポイント

管理ソフトウェア情報は、CSV ファイルをインポートして編集することもできます。編集する管理ソフトウェア情報が多い場合は、管理ソフトウェア情報を CSV ファイルにエクスポートして編集したあと、インポートすることをお勧めします。

関連リンク

- [11.2.1 管理ソフトウェア情報を追加する手順](#)
- [11.2.3 管理ソフトウェア情報を削除する手順](#)
- [11.4.3 管理ソフトウェア情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.3 管理ソフトウェア情報を削除する手順

管理する必要がなくなった管理ソフトウェア情報を削除できます。

なお、管理ソフトウェア情報を削除すると、ソフトウェアライセンス情報との関連づけも削除されます。

管理ソフトウェアを削除するには：

1. 資産画面を表示します。

2. メニューエリアで「管理ソフトウェア」－「管理ソフトウェア一覧」を選択します。
3. インフォメーションエリアで削除したい管理ソフトウェア情報を選択して、「操作メニュー」の「管理ソフトウェアを削除する」を選択します。
複数の管理ソフトウェア情報を選択して一括削除することもできます。
4. 表示されるダイアログで「OK」ボタンをクリックします。

選択した管理ソフトウェア情報が削除されます。

関連リンク

- [11.2.1 管理ソフトウェア情報を追加する手順](#)
- [11.2.2 管理ソフトウェア情報を編集する手順](#)
- [11.4.3 管理ソフトウェア情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.4 ソフトウェアライセンス情報を追加する手順

資産画面の「ソフトウェアライセンス」画面の一覧に、ソフトウェアライセンス情報を追加できます。また、ソフトウェアライセンス情報に対応する契約情報を関連づけると、レポート画面の「ソフトウェアライセンスの費用」レポートで資産運用に掛かっているコストを確認できるようになります。

ソフトウェアライセンス情報を追加するには：

1. 資産画面を表示します。
2. メニューエリアで「ソフトウェアライセンス」－「ソフトウェアライセンス一覧」を選択します。
3. インフォメーションエリアで「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ソフトウェアライセンス情報を入力して、「OK」ボタンをクリックします。

ポイント

複数のソフトウェアライセンス情報を追加したい場合は、「連続して追加」ボタンをクリックしてください。

追加したソフトウェアライセンス情報が、ソフトウェアライセンスの一覧に表示されます。

ポイント

ソフトウェアライセンス情報は、CSV ファイルをインポートして追加することもできます。追加するソフトウェアライセンス情報が多い場合は、CSV ファイルを作成してインポートすることをお勧めします。

なお、ソフトウェアライセンスをコンピュータに割り当てて、対応する管理ソフトウェア情報を追加すると、ソフトウェアライセンスの過不足と、許可なくソフトウェアを利用しているコンピュータを確認できるようになります。また、資産画面の [サマリ] - [ダッシュボード] 画面の [超過したソフトウェアライセンス] パネルにも、情報が表示されるようになります。

関連リンク

- [11.2.5 ソフトウェアライセンス情報を編集する手順](#)
- [11.2.6 ソフトウェアライセンス情報を削除する手順](#)
- [11.2.8 ライセンス状態を変更する手順](#)
- [11.2.9 予定ライセンス状態を変更する手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.5 ソフトウェアライセンス情報を編集する手順

ソフトウェアのライセンス数、ライセンス状態が変わった場合や、ソフトウェアライセンスを割り当てるコンピュータを変更する場合などに、ソフトウェアライセンス情報を編集できます。

ソフトウェアライセンス情報を編集するには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] - [ソフトウェアライセンス一覧] 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ソフトウェアライセンス情報を選択して、[編集] ボタンをクリックします。
複数のソフトウェアライセンス情報を選択して一括編集することもできます。
4. 表示されるダイアログでソフトウェアライセンス情報を編集し、[OK] ボタンをクリックします。

選択したソフトウェアライセンス情報が更新されます。

なお、保有しているソフトウェアライセンスの一部を他部署に配分したい場合は、次のように変更前の部署と変更後の部署のソフトウェアライセンス情報を両方編集してください。

1. 変更前の部署のソフトウェアライセンス情報の保有数から、移動するライセンス数を減算する

2. 変更後の部署のソフトウェアライセンス情報の保有数に、手順 1 で減算した数を加算する

変更後の部署のソフトウェアライセンス情報がない場合は、ソフトウェアライセンス情報を新たに追加してください。

ポイント

ソフトウェアライセンス情報は、CSV ファイルをインポートして編集することもできます。編集するソフトウェアライセンス情報が多い場合は、ソフトウェアライセンス情報を CSV ファイルにエクスポートして編集したあと、インポートすることをお勧めします。

ポイント

［ライセンス状態］だけ変更したい場合は、［状態を変更］ボタンをクリックして表示されるダイアログでも編集できます。

ポイント

［予定ライセンス状態］と［変更予定日］だけ変更したい場合は、［操作メニュー］の［予定ライセンス状態を変更する］を選択して表示されるダイアログでも編集できます。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.2.6 ソフトウェアライセンス情報を削除する手順](#)
- [11.2.8 ライセンス状態を変更する手順](#)
- [11.2.9 予定ライセンス状態を変更する手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.6 ソフトウェアライセンス情報を削除する手順

管理する必要がなくなったソフトウェアライセンス情報を削除できます。ソフトウェアライセンス情報は、ライセンス状態が［滅却］の場合だけ削除できます。削除する前に、ライセンス状態を［滅却］に変更してください。

なお、ソフトウェアライセンス情報を削除すると、管理ソフトウェア情報や契約情報との関連づけも削除されます。

ソフトウェアライセンス情報を削除するには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] – [ソフトウェアライセンス一覧] を選択します。
3. インフォメーションエリアで削除したいソフトウェアライセンス情報を選択して、[操作メニュー] の [ソフトウェアライセンスを削除する] を選択します。
複数のソフトウェアライセンス情報を選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したソフトウェアライセンス情報が削除されます。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.2.5 ソフトウェアライセンス情報を編集する手順](#)
- [11.2.8 ライセンス状態を変更する手順](#)
- [11.2.9 予定ライセンス状態を変更する手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.7 ライセンス状態を追加する手順

[ライセンス状態] に任意の項目を追加できます。これによって、運用に合わせたライセンス状態の管理を実現できます。

ライセンス状態を追加するには：

1. 設定画面の [資産管理項目の設定] 画面を表示します。
2. [ソフトウェアライセンス情報の追加管理項目] で [ライセンス状態] の [編集] ボタンをクリックします。
3. [管理項目の編集] ダイアログで [追加] ボタンをクリックします。
4. [項目の追加] ダイアログで項目名を入力して [OK] ボタンをクリックします。
5. [管理項目の編集] ダイアログで [OK] ボタンをクリックします。

ライセンス状態の項目が追加されます。なお、追加できる項目は、デフォルトの項目とは別に 100 種類までです。

[管理項目の編集] ダイアログでは、既存の項目を編集・削除したり、項目の並び順を変更したりできます。

ポイント

デフォルトの項目（使用中、滅却）は、編集および削除できません。

ポイント

ライセンス状態は、ソフトウェアライセンス情報を設定するときに、[(新規追加)] を選択して追加することもできます。

11.2.8 ライセンス状態を変更する手順

ライセンス状態は、[ソフトウェアライセンス情報の編集] ダイアログ以外に、[ライセンス状態の変更] ダイアログでも変更できます。

ライセンス状態を変更するには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] - [ソフトウェアライセンス一覧] を選択します。
3. インフォメーションエリアで [ライセンス状態] を変更したいソフトウェアライセンス情報を選択して、[状態を変更] ボタンをクリックします。
複数のソフトウェアライセンス情報を選択して一括変更することもできます。
4. 表示されるダイアログで、[ライセンス状態] を変更して、[OK] ボタンをクリックします。
[ノートに追記する] をチェックすると、変更前と変更後のライセンス状態、変更した日、変更した理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

選択したソフトウェアライセンス情報の [ライセンス状態] が更新されます。

ポイント

ほかの項目を変更したい場合は、[編集] ボタンをクリックして表示されるダイアログで編集できます。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.2.5 ソフトウェアライセンス情報を編集する手順](#)
- [11.2.6 ソフトウェアライセンス情報を削除する手順](#)
- [11.2.9 予定ライセンス状態を変更する手順](#)

- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)

11.2.9 予定ライセンス状態を変更する手順

予定ライセンス状態は、[ソフトウェアライセンス情報の編集] ダイアログ以外に、[予定ライセンス状態の変更] ダイアログでも変更できます。

例えば、滅却する予定のソフトウェアライセンスがある場合に [予定ライセンス状態] を変更して、変更予定日になったらソフトウェアライセンスを滅却するなどの使い方ができます。

予定ライセンス状態を変更するには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] – [ソフトウェアライセンス一覧] を選択します。
3. インフォメーションエリアで [予定ライセンス状態] を変更したいソフトウェアライセンス情報を選択して、[操作メニュー] の [予定ライセンス状態を変更する] を選択します。
複数のソフトウェアライセンス情報を選択して一括変更することもできます。
4. 表示されるダイアログで、[予定ライセンス状態] と [変更予定日] を変更して、[OK] ボタンをクリックします。
[ノートに追記する] をチェックすると、変更前と変更後のライセンス状態、変更した日、変更した理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

選択したソフトウェアライセンス情報の [予定ライセンス状態] と [変更予定日] が更新されます。

ポイント

ほかの項目を変更したい場合は、[編集] ボタンをクリックして表示されるダイアログで編集できます。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.2.5 ソフトウェアライセンス情報を編集する手順](#)
- [11.2.6 ソフトウェアライセンス情報を削除する手順](#)
- [11.2.8 ライセンス状態を変更する手順](#)
- [11.4.2 ソフトウェアライセンス情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.2.10 手動で棚卸日を更新する手順

ハードウェア資産情報およびソフトウェアライセンス情報の「棚卸日」を手動で更新できます。手もとにある少数の資産を、個別に棚卸する場合にお勧めします。

手動で棚卸日を更新するには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」または「ソフトウェアライセンス」で「棚卸日」を更新したい資産情報が含まれるグループを選択します。
3. インフォメーションエリアで「棚卸日」を更新したい資産情報を選択して、「操作メニュー」の「棚卸日を更新する」を選択します。
複数の資産情報を選択して一括更新することもできます。
4. 表示されるダイアログで、棚卸日を入力して、「OK」ボタンをクリックします。
「ノートに追記する」をチェックすると、棚卸日、棚卸の方法、棚卸の理由などを記録できます。ここで入力した情報は「ノート」タブに追記されます。

選択した資産情報の「棚卸日」が更新されます。

ポイント

「資産管理番号」または「ライセンス管理番号」が記載された CSV ファイルを利用して、「棚卸日」を一括更新することもできます。

ポイント

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2 は機器のネットワーク接続または機器の利用者の入力で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。

ポイント

ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、「棚卸日」を一括更新することもできます。

関連リンク

- [11.1.9 CSV ファイルを基に棚卸日を一括更新する手順](#)
- [11.1.10 棚卸日の自動更新を設定する手順](#)
- [11.4.1 ハードウェア資産情報をインポートする手順](#)

- 11.4.2 ソフトウェアライセンス情報をインポートする手順
- 11.5 資産情報をエクスポートする手順

11.2.11 CSV ファイルを基に棚卸日を一括更新する手順

CSV ファイルを利用して、ハードウェア資産情報およびソフトウェアライセンス情報の [棚卸日] を一括更新できます。

JP1/IT Desktop Management 2 とは別に、バーコードを利用して資産管理番号を管理している場合にお勧めします。バーコードリーダーで読み取った情報を、CSV ファイルで出力してください。CSV ファイルは次の形式になっている必要があります。

ハードウェア資産情報の場合

[棚卸日] を更新するハードウェア資産情報の [資産管理番号] の一覧

ソフトウェアライセンス情報の場合

[棚卸日] を更新するソフトウェアライセンス情報の [ライセンス管理番号] の一覧

CSV ファイルを基に棚卸日を一括更新するには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産] または [ソフトウェアライセンス] で [棚卸日] を更新したい資産情報が含まれるグループを選択します。
3. [操作メニュー] の [棚卸日を更新する (CSV)] を選択します。
4. 表示されるダイアログで [選択] ボタンをクリックして、事前に作成した CSV ファイルを指定します。
[CSV ファイル(サンプル)のダウンロード] のリンクをクリックすると、CSV ファイルのサンプルをダウンロードできます。
5. 棚卸日を入力して、[OK] ボタンをクリックします。
[ノートに追記する] をチェックすると、棚卸日、棚卸の方法、棚卸の理由などを記録できます。ここで入力した情報は [ノート] タブに追記されます。

CSV ファイルに記載された [資産管理番号] または [ライセンス管理番号] に該当する資産情報の [棚卸日] が、一括で更新されます。

注意事項

棚卸日の更新でエラーになった場合、JP1/IT Desktop Management 2 で管理されていない資産があります。資産管理番号またはライセンス管理番号を確認して、対象の資産を登録してください。

ポイント

ハードウェア資産情報の場合、棚卸日を自動更新するように設定できます。JP1/IT Desktop Management 2は機器のネットワーク接続または機器の利用者の入力で機器の存在を確認します。機器の存在を確認できたら、棚卸日が自動更新されます。

ポイント

ハードウェア資産情報およびソフトウェアライセンス情報をインポートして、[棚卸日]を一括更新することもできます。この場合は、各資産情報の[棚卸日]に異なった日付を設定できます。

関連リンク

- 11.1.11 バーコードリーダーを使用して棚卸する
- 11.1.8 手動で棚卸日を更新する手順
- 11.1.10 棚卸日の自動更新を設定する手順
- 11.4.1 ハードウェア資産情報をインポートする手順
- 11.4.2 ソフトウェアライセンス情報をインポートする手順
- 11.5 資産情報をエクスポートする手順

11.2.12 ソフトウェアライセンスをコンピュータに割り当てる手順

ソフトウェアの利用を許可するコンピュータに、ソフトウェアライセンスを割り当てられます。

管理ソフトウェア情報を登録している場合は、ソフトウェアライセンスの過不足と、許可なくソフトウェアを利用しているコンピュータを確認できるようになります。また、[サマリ] – [ダッシュボード] 画面に表示される[超過したソフトウェアライセンス]パネルにも、情報が表示されるようになります。

ソフトウェアライセンスをコンピュータに割り当てるには：

1. 資産画面を表示します。
2. メニューエリアで[ソフトウェアライセンス] – [ソフトウェアライセンス一覧]を選択します。
3. インフォメーションエリアで該当するソフトウェアライセンス情報を選択して、[操作メニュー]の[コンピュータを割り当てる]を選択します。
複数のソフトウェアライセンス情報を選択して一括で割り当てることもできます。
4. 表示されるダイアログで、ソフトウェアライセンスを割り当てるコンピュータを選択して、[OK] ボタンをクリックします。

選択したコンピュータにソフトウェアライセンスが割り当てられます。

ソフトウェアライセンスを割り当てたコンピュータの情報は、[管理ソフトウェア] 画面の [割り当て済みコンピュータ] タブで確認できます。[未インストールのコンピュータだけを表示する] をチェックすると、ソフトウェアライセンスが割り当てられているのに、ソフトウェアをインストールしていないコンピュータが表示されます。

ソフトウェアをインストールしているコンピュータの情報は、[管理ソフトウェア] 画面の [インストール済みコンピュータ] タブで確認できます。[未割り当てコンピュータだけを表示する] をチェックすると、ソフトウェアライセンスが割り当てられていないのに、ソフトウェアをインストールしているコンピュータが表示されます。

■ ポイント

[ソフトウェアライセンス] 画面の [割り当てコンピュータ] タブで、ソフトウェアライセンスを割り当てるコンピュータを追加することもできます。

■ ポイント

ソフトウェアライセンス情報を追加・編集するダイアログの [ライセンス割り当てコンピュータ] で、ソフトウェアライセンスを割り当てるコンピュータを追加することもできます。

関連リンク

- [11.2.4 ソフトウェアライセンス情報を追加する手順](#)
- [11.2.1 管理ソフトウェア情報を追加する手順](#)

11.2.13 ソフトウェアライセンスを移管する手順

機器に割り当てているソフトウェアライセンスを、そのまま別の機器に移管できます。ソフトウェアライセンスを移管できる機器は、機器種別が PC、サーバ、プリンタ、ネットワーク装置、および不明な機器です。

機器のリプレースが発生した場合、リプレース前の機器に割り当てていたソフトウェアライセンスをリプレース後の機器に移管できます。機器に割り当てていたすべてのソフトウェアライセンスを一括で移管できるので便利です。

注意事項

移管先の機器にソフトウェアライセンスが割り当てられている場合は、ソフトウェアライセンスを移管できません。この場合、あらかじめ移管先の機器で、ソフトウェアライセンスの割り当てを解除してください。

ソフトウェアライセンスを移管するには：

1. 機器画面を表示します。
2. [機器情報] 画面で移管元の機器を選択します。
3. [操作メニュー] の [ソフトウェアライセンスを移管する] を選択します。
4. 表示されるダイアログで移管先の機器を選択して、[OK] ボタンをクリックします。

選択した機器にソフトウェアライセンスが移管されます。移管元の機器からは、ソフトウェアライセンスの割り当てが解除されます。

11.2.14 ソフトウェアライセンスに対する契約情報を関連づける手順

ソフトウェアライセンスの契約費用の推移や契約種別などを管理するために、ソフトウェアライセンスに対する契約情報を関連づけられます。

契約情報の作成方法については、「[11.3.1 契約情報を追加する手順](#)」を参照してください。

ソフトウェアライセンスに対する契約情報を関連づけるには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] - [ソフトウェアライセンス一覧] を選択します。
3. インフォメーションエリアで契約情報を設定したいソフトウェアライセンス情報を選択して、[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、[契約情報] の [変更] ボタンをクリックします。
5. 表示されるダイアログで契約情報を選択して、[OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

ソフトウェアライセンスに対する契約情報が関連づけられます。

関連リンク

- [11.3.7 契約対象のソフトウェアライセンスを関連づける手順](#)

11.3 契約情報を利用する

11.3.1 契約情報を追加する手順

資産画面の [契約] - [契約一覧] 画面の一覧に、契約情報を追加できます。契約情報を追加すると、[サマリ] - [ダッシュボード] 画面の [3 か月以内に期限が切れる契約] パネルで契約期限の近い契約情報を把握できるようになります。

また、契約対象のハードウェア資産やソフトウェアライセンスを関連づけると、レポート画面の [ハードウェア資産の費用] レポートや [ソフトウェアライセンスの費用] レポートで資産運用に掛かっているコストを確認できるようになります。

契約情報を追加するには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. インフォメーションエリアで [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契約情報を入力して、[OK] ボタンをクリックします。

契約情報が追加され、契約の一覧に表示されます。

ポイント

契約情報は、CSV ファイルをインポートして一括で追加することもできます。追加する契約情報が多い場合は、CSV ファイルを作成してインポートすることをお勧めします。

関連リンク

- [11.3.2 契約情報を編集する手順](#)
- [11.3.3 契約情報を削除する手順](#)
- [11.3.5 契約状態を変更する手順](#)
- [11.4.4 契約情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.3.2 契約情報を編集する手順

契約情報を編集できます。契約期間や契約状態が変わった場合や、契約対象の資産を変更する場合などに編集します。

契約情報を編集するには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] 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契約情報を選択して、[編集] ボタンをクリックします。
複数の契約情報を選択して一括編集することもできます。
4. 表示されるダイアログで契約情報を編集して、[OK] ボタンをクリックします。

選択した契約情報が更新されます。

ポイント

契約情報は、CSV ファイルをインポートして編集することもできます。編集する契約情報が多い場合は、契約情報を CSV ファイルにエクスポートして編集したあと、インポートすることをお勧めします。

ポイント

[契約状態] だけ変更したい場合は、[状態を変更] ボタンをクリックして表示されるダイアログでも編集できます。

関連リンク

- [11.3.1 契約情報を追加する手順](#)
- [11.3.3 契約情報を削除する手順](#)
- [11.3.5 契約状態を変更する手順](#)
- [11.4.4 契約情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.3.3 契約情報を削除する手順

管理する必要がなくなった契約情報を削除できます。契約情報は、契約状態が [途中解約] および [満了] の場合だけ削除できます。

なお、契約情報を削除すると、ハードウェア資産情報やソフトウェアライセンス情報との関連づけも削除されます。

契約情報を削除するには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. インフォメーションエリアで削除したい契約情報を選択して、[操作メニュー] の [契約を削除する] を選択します。
複数の契約情報を選択して一括削除することもできます。
4. 表示されるダイアログで [OK] ボタンをクリックします。

選択した契約情報が削除されます。

関連リンク

- [11.3.1 契約情報を追加する手順](#)
- [11.3.2 契約情報を編集する手順](#)
- [11.3.5 契約状態を変更する手順](#)
- [11.4.4 契約情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.3.4 契約状態を追加する手順

[契約状態] に任意の項目を追加できます。これによって、運用に合わせた契約状態の管理を実現できます。

契約状態を追加するには：

1. 設定画面の [資産管理項目の設定] 画面を表示します。
2. [契約情報の追加管理項目] で [契約状態] の [編集] ボタンをクリックします。
3. [管理項目の編集] ダイアログで [追加] ボタンをクリックします。
4. [項目の追加] ダイアログで項目名を入力して [OK] ボタンをクリックします。
5. [管理項目の編集] ダイアログで [OK] ボタンをクリックします。

契約状態の項目が追加されます。なお、追加できる項目は、デフォルトの項目とは別に 100 種類までです。

[管理項目の編集] ダイアログでは、既存の項目を編集・削除したり、項目の並び順を変更したりできます。

ポイント

デフォルトの項目（契約中、途中解約、満了）は、編集および削除できません。また、システム管理者が追加した契約状態のうち、フィルタの条件として保存している契約状態も、削除できません。

ポイント

契約状態は、契約情報を設定するときに、[(新規追加)] を選択して追加することもできます。

11.3.5 契約状態を変更する手順

[契約状態] を変更する場合は、[契約情報の編集] ダイアログ以外に、[契約状態の変更] ダイアログでも変更できます。

契約状態を変更するには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. インフォメーションエリアで [契約状態] を変更したい契約情報を選択して、[状態を変更] ボタンをクリックします。
複数の契約情報を選択して一括変更することもできます。
4. 表示されるダイアログで、[契約状態] を変更して、[OK] ボタンをクリックします。

選択した契約情報の [契約状態] が更新されます。

ポイント

ほかの項目を変更したい場合は、[編集] ボタンをクリックして表示されるダイアログで編集できます。

関連リンク

- [11.3.1 契約情報を追加する手順](#)
- [11.3.2 契約情報を編集する手順](#)
- [11.3.3 契約情報を削除する手順](#)
- [11.4.4 契約情報をインポートする手順](#)
- [11.5 資産情報をエクスポートする手順](#)

11.3.6 契約対象のハードウェア資産を関連づける手順

契約情報とハードウェア資産情報を関連づけることで、契約対象のハードウェア資産を管理できます。また、ハードウェア資産情報を関連づけると、ハードウェア資産の契約費用の推移や契約種別などを管理できるようになります。

契約対象のハードウェア資産を関連づけるには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. インフォメーションエリアで、契約対象を設定したい契約情報を選択します。
4. 画面下部に表示される [ハードウェア資産] タブを表示します。
5. タブ中の [変更] ボタンをクリックします。
6. 表示されるダイアログで対応するハードウェア資産情報を選択して、[OK] ボタンをクリックします。

選択した契約情報にハードウェア資産情報が関連づけられます。

ポイント

契約情報を追加または編集するダイアログの [関連情報] で、契約対象のハードウェア資産情報を関連づけることもできます。

関連リンク

- [11.1.12 ハードウェア資産に対する契約情報を関連づける手順](#)

11.3.7 契約対象のソフトウェアライセンスを関連づける手順

契約情報とソフトウェアライセンス情報を関連づけることで、契約対象のソフトウェアライセンスを管理できます。また、ソフトウェアライセンス情報を関連づけると、ソフトウェアライセンスの契約費用の推移や契約種別などを管理できるようになります。

契約対象のソフトウェアライセンスを関連づけるには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. インフォメーションエリアで、契約対象を設定したい契約情報を選択します。
4. 画面下部に表示される [ソフトウェアライセンス] タブを表示します。

5. タブ中の [変更] ボタンをクリックします。

6. 表示されるダイアログで対応するソフトウェアライセンス情報を選択して、[OK] ボタンをクリックします。

選択した契約情報にソフトウェアライセンス情報が関連づけられます。

ポイント

契約情報を追加または編集するダイアログの [関連情報] で、契約対象のソフトウェアライセンス情報を関連づけることもできます。

関連リンク

- [11.2.14 ソフトウェアライセンスに対する契約情報を関連づける手順](#)

11.4 資産情報をインポートする

11.4.1 ハードウェア資産情報をインポートする手順

CSV ファイルのハードウェア資産情報をインポートして、新規にハードウェア資産情報を追加したり、ハードウェア資産情報を一括で編集したりできます。

ハードウェア資産情報のインポートは、[資産情報をインポートしましょう] ウィザードで実行します。

ポイント

ハードウェア資産情報は、`ioutils importasset` コマンドを実行してインポートすることもできます。定期的に CSV ファイルからハードウェア資産情報をインポートする場合は、コマンドを使用することをお勧めします。

[資産情報をインポートしましょう] ウィザードでは、CSV ファイルを読み込んだあとに、CSV ファイルの項目と JP1/IT Desktop Management 2 の管理項目を対応づけます。また、インポートする際に既存の情報と引き当てるキー（マッピングキー）を設定します。インポートの設定が終わったら設定内容を確認し、設定内容に問題がなければインポートを実行します。

ハードウェア資産情報をインポートするには：

1. 資産画面を表示します。
2. メニューエリアの [ハードウェア資産情報] で任意のグループを選択します。
3. [操作メニュー] の [ハードウェア資産一覧をインポートする] を選択してウィザードを起動します。
4. [はじめに...] 画面でインポートの流れを確認して、[次へ] ボタンをクリックします。
5. [インポートファイルを読み込む] 画面でインポートする CSV ファイルを指定して、[次へ] ボタンをクリックします。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
6. [データの項目名を対応づける] 画面で [マッピングキー]、[CSV ファイルの項目名]、[ヘッダ行]、および [データ開始行] を指定して、[次へ] ボタンをクリックします。
[テンプレート名] から作成済みのテンプレートを選択することもできます。
7. [テンプレートの保存] ダイアログで、テンプレート名と説明を指定して、[はい] ボタンをクリックします。
テンプレートを保存しない場合は、[いいえ] ボタンをクリックします。
8. [設定内容を確認する] 画面で設定内容を確認して、[インポート] ボタンをクリックします。

一部のデータがインポートできなかった場合は、[無効となったデータ、追加または更新ができなかった項目]が表示されます。[無効となったデータ、追加または更新ができなかった項目]を確認して CSV ファイルを修正したあと、[CSV ファイルの読み込みとチェックを再実行] ボタンで再度 CSV ファイルを読み込んでからインポートすることをお勧めします。なお、[エクスポート] ボタンをクリックすると、表示内容を出力できます。

9. [完了!] 画面でインポート結果を確認して、[閉じる] ボタンをクリックします。

CSV ファイルのデータがインポートされます。[インポート履歴の確認へ] ボタンをクリックすると、インポート状況を確認できます。

インポートされた情報が意図したとおりに登録されているか確認してください。もし、正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

ポイント

[資産情報をインポートしましょう] ウィザードは、設定画面の [資産管理] — [インポート履歴の確認] から起動できます。設定画面から起動した場合は、[インポートファイルを読み込む] 画面で [インポートする資産情報] に [ハードウェア資産情報] を指定してください。

関連リンク

- [11.5 資産情報をエクスポートする手順](#)
- [17.4 ioutils exportasset \(ハードウェア資産情報のエクスポート\)](#)
- [17.5 ioutils importasset \(ハードウェア資産情報のインポート\)](#)
- [17.8 ioutils exporttemplate \(テンプレートのエクスポート\)](#)
- [17.9 ioutils importtemplate \(テンプレートのインポート\)](#)

11.4.2 ソフトウェアライセンス情報をインポートする手順

CSV ファイルのソフトウェアライセンス情報をインポートして、新規にソフトウェアライセンス情報を追加したり、ソフトウェアライセンス情報を一括で編集したりできます。

ソフトウェアライセンス情報のインポートは、[資産情報をインポートしましょう] ウィザードで実行します。

[資産情報をインポートしましょう] ウィザードでは、CSV ファイルを読み込んだあとに、CSV ファイルの項目と JP1/IT Desktop Management 2 の管理項目を対応づけます。また、インポートする際に既存の情報と引き当てるキー（マッピングキー）を設定します。インポートの設定が終わったら設定内容を確認し、設定内容に問題がなければインポートを実行します。

ソフトウェアライセンス情報をインポートするには：

1. 資産画面を表示します。
2. メニューエリアで [ソフトウェアライセンス] – [ソフトウェアライセンス一覧] を選択します。
3. [操作メニュー] の [ソフトウェアライセンス一覧をインポートする] を選択してウィザードを起動します。
4. [はじめに...] 画面でインポートの流れを確認して、[次へ] ボタンをクリックします。
5. [インポートファイルを読み込む] 画面でインポートする CSV ファイルを指定して、[次へ] ボタンをクリックします。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
6. [データの項目名を対応づける] 画面で [マッピングキー]、[CSV ファイルの項目名]、[ヘッダ行]、および [データ開始行] を指定して、[次へ] ボタンをクリックします。
[テンプレート名] から作成済みのテンプレートを選択することもできます。
7. [テンプレートの保存] ダイアログで、テンプレート名と説明を指定して、[はい] ボタンをクリックします。
テンプレートを保存しない場合は、[いいえ] ボタンをクリックします。
8. [設定内容を確認する] 画面で設定内容を確認して、[インポート] ボタンをクリックします。
一部のデータがインポートできなかった場合は、[無効となったデータ、追加または更新ができなかった項目] が表示されます。[無効となったデータ、追加または更新ができなかった項目] を確認して CSV ファイルを修正したあと、[CSV ファイルの読み込みとチェックを再実行] ボタンで再度 CSV ファイルを読み込んでからインポートすることをお勧めします。なお、[エクスポート] ボタンをクリックすると、表示内容を出力できます。
9. [完了!] 画面でインポート結果を確認して、[閉じる] ボタンをクリックします。

CSV ファイルのデータがインポートされます。[インポート履歴の確認へ] ボタンをクリックすると、インポート状況を確認できます。

インポートされた情報が意図したとおりに登録されているか確認してください。もし、正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

インポートが完了したら、ソフトウェアライセンスに対応する管理ソフトウェア情報を設定してください。ソフトウェアライセンスの利用状況が確認できるようになります。

ポイント

「資産情報をインポートしましょう」ウィザードは、設定画面の「資産管理」－「インポート履歴の確認」からも起動できます。設定画面から起動した場合は、「インポートファイルを読み込む」画面で「インポートする資産情報」に「ソフトウェアライセンス情報」を指定してください。

関連リンク

- 11.5 資産情報をエクスポートする手順
- 17.8 ioutils exporttemplate (テンプレートのエクスポート)
- 17.9 ioutils importtemplate (テンプレートのインポート)

11.4.3 管理ソフトウェア情報をインポートする手順

CSV ファイルの管理ソフトウェア情報をインポートして、新規に管理ソフトウェア情報を追加したり、管理ソフトウェア情報を一括で編集したりできます。

管理ソフトウェア情報のインポートは、「資産情報をインポートしましょう」ウィザードで実行します。

「資産情報をインポートしましょう」ウィザードでは、CSV ファイルを読み込んだあとに、CSV ファイルの項目と JP1/IT Desktop Management 2 の管理項目を対応づけます。また、インポートする際に既存の情報と引き当てるキー（マッピングキー）を設定します。インポートの設定が終わったら設定内容を確認し、設定内容に問題がなければインポートを実行します。

管理ソフトウェア情報をインポートするには：

1. 資産画面を表示します。
2. メニューエリアで「管理ソフトウェア」－「管理ソフトウェア一覧」を選択します。
3. 「操作メニュー」の「管理ソフトウェア一覧をインポートする」を選択してウィザードを起動します。
4. 「はじめに...」画面でインポートの流れを確認して、「次へ」ボタンをクリックします。
5. 「インポートファイルを読み込む」画面でインポートする CSV ファイルを指定して、「次へ」ボタンをクリックします。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
6. 「データの項目名を対応づける」画面で「マッピングキー」、「CSV ファイルの項目名」、「ヘッダ行」、および「データ開始行」を指定して、「次へ」ボタンをクリックします。
「テンプレート名」から作成済みのテンプレートを選択することもできます。

7. [テンプレートの保存] ダイアログで、テンプレート名と説明を指定して、[はい] ボタンをクリックします。

テンプレートを保存しない場合は、[いいえ] ボタンをクリックします。

8. [設定内容を確認する] 画面で設定内容を確認して、[インポート] ボタンをクリックします。

一部のデータがインポートできなかった場合は、[無効となったデータ、追加または更新ができなかった項目] が表示されます。[無効となったデータ、追加または更新ができなかった項目] を確認して CSV ファイルを修正したあと、[CSV ファイルの読み込みとチェックを再実行] ボタンで再度 CSV ファイルを読み込んでからインポートすることをお勧めします。なお、[エクスポート] ボタンをクリックすると、表示内容を出力できます。

9. [完了!] 画面でインポート結果を確認して、[閉じる] ボタンをクリックします。

CSV ファイルのデータがインポートされます。[インポート履歴の確認へ] ボタンをクリックすると、インポート状況を確認できます。

インポートされた情報が意図したとおりに登録されているか確認してください。もし、正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

インポートが完了したら、管理ソフトウェア情報を編集して、[インストールソフトウェア名] と [対象ソフトウェアライセンス情報] を設定してください。ソフトウェアライセンスの利用状況が確認できるようになります。

ポイント

[資産情報をインポートしましょう] ウィザードは、設定画面の [資産管理] — [インポート履歴の確認] から起動できます。設定画面から起動した場合は、[インポートファイルを読み込む] 画面で [インポートする資産情報] に [管理ソフトウェア情報] を指定してください。

関連リンク

- 11.5 資産情報をエクスポートする手順
- 17.8 ioutils exporttemplate (テンプレートのエクスポート)
- 17.9 ioutils importtemplate (テンプレートのインポート)

11.4.4 契約情報をインポートする手順

CSV ファイルの契約情報をインポートして、新規に契約情報を追加したり、契約情報を一括で編集したりできます。

契約情報のインポートは、[資産情報をインポートしましょう] ウィザードで実行します。

[資産情報をインポートしましょう] ウィザードでは、CSV ファイルを読み込んだあとに、CSV ファイルの項目と JP1/IT Desktop Management 2 の管理項目を対応づけます。また、インポートする際に既存の情報と引き当てるキー（マッピングキー）を設定します。インポートの設定が終わったら設定内容を確認し、設定内容に問題がなければインポートを実行します。

契約情報をインポートするには：

1. 資産画面を表示します。
2. メニューエリアで [契約] - [契約一覧] を選択します。
3. [操作メニュー] の [契約一覧をインポートする] を選択してウィザードを起動します。
4. [はじめに...] 画面でインポートの流れを確認して、[次へ] ボタンをクリックします。
5. [インポートファイルを読み込む] 画面でインポートする CSV ファイルを指定して、[次へ] ボタンをクリックします。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
6. [データの項目名を対応づける] 画面で [マッピングキー]、[CSV ファイルの項目名]、[ヘッダ行]、および [データ開始行] を指定して、[次へ] ボタンをクリックします。
[テンプレート名] から作成済みのテンプレートを選択することもできます。
7. [テンプレートの保存] ダイアログで、テンプレート名と説明を指定して、[はい] ボタンをクリックします。
テンプレートを保存しない場合は、[いいえ] ボタンをクリックします。
8. [設定内容を確認する] 画面で設定内容を確認して、[インポート] ボタンをクリックします。
一部のデータがインポートできなかった場合は、[無効となったデータ、追加または更新ができなかった項目] が表示されます。[無効となったデータ、追加または更新ができなかった項目] を確認して CSV ファイルを修正したあと、[CSV ファイルの読み込みとチェックを再実行] ボタンで再度 CSV ファイルを読み込んでからインポートすることをお勧めします。なお、[エクスポート] ボタンをクリックすると、表示内容を出力できます。
9. [完了!] 画面でインポート結果を確認して、[閉じる] ボタンをクリックします。

CSV ファイルのデータがインポートされます。[インポート履歴の確認へ] ボタンをクリックすると、インポート状況を確認できます。

インポートされた情報が意図したとおりに登録されているか確認してください。もし、正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

ポイント

「資産情報をインポートしましょう」ウィザードは、設定画面の「資産管理」－「インポート履歴の確認」からも起動できます。設定画面から起動した場合は、「インポートファイルを読み込む」画面で「インポートする資産情報」に「契約情報」を指定してください。

関連リンク

- 11.5 資産情報をエクスポートする手順
- 17.8 ioutils exporttemplate (テンプレートのエクスポート)
- 17.9 ioutils importtemplate (テンプレートのインポート)

11.4.5 契約会社リストをインポートする手順

CSV ファイルの契約会社リストをインポートして、新規に契約会社情報を追加したり、契約会社リストを一括で編集したりできます。

契約会社リストのインポートは、「資産情報をインポートしましょう」ウィザードで実行します。

「資産情報をインポートしましょう」ウィザードでは、CSV ファイルを読み込んだあとに、CSV ファイルの項目と JP1/IT Desktop Management 2 の管理項目を対応づけます。また、インポートする際に既存の情報と引き当てるキー（マッピングキー）を設定します。インポートの設定が終わったら設定内容を確認し、設定内容に問題がなければインポートを実行します。

契約会社リストをインポートするには：

1. 設定画面の「資産管理」－「契約会社リストの設定」を選択します。
2. 「操作メニュー」の「契約会社一覧をインポートする」を選択してウィザードを起動します。
3. 「はじめに...」画面でインポートの流れを確認して、「次へ」ボタンをクリックします。
4. 「インポートファイルを読み込む」画面でインポートする CSV ファイルを指定して、「次へ」ボタンをクリックします。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
5. 「データの項目名を対応づける」画面で「マッピングキー」、「CSV ファイルの項目名」、「ヘッダ行」、および「データ開始行」を指定して、「次へ」ボタンをクリックします。
「テンプレート名」から作成済みのテンプレートを選択することもできます。
6. 「テンプレートの保存」ダイアログで、テンプレート名と説明を指定して、「はい」ボタンをクリックします。

テンプレートを保存しない場合は、[いいえ] ボタンをクリックします。

7. [設定内容を確認する] 画面で設定内容を確認して、[インポート] ボタンをクリックします。

一部のデータがインポートできなかった場合は、[無効となったデータ、追加または更新ができなかった項目] が表示されます。[無効となったデータ、追加または更新ができなかった項目] を確認して CSV ファイルを修正したあと、[CSV ファイルの読み込みとチェックを再実行] ボタンで再度 CSV ファイルを読み込んでからインポートすることをお勧めします。なお、[エクスポート] ボタンをクリックすると、表示内容を出力できます。

8. [完了!] 画面でインポート結果を確認して、[閉じる] ボタンをクリックします。

CSV ファイルのデータがインポートされます。[インポート履歴の確認へ] ボタンをクリックすると、インポート状況を確認できます。

インポートされた情報が意図したとおりに登録されているか確認してください。もし、正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

ポイント

[資産情報をインポートしましょう] ウィザードは、設定画面の [資産管理] – [インポート履歴の確認] から起動できます。設定画面から起動した場合は、[インポートファイルを読み込む] 画面で [インポートする資産情報] に [契約会社リスト] を指定してください。

関連リンク

- [15.4.12 契約会社リストをエクスポートする手順](#)
- [17.8 ioutils exporttemplate \(テンプレートのエクスポート\)](#)
- [17.9 ioutils importtemplate \(テンプレートのインポート\)](#)

11.5 資産情報をエクスポートする手順

資産画面のインフォメーションエリアに表示された資産情報を、CSV ファイルにエクスポートできます。

特定の資産情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、総務部の資産情報だけエクスポートする場合は、[部署] の階層に「総務部」が設定されている資産情報をフィルタリングして表示します。

ポイント

ハードウェア資産情報は、`ioutils exportasset` コマンドを実行してエクスポートすることもできます。定期的に資産情報をエクスポートする場合は、コマンドを使用することをお勧めします。

ポイント

資産画面の [ハードウェア資産] 画面でインフォメーションエリアに「-」が表示されている項目は、ハードウェア資産情報をエクスポートすると、「-」の部分が空文字で出力されます。これは、エクスポートしたハードウェア資産情報をそのままインポートする際に、正常にインポートできるようにするためです。

資産情報をエクスポートするには：

1. 資産画面を表示します。
2. エクスポートする資産情報をインフォメーションエリアに表示します。
3. [操作メニュー] の [資産情報の一覧名をエクスポートする] を選択します。
4. [エクスポートする項目の選択] ダイアログで、エクスポートする項目をチェックして、[OK] ボタンをクリックします。

エクスポートされる CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトの文字コードは、「UTF-8」です。

5. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

関連リンク

- [17.4 ioutils exportasset \(ハードウェア資産情報のエクスポート\)](#)

12

ソフトウェアやファイルを配布する

ここでは、ソフトウェアのインストール・アンインストールやファイルの配布について説明します。

12.1 コンピュータにソフトウェアをインストールする手順

[ソフトウェアをインストールしましょう] ウィザードを使って、利用者のコンピュータにソフトウェアを配布してインストールできます。

[ソフトウェアをインストールしましょう] ウィザードでは、インストールするソフトウェアを登録したパッケージと、パッケージの配布を実行するタスクを作成します。ウィザードを完了すると、タスクに指定したスケジュールに従って、パッケージが配布されます。

コンピュータにソフトウェアをインストールするには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [操作メニュー] から [インストールウィザードを起動する] を選択してウィザードを起動します。
4. [はじめに...] 画面でウィザードの流れを確認して、[次へ] ボタンをクリックします。
5. [ソフトウェアを指定する] 画面で [新しいパッケージを作成する] を選択して、パッケージに登録するファイルを指定し、[次へ] ボタンをクリックします。
事前にパッケージを作成している場合は、作成済みのパッケージを選択することもできます。
6. [パッケージを設定する] 画面でパッケージ情報を設定して、[次へ] ボタンをクリックします。
7. [パッケージ配布タスクを作成する] 画面で、配布を実行するスケジュールなどを設定して、[次へ] ボタンをクリックします。
[対象のコンピュータでの動作] をクリックすると、インストールを実行するタイミングや、利用者に通知するメッセージなどを設定できます。
8. [対象のコンピュータを選択する] 画面で、[変更] ボタンをクリックします。
9. [対象のコンピュータの変更] ダイアログで、ソフトウェアをインストールするコンピュータを指定して、[OK] ボタンをクリックします。
10. [次へ] ボタンをクリックします。
11. [設定内容を確認する] 画面で、設定内容を確認して [完了] ボタンをクリックします。
12. [完了!] 画面で、[閉じる] ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータにソフトウェアが配布されてインストールされます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク] 画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でソフトウェアのインストールを延期できます。

関連リンク

- [12.6 利用者側でダウンロードやインストールを延期する](#)
- [12.5.5 タスクを中止する手順](#)

12.2 コンピュータにファイルを配布する手順

[ファイルを配布しましょう] ウィザードを使って、利用者のコンピュータにファイルを配布できます。

[ファイルを配布しましょう] ウィザードでは、配布するファイルを登録したパッケージと、パッケージの配布を実行するタスクを作成します。ウィザードを完了すると、タスクに指定したスケジュールに従って、パッケージが配布されます。

コンピュータにファイルを配布するには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [操作メニュー] から [ファイル配布ウィザードを起動する] を選択してウィザードを起動します。
4. [はじめに...] 画面でウィザードの流れを確認して、[次へ] ボタンをクリックします。
5. [ファイルを指定する] 画面で [新しいパッケージを作成する] を選択して、パッケージに登録するファイルを指定し、[次へ] ボタンをクリックします。
事前にパッケージを作成している場合は、作成済みのパッケージを選択することもできます。
6. [パッケージを設定する] 画面でパッケージ情報を設定して、[次へ] ボタンをクリックします。
7. [パッケージ配布タスクを作成する] 画面で、配布を実行するスケジュールなどを設定して、[次へ] ボタンをクリックします。
[対象のコンピュータでの動作] をクリックすると、パッケージ配布後にファイルを配布するタイミングや、利用者に通知するメッセージなどを設定できます。
8. [対象のコンピュータを選択する] 画面で、[変更] ボタンをクリックします。
9. [対象のコンピュータの変更] ダイアログで、ファイルを配布するコンピュータを指定して、[OK] ボタンをクリックします。
10. [次へ] ボタンをクリックします。
11. [設定内容を確認する] 画面で、設定内容を確認して [完了] ボタンをクリックします。
12. [完了!] 画面で、[閉じる] ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータにファイルが配布されます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク一覧] 画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でファイルの配布を延期できます。

関連リンク

- [12.6 利用者側でダウンロードやインストールを延期する](#)
- [12.5.5 タスクを中止する手順](#)

12.3 コンピュータからソフトウェアをアンインストールする手順

[ソフトウェアをアンインストールしましょう] ウィザードを使って、利用者のコンピュータからソフトウェアをアンインストールできます。

[ソフトウェアをアンインストールしましょう] ウィザードでは、ソフトウェアをアンインストールするためのタスクを作成します。ウィザードを完了すると、指定したスケジュールに従って、アンインストールタスクが実行されます。

コンピュータからソフトウェアをアンインストールするには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [操作メニュー] から [アンインストールウィザードを起動する] を選択してウィザードを起動します。
4. [はじめに...] 画面でウィザードの流れを確認して、[次へ] ボタンをクリックします。
5. [アンインストールタスクを作成する] 画面で、アンインストールするソフトウェアの情報や、タスクを実行するスケジュールなどを設定して、[次へ] ボタンをクリックします。
[対象のコンピュータでの動作] をクリックすると、アンインストールを実行するタイミングや、利用者に通知するメッセージなどを設定できます。
この画面で設定したソフトウェア名およびバージョンに完全一致するソフトウェアだけがアンインストールされます。
6. [対象のコンピュータを選択する] 画面で、[変更] ボタンをクリックします。
7. [対象のコンピュータの変更] ダイアログで、ソフトウェアをアンインストールするコンピュータを指定して、[OK] ボタンをクリックします。
8. [次へ] ボタンをクリックします。
9. [設定内容を確認する] 画面で、設定内容を確認して [完了] ボタンをクリックします。
10. [完了!] 画面で、[閉じる] ボタンをクリックします。

作成したタスクのスケジュールに従って、指定したコンピュータからソフトウェアがアンインストールされます。タスクの実行状況は、配布 (ITDM 互換) 画面の [タスク一覧] 画面で確認してください。

ポイント

急ぎの業務や重要な業務の最中は、利用者側でソフトウェアのアンインストールを延期できます。詳細については、「[12.6 利用者側でダウンロードやインストールを延期する](#)」を参照してください。

関連リンク

- [12.5.5 タスクを中止する手順](#)

12.4 パッケージを管理する

12.4.1 パッケージを追加する手順

配布（ITDM 互換）画面の [パッケージ] 画面の一覧に、ソフトウェアやファイルを登録したパッケージを追加できます。

パッケージを配布すると、対象のコンピュータにソフトウェアをインストールしたり、ファイルを配布したりできます。なお、パッケージを配布するためには、対応するタスクを作成する必要があります。タスクの作成方法については、「[12.5.1 タスクを追加する手順](#)」を参照してください。

パッケージを追加するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで [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、パッケージの情報を入力して、[OK] ボタンをクリックします。

パッケージが追加され、パッケージ一覧に表示されます。

関連リンク

- [12.4.2 パッケージを編集する手順](#)
- [12.4.3 パッケージを削除する手順](#)
- [12.4.4 パッケージ情報をエクスポートする手順](#)

12.4.2 パッケージを編集する手順

登録済みのパッケージを編集できます。パッケージの説明、展開先フォルダ、配布先フォルダなどを変更したいときに編集します。

パッケージを編集するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] 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パッケージの [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。

選択したパッケージが更新されます。

関連リンク

- [12.4.1 パッケージを追加する手順](#)
- [12.4.3 パッケージを削除する手順](#)
- [12.4.4 パッケージ情報をエクスポートする手順](#)

12.4.3 パッケージを削除する手順

利用しなくなったパッケージを削除できます。

■ 注意事項

タスクで指定されているパッケージは削除できません。[パッケージ一覧] 画面の [タスク] タブを確認して該当するタスクをすべて中止し、[タスク一覧] 画面でタスクを削除してから、パッケージを削除してください。

パッケージを削除するには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [パッケージ] - [パッケージ一覧] を選択します。
3. インフォメーションエリアで削除したいパッケージを選択して、[削除] ボタンを選択します。
複数のパッケージを選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したパッケージが削除されます。

関連リンク

- [12.4.1 パッケージを追加する手順](#)
- [12.4.2 パッケージを編集する手順](#)
- [12.4.4 パッケージ情報をエクスポートする手順](#)

12.4.4 パッケージ情報をエクスポートする手順

配布 (ITDM 互換) 画面のインフォメーションエリアに表示されたパッケージ情報を、CSV ファイルにエクスポート (一括出力) できます。

特定のパッケージ情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、ファイル配布のパッケージ情報だけエクスポートする場合は、[パッケージ種別] に「ファイル配布」が設定されているパッケージ情報をフィルタリングして表示します。

パッケージ情報をエクスポートするには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [パッケージ] – [パッケージ一覧] を選択します。
3. エクスポートするパッケージ情報をインフォメーションエリアに表示します。
4. [操作メニュー] の [パッケージ一覧をエクスポートする] を選択します。
5. 表示されるダイアログで、エクスポートする項目にチェックをして、[OK] ボタンをクリックします。
エクスポートする CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトの文字コードは「UTF-8」です。
6. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

関連リンク

- [12.4.1 パッケージを追加する手順](#)
- [12.4.2 パッケージを編集する手順](#)
- [12.4.3 パッケージを削除する手順](#)

12.5 タスクを管理する

12.5.1 タスクを追加する手順

配布（ITDM 互換）画面の [タスク] 画面の一覧に、タスクを追加できます。タスクを追加すると、対象のコンピュータにソフトウェアをインストール、ファイルを配布、またはソフトウェアをアンインストールできます。

なお、パッケージ配布タスクを作成する場合は、配布するソフトウェアやファイルを登録したパッケージを事前に作成する必要があります。パッケージの作成方法については、「[12.4.1 パッケージを追加する手順](#)」を参照してください。

タスクを追加するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] - [タスク一覧] を選択します。
3. インフォメーションエリアで [パッケージ配布のタスクを追加] ボタンまたは [アンインストールのタスクを追加] ボタンをクリックします。
4. 表示されるダイアログで、タスクの情報を入力して、[OK] ボタンをクリックします。

タスクが追加され、タスク一覧に表示されます。

ポイント

自動対策で実行されるタスクは、セキュリティポリシーで更新プログラム、使用必須ソフトウェアまたは使用禁止ソフトウェアの自動対策を設定するときに作成されます。

ポイント

アンインストールタスクは、機器画面の [ソフトウェア情報] 画面で、使用禁止ソフトウェアを設定することでも作成できます。

ポイント

登録済みのタスクをベースに別のタスクを追加したい場合は、タスクをコピーしてください。

関連リンク

- [6.20 使用禁止ソフトウェアを設定する手順](#)

- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.4 タスクを削除する手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.5 タスクを中止する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.2 タスクを編集する手順

登録済みのタスクを編集できます。実行スケジュールを変更したり、対象のコンピュータを追加したりするときに編集します。

タスクを編集するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] – [タスク一覧] 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タスクの [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タスクの情報を編集して、[OK] ボタンをクリックします。

選択したタスクが更新されます。

ポイント

登録済みのタスクをベースに別のタスクを追加したい場合は、タスクをコピーしてください。

なお、自動対策で実行されるタスクは編集できません。

関連リンク

- [12.5.1 タスクを追加する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.4 タスクを削除する手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.5 タスクを中止する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.3 タスクをコピーする手順

登録済みのタスクをコピーして編集できます。登録済みのタスクをベースに別のタスクを追加する場合に、タスクをコピーします。

例えば、対象のコンピュータの台数が多いので複数の日に分けてパッケージを配布する場合に、登録済みのタスクの実行スケジュールと対象コンピュータを編集して、新しいタスクを追加できます。

タスクをコピーするには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] - [タスク一覧] を選択します。
3. インフォメーションエリアでコピーしたいタスクの [コピー] ボタンをクリックします。
4. 表示されるダイアログでタスクの情報を編集して、[OK] ボタンをクリックします。

新しいタスクが追加され、パッケージ一覧に表示されます。

なお、自動対策で実行されるタスクはコピーできません。

関連リンク

- [12.5.1 タスクを追加する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.4 タスクを削除する手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.5 タスクを中止する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.4 タスクを削除する手順

不要になったタスクを削除できます。

実行中のタスクを削除する場合は、タスクが中止されてから削除されます。ただし、利用者のコンピュータにパッケージが配布され、すでにソフトウェアのインストール、ファイルの配布、またはソフトウェアのアンインストールの処理が開始されている場合は、タスクを中止できないため削除できません。

注意事項

自動対策で実行されるタスクを削除する場合は、セキュリティポリシーの「使用ソフトウェア」で設定した自動対策を解除、使用禁止ソフトウェアまたは使用必須ソフトウェアを削除してください。セキュリティポリシーの設定に応じて、タスクが自動的に削除されます。

タスクを削除するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで「タスク」－「タスク一覧」を選択します。
3. インフォメーションエリアで削除したいタスクを選択して、「操作メニュー」の「削除する」を選択します。
複数のタスクを選択して一括削除することもできます。
4. 表示されるダイアログで、「OK」ボタンをクリックします。

選択したタスクが削除されます。

関連リンク

- [12.5.1 タスクを追加する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.5 タスクを中止する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.5 タスクを中止する手順

タスク状態が、「成功」、「失敗」、および「キャンセル」以外のタスクを中止できます。

注意事項

利用者のコンピュータにパッケージが配布され、すでにソフトウェアのインストール、ファイルの配布、またはソフトウェアのアンインストールの処理が開始されている場合は、タスクを中止できません。

タスクを中止するには：

1. 配布（ITDM 互換）画面を表示します。

2. メニューエリアで [タスク] – [タスク一覧] を選択します。
3. インフォメーションエリアで中止したいタスクを選択して、[操作メニュー] の [タスクを中止する] を選択します。
複数のタスクを選択して一括で中止することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

タスクが中止されます。

コンピュータを指定してタスクを中止するには：

1. 配布 (ITDM 互換) 画面を表示します。
2. メニューエリアで [タスク] – [タスク一覧] を選択します。
3. インフォメーションエリアで中止したいタスクを選択して、[タスク状態] タブを表示します。
4. タブ中で、タスクを中止したいコンピュータを選択します。
複数のコンピュータを選択して一括で中止することもできます。
5. タブ中の [タスクを中止] 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。

タスクが中止されます。

関連リンク

- [12.5.1 タスクを追加する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.4 タスクを削除する手順](#)
- [12.5.6 タスクを再実行する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.6 タスクを再実行する手順

タスクの実行に失敗したり、タスクを中止したりした場合は、タスクを再実行できます。

タスクの再実行は、[タスク状態] タブの [タスク状態] が [失敗] または [キャンセル] のコンピュータにだけできます。

タスクを再実行するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] – [タスク一覧] を選択します。
3. インフォメーションエリアで再実行したいタスクを選択して、[操作メニュー] の [タスクを再実行する] を選択します。
複数のタスクを選択して一括で再実行することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

すぐにタスクが再実行されます。

コンピュータを指定してタスクを再実行するには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] – [タスク一覧] を選択します。
3. インフォメーションエリアで再実行したいタスクを選択して、[タスク状態] タブを表示します。
4. タブ中で、タスクを再実行したいコンピュータを選択します。
複数のコンピュータを選択して一括で再実行することもできます。
5. タブ中の [タスクを再実行] 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。

すぐにタスクが再実行されます。

注意事項

タスクに指定した実行スケジュールに関係なく、即時再実行されます。指定した実行スケジュールでタスクを再実行したい場合は、タスクを編集またはコピーしてください。

関連リンク

- [12.5.1 タスクを追加する手順](#)
- [12.5.2 タスクを編集する手順](#)
- [12.5.3 タスクをコピーする手順](#)
- [12.5.4 タスクを削除する手順](#)
- [12.5.5 タスクを中止する手順](#)
- [12.5.7 タスク情報をエクスポートする手順](#)

12.5.7 タスク情報をエクスポートする手順

資産画面のインフォメーションエリアに表示されたタスク情報を、CSV ファイルにエクスポート（一括出力）できます。

特定のタスク情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、管理者が作成したタスクの情報だけエクスポートする場合は、[タスク種別] に「管理者が実行するタスク」が設定されているタスクをフィルタリングして表示します。

タスク情報をエクスポートするには：

1. 配布（ITDM 互換）画面を表示します。
2. メニューエリアで [タスク] - [タスク一覧] を選択します。
3. エクスポートするタスク情報をインフォメーションエリアに表示します。
4. [操作メニュー] の [タスク一覧をエクスポートする] を選択します。
5. 表示されるダイアログで、エクスポートする項目にチェックをして、[OK] ボタンをクリックします。
エクスポートする CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトの文字コードは「UTF-8」です。
6. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

12.6 利用者側でダウンロードやインストールを延期する

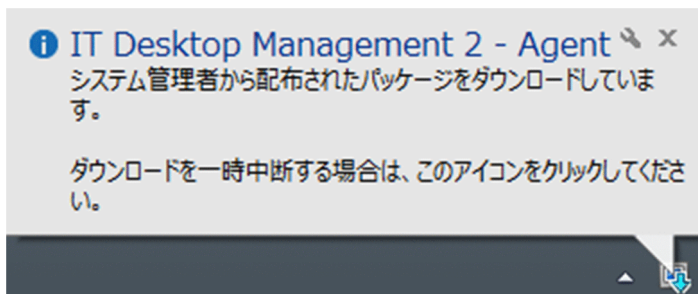
パッケージが配布されたコンピュータでは、利用者の都合に応じて、パッケージのダウンロードやソフトウェアのインストールを延期できます。急ぎの業務や重要な業務の最中は、ダウンロードやインストールを延期することで、作業が中断することを防げます。

ポイント

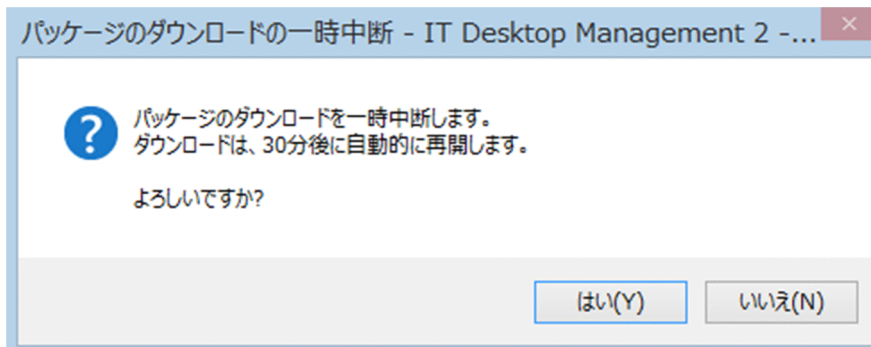
インストールの延期と同様に、ファイルの配布やアンインストールも延期できます。

ダウンロードを延期する

配布されたパッケージのダウンロードが始まると、利用者のコンピュータのタスクバーに、次のアイコンとバルーンヒントが表示されます。バルーンヒントの表示は、エージェント設定の［利用者への通知設定］の設定に従います。



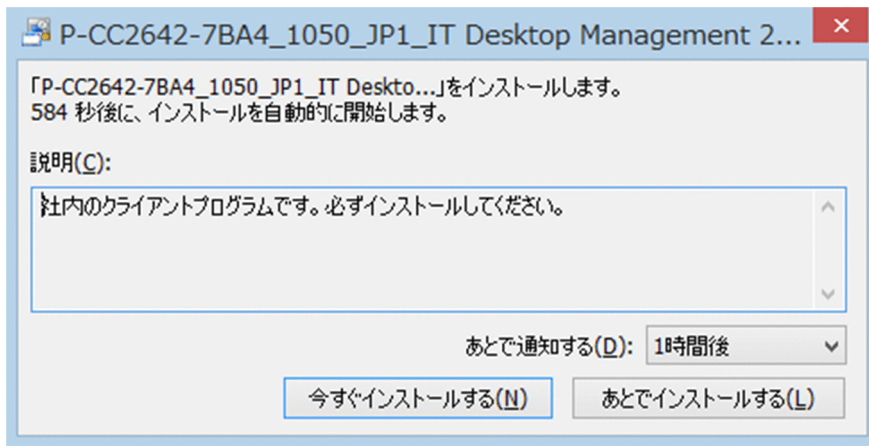
アイコンをクリックすると、パッケージのダウンロードを一時中断するダイアログが表示されます。



このダイアログで［はい］ボタンをクリックすると、ダウンロードを一時中断できます。一定時間が経過すると自動的にダウンロードが再開されます。

インストールを延期する

タスクを作成する場合に、［実行前メッセージ］が表示されるように設定したとき、ソフトウェアのインストールが開始される前に、利用者のコンピュータにインストールの開始を通知するダイアログが表示されます。



このダイアログで「あとでインストールする」ボタンをクリックすると、ソフトウェアのインストールを延期できます。延期した場合は、「あとで通知する」のプルダウンメニューで設定した時間が経過したあとで、ダイアログが再表示されます。再表示までの時間は、「10 分後」「30 分後」「1 時間後」の中から選択できます。

13

イベントを参照する

ここでは、JP1/IT Desktop Management 2 で出力されるイベントの参照方法について説明します。

13.1 イベントの詳細を確認する手順

イベントの詳細を確認すると、イベントの内容を確認したり、イベントの情報をクリップボードにコピーして活用したりできます。

イベントの詳細を表示するには：

1. イベント画面を表示します。
2. メニューエリアの「イベント」で表示したいイベントが属するグループを選択します。
3. インフォメーションエリアで、詳細を表示したいイベントを選択します。
4. 「操作メニュー」の「イベント詳細を表示する」を選択します。

「イベント詳細」ダイアログに選択したイベントの詳細が表示されます。

ポイント

インフォメーションエリアでイベントの「内容」をクリックしても、イベント詳細が表示されます。

ポイント

「イベント詳細」ダイアログの「クリップボードにコピー」ボタンをクリックすると、イベントの詳細をコピーできます。イベントの内容を報告する場合に便利です。

なお、イベントのサマリは、ホーム画面の「イベントの状況」パネルやレポート画面の「ダイジェストレポート」画面で確認できます。

13.2 イベント情報をエクスポートする手順

イベント画面のインフォメーションエリアに表示されたイベント情報を、CSV ファイルにエクスポート（一括出力）できます。

特定のイベント情報だけエクスポートしたい場合は、フィルタを使って情報を絞り込んでください。

例えば、早急に対処が必要なイベント情報だけエクスポートする場合は、[重大度] が [緊急]、[確認状態] が [未確認] のイベントをフィルタリングして表示します。

イベント情報をエクスポートするには：

1. イベント画面を表示します。
2. エクスポートするイベント情報をインフォメーションエリアに表示します。
3. [操作メニュー] の [イベント一覧をエクスポートする] を選択します。
4. 表示されるダイアログで、エクスポートする項目をチェックして、[OK] ボタンをクリックします。
エクスポートする CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトの文字コードは「UTF-8」です。
5. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

14

レポートを参照する

ここでは、レポートを表示して、組織内のセキュリティ管理や資産管理の状況を確認する方法について説明します。

14.1 レポートを表示する手順

JP1/IT Desktop Management 2 では、目的に応じて 20 種類のレポートを表示できます。

レポートを表示するには：

1. レポート画面を表示します。
2. メニューエリアから表示したいレポートをクリックします。

インフォメーションエリアに、レポートが表示されます。

なお、導入直後の場合、機能を使用していない場合など、レポートの集計対象のデータが存在しないときは、レポート内の詳細情報は表示されません。このようなときは、集計対象のデータがデータベースに保管されるように、JP1/IT Desktop Management 2 を運用してください。

ポイント

各レポートは、操作画面とは別のウィンドウで表示することもできます。複数のレポートを並べて表示したい場合に便利です。レポートを別のウィンドウで表示するには、インフォメーションエリアで、画面右上の「新しいウィンドウで開く」ボタンをクリックしてください。

14.2 最新のデータでレポートを表示する手順

一部のレポートでは、定期的に行われた集計結果が表示されます。このため、最新のデータでレポートを表示したい場合は、集計を実行する必要があります。

最新のデータでレポートを表示するには：

1. レポート画面を表示します。
2. メニューエリアから表示したいレポートをクリックします。
3. インフォメーションエリアで、画面右上の【集計】 ボタンをクリックします。
4. 表示されるダイアログで【OK】 ボタンをクリックします。

集計が実行され、最新のデータのレポートが表示されます。

ポイント

【集計】 ボタンが表示されるのは、次に示すレポートです。

- 【現状セキュリティ診断】 レポート
- 【危険レベルの状況】 レポート
- 【更新プログラムの適用状況】 レポート
- 【ウィルス対策製品の状況】 レポート
- 【使用必須ソフトウェアのインストール状況】 レポート
- 【使用禁止ソフトウェアのインストール状況】 レポート
- 【セキュリティ設定の状況】 レポート
- 【機器の管理状況】 レポート
- 【グリーン IT（省電力設定状況）】 レポート
- 【ハードウェア資産】 レポート

ポイント

【ライセンス超過ソフトウェア】 レポートおよび【ライセンス余剰ソフトウェア】 レポートは、レポートを表示するタイミングで最新のデータが集計されます。

14.3 レポートを印刷する手順

レポートを印刷できます。印刷したレポートは、そのまま報告書として利用することもできます。

レポートを印刷するには：

1. レポート画面を表示します。
2. メニューエリアから表示したいレポートをクリックします。
3. インフォメーションエリアで、画面右上の【印刷】 ボタンをクリックします。
4. 表示されるダイアログでプリンタドライバを選択し、【印刷】 ボタンをクリックします。

レポートが印刷されます。

14.4 レポートを PDF ファイルで保存する手順

レポートを PDF ファイルで保存することで、電子データで過去のレポートを保管できます。また、メールに添付して組織内に展開することもできます。

注意事項

レポートを PDF ファイルで保存するには、PDF 出力できるプリンタドライバが必要です。

レポートを PDF ファイルで保存するには：

1. レポート画面を表示します。
2. メニューエリアから表示したいレポートをクリックします。
3. インフォメーションエリアで、画面右上の [印刷] ボタンをクリックします。
4. 表示されるダイアログで、PDF 出力できるプリンタドライバを選択し、[印刷] ボタンをクリックします。

レポートが、PDF ファイルで保存されます。

15

設定をカスタマイズする

ここでは、設定画面およびセットアップでカスタマイズできる項目について説明します。

15.1 エージェントの設定

エージェントを導入しているコンピュータに対して、エージェント設定を作成して割り当てることで、エージェントのセットアップをリモートで管理できます。

また、エージェントレスで管理している機器に対しては、機器情報を収集する頻度を設定できます。

関連リンク

- [15.1.1 エージェント設定の管理](#)
- [15.1.7 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](#)

15.1.1 エージェント設定の管理

コンピュータに導入されたエージェントには、エージェント設定が割り当てられています。エージェント設定では、対象の機器の監視間隔やセットアップ、アンインストールのパスワード保護、リモートコントロール時の動作などを設定できます。エージェント設定を管理することで、各エージェントのセットアップ内容をリモートで管理できます。

特別なエージェント設定を作成していない場合、デフォルトでは「デフォルトエージェント設定」が割り当てられます。複数のエージェント設定を使い分ける必要がない場合は、デフォルトエージェント設定を編集することで、一括してエージェントの設定を変更できます。デフォルトエージェント設定は、パスワード保護のためのパスワードに、デフォルトで「manager」が設定されています。

コンピュータによって監視間隔の設定を分けたい場合や、流量制御の有無を使い分けたい場合などは、エージェント設定を作成します。エージェント設定を作成する方法については、「[15.1.2 エージェント設定を追加する手順](#)」を参照してください。

運用状況に変更があった場合、エージェント設定を編集します。エージェント設定を編集する方法については、「[15.1.3 エージェント設定を編集する手順](#)」を参照してください。

運用状況の変更に伴ってエージェント設定が不要になった場合、エージェント設定を削除します。エージェント設定を削除する方法については、「[15.1.5 エージェント設定を削除する手順](#)」を参照してください。

なお、エージェント設定は作成後に各エージェントに割り当てる必要があります。エージェント設定を各エージェントに割り当てる方法については、「[15.1.6 エージェント設定を割り当てる手順](#)」を参照してください。

ポイント

エージェント設定の割り当てを解除すると、自動的に「デフォルトエージェント設定」が割り当てられます。

関連リンク

- [6.1 機器の管理を始める方法](#)

15.1.2 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や、流量制御の有無を使い分けたい場合、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。

15.1.3 エージェント設定を編集する手順

エージェントの監視間隔を変更したい場合や、エージェント保護の設定を変更したい場合、エージェント設定を編集できます。

エージェント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 [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編集し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. 表示されるダイアログでエージェント設定の情報を編集して、[OK] ボタンをクリックします。

エージェント設定が更新されます。また、エージェント設定が割り当てられているコンピュータの設定が自動的に更新されます。

なお、「デフォルトエージェント設定」を編集する場合、エージェントを配信して新規インストールするときのインストール先フォルダを設定できます。デフォルトは、「%ProgramFiles%¥Hitachi¥jpltdma」です。

関連リンク

- [15.1.2 エージェント設定を追加する手順](#)
- [15.1.5 エージェント設定を削除する手順](#)
- [15.1.6 エージェント設定を割り当てる手順](#)

15.1.4 ネットワークモニタを有効化するコンピュータのエージェント設定を編集する手順

ネットワークモニタを有効化するコンピュータは、次に示すとおりのエージェント設定にしておく必要があります。

エージェント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 [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編集し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. 表示されるダイアログで次に示すチェックボックスをチェックして、[OK] ボタンをクリックします。
 - ・ [基本設定] - [上位システムと通信する]
 - ・ [基本設定] - [コンピュータから収集した情報を、定期的に上位システムに通知する]

エージェント設定が更新されます。また、エージェント設定が割り当てられているコンピュータの設定が自動的に更新されます。

15.1.5 エージェント設定を削除する手順

利用しなくなったエージェント設定を削除できます。

グループまたはコンピュータに割り当て済みのエージェント設定は削除できません。削除する場合は、あらかじめエージェント設定の割り当てを解除しておいてください。

エージェント設定の割り当ての解除方法については、「[15.1.6 エージェント設定を割り当てる手順](#)」を参照してください。

なお、「デフォルトエージェント設定」は削除できません。

エージェント設定を削除するには：

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削除したいエージェント設定を選択して、[削除] ボタンをクリックします。
複数のエージェント設定を選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したエージェント設定が削除されます。

関連リンク

- [15.1.2 エージェント設定を追加する手順](#)
- [15.1.3 エージェント設定を編集する手順](#)

15.1.6 エージェント設定を割り当てる手順

グループ単位またはコンピュータ単位に、エージェント設定を割り当てられます。また、割り当てたエージェント設定を解除することもできます。

デフォルトでは、「デフォルトエージェント設定」が割り当たっています。ほかのエージェント設定を割り当てている場合、割り当てを解除すると、対象のグループまたはコンピュータには「デフォルトエージェント設定」が割り当てられます。

エージェント設定を割り当てるには：

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] - [エージェント設定の割り当て] を選択します。
3. グループ単位にエージェント設定を割り当てる場合は、画面上部で対象のグループを選択して [割り当て] ボタンをクリックします。グループの構成を変更したい場合は、[対象の構成を変更] ボタンをクリックしてください。
コンピュータ単位にエージェント設定を割り当てる場合は、画面下部で対象のコンピュータを選択して [割り当て] ボタンをクリックします。
4. 表示されるダイアログで、割り当てたいエージェント設定を選択して [OK] ボタンをクリックします。
5. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したグループまたはコンピュータに、エージェント設定が割り当てられます。

エージェント設定の割り当てを解除するには：

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] - [エージェント設定の割り当て] を選択します。

3. グループのエージェント設定を解除する場合は、画面上部で対象のグループを選択して「割り当てを解除」ボタンをクリックします。グループを変更したい場合は、「対象の構成を変更」ボタンをクリックしてください。

コンピュータのエージェント設定を解除する場合は、画面下部で対象のコンピュータを選択して「割り当てを解除」ボタンをクリックします。

4. 表示されるダイアログで、「OK」ボタンをクリックします。

グループのエージェント設定を解除する場合は、選択したグループに含まれるグループのエージェント設定も解除するかどうか設定できます。

グループまたはコンピュータのエージェント設定の割り当てが解除されます。エージェント設定の割り当てを解除すると、デフォルトエージェント設定になります。なお、デフォルトエージェント設定は解除できません。

ポイント

エージェント設定の割り当てには、「直接」または「間接」があります。グループを選択してエージェント設定を割り当てた場合、選択したグループには「直接」で割り当てられます。選択したグループの下位にあるグループとコンピュータには、「間接」で割り当てられます。ただし、下位のグループまたはコンピュータに「直接」で割り当てられている場合、そのグループまたはコンピュータには割り当てられません（「直接」が優先されます）。

関連リンク

- [15.1.2 エージェント設定を追加する手順](#)
- [15.1.3 エージェント設定を編集する手順](#)
- [15.1.5 エージェント設定を削除する手順](#)

15.1.7 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。

ポイント

情報を効率良く収集・更新するためには、エージェントレスの機器 1,000 台ごとに 1 時間の間隔を設定してください。例えば、エージェントレスの機器が 800 台ある場合は、1 時間ごとに更新されるように設定します。

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

JP1/IT Desktop Management 2 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。

15.2 機器の探索の設定

Active Directory の探索やネットワークの探索の設定をカスタマイズできます。また、設定した条件で探索を即時実行できます。

Active Directory の探索条件の設定については、「[15.2.2 探索条件を設定する手順（Active Directory の探索）](#)」を参照してください。

ネットワークの探索条件の設定については、「[15.2.1 探索条件を設定する手順（ネットワークの探索）](#)」を参照してください。

15.2.1 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 JP1/IT Desktop Management 2 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

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

15.2.2 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 JP1/IT Desktop Management 2 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。

JP1/IT Desktop Management 2 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

- [15.2.4 機器の探索状況の確認](#)

15.2.3 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。

15.2.4 機器の探索状況の確認

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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

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

15.2.5 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。

15.2.6 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

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

15.2.7 管理対象の機器を確認する手順

JP1/IT Desktop Management 2 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

- [15.2.8 除外対象の機器を確認する手順](#)

15.2.8 除外対象の機器を確認する手順

JP1/IT Desktop Management 2 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

- [15.2.7 管理対象の機器を確認する手順](#)

15.3 セキュリティ管理の設定

管理対象のコンピュータのセキュリティ状態を判定するスケジュールを変更できます。また、操作ログの自動取り込みとエクスポートに関する設定もできます。

関連リンク

- [15.3.1 セキュリティ判定のスケジュールを変更する手順](#)

15.3.1 セキュリティ判定のスケジュールを変更する手順

コンピュータのセキュリティ状態を判定する時刻と間隔を変更できます。ここで設定したスケジュールに従って、セキュリティ画面やレポートの情報が更新されます。

セキュリティ判定のスケジュールを変更するには：

1. 設定画面を表示します。
2. メニューエリアで [セキュリティ管理] - [セキュリティのスケジュール設定] を選択します。
3. インフォメーションエリアで、[実施時刻] と [実施間隔 (日)] を設定します。
4. [適用] ボタンをクリックします。

設定したスケジュールに従って、管理対象のコンピュータのセキュリティ状態が判定されます。

ポイント

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自動的にサポートサービスサイトからダウンロードするように設定している場合、最新情報で判定するために、サポートサービスの情報を更新してから判定するようにスケジュールを設定することをお勧めします。

関連リンク

- [15.8.3 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](#)

15.3.2 操作ログを自動的に取り込む手順

操作ログを自動的に取り込むように設定できます。

操作ログを自動的に取り込むには：

1. 設定画面を表示します。

2. メニューエリアで [セキュリティ管理] – [操作ログの設定] を選択します。
3. インフォメーションエリアで、[操作ログの自動取り込み] を設定します。
4. [適用] ボタンをクリックします。

設定した内容に従って、操作ログが自動的に取り込まれます。

関連リンク

- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [10.7.2 コンピュータを選択して操作ログを取り込む手順](#)

15.3.3 操作ログを定期的にエクスポートする手順

操作ログを定期的に CSV ファイル形式でエクスポートするように設定できます。

操作ログを定期的にエクスポートするには：

1. 設定画面を表示します。
2. メニューエリアで [セキュリティ管理] – [操作ログの設定] を選択します。
3. インフォメーションエリアで、[操作ログのエクスポート] を設定します。
4. [適用] ボタンをクリックします。

設定した内容に従って、操作ログが定期的にエクスポートされます。

ポイント

エクスポートされた操作ログは、セットアップの [操作ログの設定] 画面で設定した、操作ログの保管先フォルダ配下の export フォルダに格納されます。

関連リンク

- [10.7.1 管理用サーバに過去の操作ログを取り込む手順](#)
- [10.7.2 コンピュータを選択して操作ログを取り込む手順](#)
- [付録 A.4 エクスポートした操作ログの出力形式](#)

15.4 資産管理の設定

資産管理で使用する管理項目を追加したり、各項目の情報の入力方法を変更したりできます。

また、契約情報を管理するときに使用する、契約会社のリストを設定できます。

関連リンク

- [15.4.1 資産管理項目を追加する手順](#)
- [15.4.8 契約会社情報の管理](#)

15.4.1 資産管理項目を追加する手順

手もとに機器の管理台帳がある場合に、JP1/IT Desktop Management 2 では用意されていない項目を、独自の資産管理項目として追加できます。

資産管理項目を追加するには：

1. 設定画面の「資産管理項目の設定」画面を表示します。
2. 項目を追加したいカテゴリの「項目を追加」ボタンをクリックします。
3. 表示されるダイアログで、項目名や情報の入力方法を設定します。

設定した資産管理項目が追加されます。追加された項目は、資産画面に表示できます。

15.4.2 資産管理項目の入力方法やデータ型を変更する手順

資産管理項目の入力方法を変更できます。

例えば、一部の情報をコンピュータの利用者に入力してもらうように設定すると、管理者が情報をメンテナンスする手間を省けます。

資産管理項目の入力方法を変更するには：

1. 設定画面の「資産管理項目の設定」画面を表示します。
2. 入力方法を変更したい項目の「編集」ボタンをクリックします。
入力方法やデータ型は、項目を新規追加するときに設定することもできます。
3. 表示されるダイアログで、入力方法を編集します。

入力方法が変更されます。

ポイント

〔部署〕または〔設置場所〕のデータ型を階層型にした場合は、階層構成を編集できます。ここで編集した階層構成は、資産画面や機器画面などのメニューエリアに反映されます。

ポイント

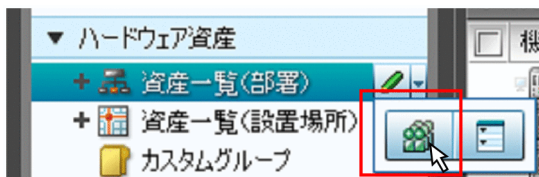
〔部署〕または〔設置場所〕のデータ型は変更できます。それ以外の追加した資産管理項目は、一度設定したデータ型をほかのデータ型に変更できません。

15.4.3 部署・設置場所の定義を追加する手順

管理する部署や設置場所が増えた場合、部署・設置場所の定義を追加できます。定義を追加すると、追加した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を追加するには：

1. 資産画面を表示します。
2. メニューエリアの〔ハードウェア資産〕で、〔資産一覧（部署）〕または〔資産一覧（設置場所）〕を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の〔資産管理〕－〔資産管理項目の設定〕を選択して表示される画面で、〔資産情報と機器情報の共通管理項目〕の〔部署〕または〔設置場所〕の〔編集〕ボタンをクリックしても追加できます。

3. 表示されるダイアログで〔データ型〕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部署・設置場所を追加します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が追加されて、資産画面や機器画面などのメニューエリアに追加したグループが表示されます。

関連リンク

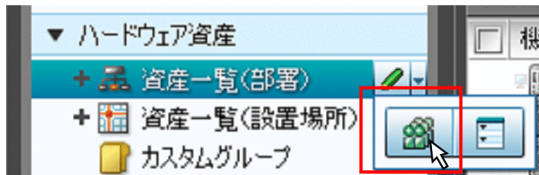
- 6.29 部署・設置場所の定義を編集する手順
- 6.30 部署・設置場所の定義を削除する手順

15.4.4 部署・設置場所の定義を編集する手順

管理する部署が統合されたり設置場所の名称が変更になったりした場合、部署・設置場所の定義を編集できます。定義を編集すると、編集した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を編集するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】を選択し、表示されるアイコンをクリックします。



ポイント

設定画面の【資産管理】－【資産管理項目の設定】を選択して表示される画面で、【資産情報と機器情報の共通管理項目】の【部署】または【設置場所】の【編集】ボタンをクリックしても編集できます。

3. 表示されるダイアログで【データ型】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部署・設置場所の名称や階層を編集します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が編集されて、資産画面や機器画面などのメニューエリアに編集したグループが表示されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除しま

す。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が変更されると、資産画面の「ソフトウェアライセンス」－「ソフトウェアライセンス一覧」、[ソフトウェアライセンス状況]－「ソフトウェアライセンス状況一覧」および資産画面の「契約」－「契約一覧」に表示される部署の情報も変更されます。

関連リンク

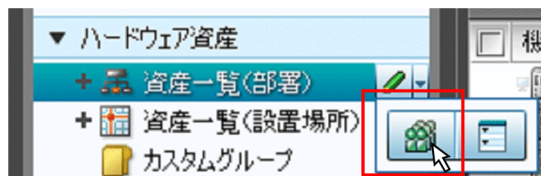
- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)

15.4.5 部署・設置場所の定義を削除する手順

管理していた部署や設置場所を管理しなくなった場合、部署・設置場所の定義を削除できます。定義を削除すると、削除した部署・設置場所が、資産画面や機器画面などのメニューエリアに反映されます。

部署・設置場所の定義を削除するには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」で、「資産一覧（部署）」または「資産一覧（設置場所）」を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで「データ型」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部署・設置場所の定義を削除します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

部署・設置場所の定義が削除されます。

定義が削除されても、各機器の利用者情報（実態）は変更されません。このため、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。実態と定義を一致させるためには、部署・設置場所の定義を編集したあとで、利用者情報を定義に合わせて更新してください。利用者情報を更新したら、メニューエリアの表示を定義に合わせるために、旧体制で使われていた階層だけを削除しま

す。旧体制で使われていた階層だけを削除する手順については、「[6.31 旧体制で使われていた階層だけを削除する手順](#)」を参照してください。

ポイント

部署の定義が削除されると、資産画面の次の画面に表示されていた該当する部署の情報は、「不明」と表示されます。

- [ソフトウェアライセンス] – [ソフトウェアライセンス一覧] 画面
- [ソフトウェアライセンス状況] – [ソフトウェアライセンス状況一覧] 画面
- [契約] – [契約一覧] 画面

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)

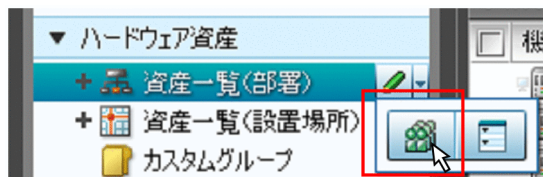
15.4.6 言語ごとの部署・設置場所の表示名を設定する手順

利用者のコンピュータの言語に応じた、部署・設置場所の表示名を設定できます。複数言語の OS を利用している環境で、部署を・設置場所を管理する場合に便利です。

なお、言語ごとの部署・設置場所の表示名を設定するには、部署・設置場所の入力方法が「[利用者が入力](#)」になっている必要があります。

言語ごとの部署・設置場所の表示名を設定するには：

1. 資産画面を表示します。
2. メニューエリアの「ハードウェア資産」で、「資産一覧（部署）」または「資産一覧（設置場所）」を選択し、表示されるアイコンをクリックします。



3. 「他言語の設定へ」のリンクをクリックします。
4. 表示されるダイアログで、言語ごとに表示名を設定します。
5. [OK] ボタンをクリックします。
6. [OK] ボタンをクリックします。

他言語環境での部署・設置場所の表示名が設定されます。

関連リンク

- [6.28 部署・設置場所の定義を追加する手順](#)
- [6.29 部署・設置場所の定義を編集する手順](#)
- [6.30 部署・設置場所の定義を削除する手順](#)
- [6.32 部署・設置場所の名称を変更する手順](#)
- [6.33 部署・設置場所を削除する手順](#)

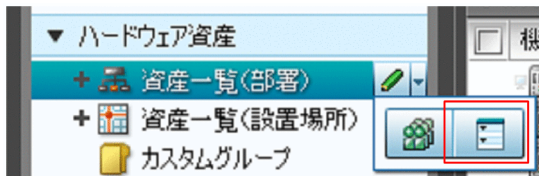
15.4.7 旧体制で使われていた階層だけを削除する手順

職制変更に伴い設定画面で部署・設置場所の階層（定義）を削除しても、資産画面や機器画面などのメニューエリアには、削除した階層が表示されたままになります。メニューエリアの表示を定義に合わせるためには、旧体制で使われていた階層だけを削除する必要があります。メニューエリアの階層は、資産画面、機器画面およびセキュリティ画面のメニューエリアから表示できるダイアログで削除できます。

資産画面で削除する場合を例に、手順を次に示します。

旧体制で使われていた階層だけを削除するには：

1. 資産画面を表示します。
2. メニューエリアの【ハードウェア資産】で、【資産一覧（部署）】または【資産一覧（設置場所）】を選択し、表示されるアイコンをクリックします。



3. 表示されるダイアログで、削除したい階層を選択します。
4. 【削除】 ボタンをクリックします。
5. 表示されるダイアログで、【OK】 ボタンをクリックします。
6. 【閉じる】 ボタンをクリックします。

旧体制で使われていた階層だけが削除されて、資産画面や機器画面のメニューエリアの表示が定義と一致します。

15.4.8 契約会社情報の管理

組織内の契約情報を JP1/IT Desktop Management 2 で管理するとき、保守契約などの契約を結んでいる契約会社情報を登録して管理できます。この契約会社情報の一覧を契約会社リストと呼びます。契約会社リストは、設定画面の [資産管理] - [契約会社リストの設定] で管理します。

契約会社情報を管理すると、契約情報に契約会社の情報を設定できるため、契約情報からすぐに会社の所在地や契約の担当者、連絡先などを確認できます。さらに、契約情報をハードウェア資産情報やソフトウェアライセンス情報と関連づけると、資産画面のそれぞれの [契約情報] タブから、対応する契約会社の情報を確認できます。

契約会社情報を契約会社リストに追加する方法については、「[15.4.9 契約会社情報を追加する手順](#)」を参照してください。

契約会社の所在地や担当者の変更に伴って契約会社情報を更新する場合、契約会社情報を編集します。契約会社情報を編集する方法については、「[15.4.10 契約会社情報を編集する手順](#)」を参照してください。

複数の契約会社情報を編集する場合、契約会社リストをエクスポートしたあとで、編集してからインポートすることで一括更新できます。契約会社リストをエクスポートする方法については、「[15.4.12 契約会社リストをエクスポートする手順](#)」を参照してください。また、契約会社リストをインポートする方法については、「[11.4.5 契約会社リストをインポートする手順](#)」を参照してください。

契約を解除する場合、不要になった契約会社情報を削除します。契約会社情報を削除する方法については、「[15.4.11 契約会社情報を削除する手順](#)」を参照してください。

関連リンク

- [1.11 資産に関する契約を管理する流れ](#)

15.4.9 契約会社情報を追加する手順

設定画面の [資産管理] - [契約会社リストの設定] 画面の契約会社リストに、契約会社情報を追加できます。契約会社情報を追加すると、資産画面の [契約] 画面で、契約情報に契約会社名を設定できます。契約情報に契約会社情報へのリンクができるので、すぐに会社の所在地や契約の担当者、連絡先などを確認できて便利です。

契約会社情報を追加するには：

1. 設定画面を表示します。
2. メニューエリアで [資産管理] - [契約会社リストの設定] を選択します。
3. インフォメーションエリアで [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契約会社の情報を入力して、[OK] ボタンをクリックします。

契約会社情報が追加され、契約会社リストに表示されます。

関連リンク

- [15.4.10 契約会社情報を編集する手順](#)
- [15.4.11 契約会社情報を削除する手順](#)
- [11.4.5 契約会社リストをインポートする手順](#)
- [15.4.12 契約会社リストをエクスポートする手順](#)

15.4.10 契約会社情報を編集する手順

契約会社の所在地や担当者、連絡先などを変更したい場合、契約会社情報を編集できます。

契約会社情報を編集するには：

1. 設定画面を表示します。
2. メニューエリアで「資産管理」－「契約会社リストの設定」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契約会社情報の「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契約会社情報を編集して、「OK」ボタンをクリックします。

契約会社情報が更新されます。

ポイント

複数の契約会社情報を編集する場合、契約会社リストをエクスポートしたあとで、編集してからインポートすることで一括更新できます。

関連リンク

- [15.4.9 契約会社情報を追加する手順](#)
- [15.4.11 契約会社情報を削除する手順](#)
- [11.4.5 契約会社リストをインポートする手順](#)
- [15.4.12 契約会社リストをエクスポートする手順](#)

15.4.11 契約会社情報を削除する手順

契約を解除して利用しなくなった契約会社情報を、契約会社リストから削除できます。

契約会社情報が契約情報で設定されている場合は、削除できません。あらかじめ契約情報を編集して、契約会社名に該当の契約会社情報が設定されないようにしてください。契約情報の編集方法については、「[11.3.2 契約情報を編集する手順](#)」を参照してください。

契約会社情報を削除するには：

1. 設定画面を表示します。
2. メニューエリアで「資産管理」－「契約会社リストの設定」を選択します。
3. インフォメーションエリアで削除したい契約会社情報を選択して、「削除」ボタンをクリックします。
複数の契約会社情報を選択して一括削除することもできます。
4. 表示されるダイアログで、「OK」ボタンをクリックします。

選択した契約会社情報が削除されます。

関連リンク

- [15.4.9 契約会社情報を追加する手順](#)
- [15.4.10 契約会社情報を編集する手順](#)
- [11.4.5 契約会社リストをインポートする手順](#)
- [15.4.12 契約会社リストをエクスポートする手順](#)

15.4.12 契約会社リストをエクスポートする手順

契約会社リストを CSV ファイルにエクスポート（一括出力）できます。

契約会社リストをエクスポートするには：

1. 設定画面を表示します。
2. メニューエリアで「資産管理」－「契約会社リストの設定」を選択します。
3. 「操作メニュー」の「契約会社一覧をエクスポートする」を選択します。
4. 「エクスポートする項目の選択」ダイアログで、エクスポートする項目をチェックして、「OK」ボタンをクリックします。
エクスポートされる CSV ファイルの文字コードを指定する場合は、「文字エンコーディング」を変更してください。デフォルトでは文字コードは「UTF-8」になります。
5. 表示された画面の「保存」ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

関連リンク

- [15.4.9 契約会社情報を追加する手順](#)
- [15.4.10 契約会社情報を編集する手順](#)
- [15.4.11 契約会社情報を削除する手順](#)

15.5 機器管理の設定

Windows の [プログラムと機能] に登録されていないソフトウェアの情報を収集するための、ソフトウェア検索条件を設定できます。

また、コンピュータの電源を制御するための AMT の設定ができます。

関連リンク

- [15.5.6 AMT の認証情報を設定する手順](#)

15.5.1 ソフトウェア検索条件を追加する手順

設定画面の [機器] - [ソフトウェア検索条件の設定] 画面の一覧に、ソフトウェア検索条件を追加できます。ソフトウェア検索条件を追加すると、管理対象のコンピュータで検索条件に一致したソフトウェアの情報をインストールソフトウェア情報として取得できます。取得したインストールソフトウェア情報は、セキュリティポリシーで使用必須ソフトウェアまたは使用禁止ソフトウェアとして設定すると、導入状況を監視できるようになります。

ソフトウェア検索条件を追加するには：

1. 設定画面を表示します。
2. メニューエリアで [機器] - [ソフトウェア検索条件の設定] を選択します。
3. インフォメーションエリアで [ソフトウェア検索条件を追加] ボタンをクリックします。
4. 表示されるダイアログで検索条件を入力して、[OK] ボタンをクリックします。
5. [適用] ボタンをクリックします。

ソフトウェア検索条件が追加されます。

関連リンク

- [15.5.2 ソフトウェア検索条件を編集する手順](#)
- [15.5.3 ソフトウェア検索条件を削除する手順](#)
- [15.5.4 ソフトウェア検索条件をインポートする手順](#)
- [15.5.5 ソフトウェア検索条件をエクスポートする手順](#)

15.5.2 ソフトウェア検索条件を編集する手順

ソフトウェア検索条件を編集できます。ソフトウェア名や検索に用いるファイル名を変更したい場合に編集します。

ソフトウェア検索条件を編集するには：

1. 設定画面を表示します。
2. メニューエリアで [機器] - [ソフトウェア検索条件の設定] 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ソフトウェア検索条件の [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ソフトウェア検索条件を編集して、[OK] ボタンをクリックします。

選択したソフトウェア検索条件が更新されます。

関連リンク

- [15.5.1 ソフトウェア検索条件を追加する手順](#)
- [15.5.3 ソフトウェア検索条件を削除する手順](#)
- [15.5.4 ソフトウェア検索条件をインポートする手順](#)
- [15.5.5 ソフトウェア検索条件をエクスポートする手順](#)

15.5.3 ソフトウェア検索条件を削除する手順

利用しなくなったソフトウェア検索条件を削除できます。

ソフトウェア検索条件を削除するには：

1. 設定画面を表示します。
2. メニューエリアで [機器] - [ソフトウェア検索条件の設定] を選択します。
3. インフォメーションエリアで削除したいソフトウェア検索条件を選択して、[削除] ボタンをクリックします。
複数のソフトウェア検索条件を選択して一括削除することもできます。
4. 表示されるダイアログで、[OK] ボタンをクリックします。

選択したソフトウェア検索条件が削除されます。

関連リンク

- [15.5.1 ソフトウェア検索条件を追加する手順](#)
- [15.5.2 ソフトウェア検索条件を編集する手順](#)
- [15.5.4 ソフトウェア検索条件をインポートする手順](#)
- [15.5.5 ソフトウェア検索条件をエクスポートする手順](#)

15.5.4 ソフトウェア検索条件をインポートする手順

CSV ファイルのソフトウェア検索条件をインポートして、一括でソフトウェア検索条件を追加できます。

ソフトウェア検索条件をインポートするには：

1. 設定画面を表示します。
2. メニューエリアで [機器] - [ソフトウェア検索条件の設定] を選択します。
3. インフォメーションエリアで [操作メニュー] の [ソフトウェア検索条件一覧をインポートする] を選択します。
4. [ソフトウェア検索条件のインポート] ダイアログで、インポートしたい CSV ファイルを指定します。
インポートする CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトでは文字コードは「UTF-8」になります。
この画面から CSV ファイルのサンプルをダウンロードできます。CSV ファイルを作成するときに参考にしてください。
5. [OK] ボタンをクリックします。

CSV ファイルのデータがインポートされます。インポートされた情報が意図したとおりに登録されているか確認してください。正しく反映されなかったレコードがある場合は、CSV ファイルを修正して再度インポートしてください。

関連リンク

- [15.5.1 ソフトウェア検索条件を追加する手順](#)
- [15.5.2 ソフトウェア検索条件を編集する手順](#)
- [15.5.3 ソフトウェア検索条件を削除する手順](#)
- [15.5.5 ソフトウェア検索条件をエクスポートする手順](#)

15.5.5 ソフトウェア検索条件をエクスポートする手順

ソフトウェア検索条件を CSV ファイルにエクスポート（一括出力）できます。

ソフトウェア検索条件をエクスポートするには：

1. 設定画面を表示します。
2. メニューエリアで [機器] - [ソフトウェア検索条件の設定] を選択します。
3. [操作メニュー] の [ソフトウェア検索条件一覧をエクスポートする] を選択します。

4. [エクスポートする項目の選択] ダイアログで、エクスポートする項目をチェックして、[OK] ボタンをクリックします。

エクスポートされる CSV ファイルの文字コードを指定する場合は、[文字エンコーディング] を変更してください。デフォルトでは文字コードは「UTF-8」になります。

5. 表示された画面の [保存] ボタンをクリックします。

ダウンロード先に、指定したファイル名で CSV ファイルが保存されます。

関連リンク

- [15.5.1 ソフトウェア検索条件を追加する手順](#)
- [15.5.2 ソフトウェア検索条件を編集する手順](#)
- [15.5.3 ソフトウェア検索条件を削除する手順](#)
- [15.5.4 ソフトウェア検索条件をインポートする手順](#)

15.5.6 AMT の認証情報を設定する手順

AMT を利用してコンピュータの電源を制御する場合、および AMT ファームウェアバージョンの情報を取得する場合は、AMT の認証情報を設定しておく必要があります。

また、エージェント設定からコンピュータの AMT を設定する場合、AMT を自動的に有効化するための管理者権限のパスワードを設定する必要があります。

AMT の認証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 [機器] - [AMT の設定] を選択します。
3. AMT の認証情報を設定します。

AMT を利用してコンピュータの電源を制御する場合、および AMT ファームウェアバージョンの情報を取得する場合は、インフォメーションエリアで [ユーザー ID]、[パスワード] および [パスワード確認] を入力します。

コンピュータの AMT を自動的に有効化する場合は、[管理者権限のパスワード] の [パスワード] および [パスワード確認] に AMT の管理者権限のパスワードを入力します。

4. [適用] ボタンをクリックします。

利用者のコンピュータに対して、AMT を利用して電源を制御できるようになります。

なお、AMT を利用するためには、JP1/IT Desktop Management 2 での設定以外に、管理用サーバと利用者のコンピュータで AMT 自体の設定が必要です。

注意事項

〔認証情報〕に設定した AMT のユーザー情報（AMT 管理ユーザー）のユーザー名とパスワードは、管理用サーバの設定と、管理対象のコンピュータで一致させる必要があります。

ポイント

エージェント導入済みのコンピュータの場合、エージェント設定から AMT の設定ができます。これによって、各コンピュータの BIOS を操作する手間を軽減できます。

ポイント

コンピュータの AMT に管理者権限のパスワードが未設定の場合は、〔管理者権限のパスワード〕に設定したパスワードが AMT に登録されます。管理者権限のパスワードが登録済みの場合、パスワードは設定できません。登録済みのパスワードを指定してください。また、管理者権限のパスワードが設定済みでかつ AMT が無効になっているときは、あらかじめコンピュータの AMT を有効にしておく必要があります。

関連リンク

- ・ [6.23 コンピュータの電源を制御する手順](#)

15.5.7 機器の変更履歴の取得を設定する手順

機器情報に変更があった場合、その変更を変更履歴として取得するよう設定できます。

変更履歴の取得設定をするには：

1. 設定画面を表示します。
2. メニューエリアで〔機器〕－〔変更履歴の設定〕を選択します。
3. 〔変更履歴を取得する〕をチェックします。
4. 〔変更履歴の取得対象〕から、変更履歴を取得する機器情報をチェックします。
ここでチェックした機器情報の変更履歴だけを取得します。
5. 〔適用〕 ボタンをクリックします。

変更履歴を取得できるようになります。変更履歴は機器画面の〔変更履歴〕画面で確認できます。また、セットアップで保存用の変更履歴の出力設定をすると、取得した変更履歴を保存用の変更履歴としてファイル出力できます。

15.6 レポートの設定

各レポートを保存しておく期間と、レポートを集計するときの起点となる月や曜日などを変更できます。

また、日刊、週刊、および月刊のダイジェストレポートの送付先を設定できます。

関連リンク

- [15.6.1 レポートの保存期間と開始日を変更する手順](#)
- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)

15.6.1 レポートの保存期間と開始日を変更する手順

各レポートを保存しておく期間と、レポートを集計するときの起点となる開始日を変更できます。

レポートを保存しておくことで、過去にさかのぼってレポートを参照できます。なお、保存期間が過ぎると、集計データが自動的に削除されてレポートを参照できなくなります。

レポートの保存期間と開始日を変更するには：

1. 設定画面を表示します。
2. メニューエリアで [レポート] - [保存期間と開始日の設定] を選択します。
3. インフォメーションエリアで、レポートを保存したい期間を選択します。
4. レポートを集計するときの起点となる曜日、日、月を選択します。
5. [適用] ボタンをクリックします。

レポートの保存期間と開始日が変わります。

ポイント

デフォルトでは、レポートの保存期間は [5 年]、週の始めは [月曜日]、月の始めは [1]、年度の始めは [4 月] です。

15.6.2 ダイジェストレポートの送付先を設定する手順

日刊、週刊、および月刊のダイジェストレポートの送付先を設定できます。

指定したメールアドレスに対して、ダイジェストレポートが作成されたタイミングでレポートの内容が通知されるようになります。これによって、JP1/IT Desktop Management 2 を操作しなくても、メールの内容から管理状況を把握できるようになります。

ダイジェストレポートの送付先を設定するには：

1. 設定画面を表示します。
2. メニューエリアで [レポート] - [ダイジェストレポートの設定] を選択します。
3. インフォメーションエリアで、ダイジェストレポートを送付するユーザー ID にチェックします。
4. [適用] ボタンをクリックします。

ダイジェストレポートの送付先が設定されます。

ポイント

ユーザー ID をチェックすると、メールアドレスを編集できます。メールアドレスが設定されていない場合はメールアドレスを入力することもできます。なお、ここで設定したメールアドレスは設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面のユーザーアカウントにも反映されます。

ポイント

送付先のユーザー ID には、そのユーザー ID に設定されている業務分掌に関係なく、すべて同じ内容のダイジェストレポートが送付されます。

関連リンク

- [15.8.1 メールサーバを設定する手順](#)
- [4. ユーザーアカウントを管理する](#)

15.7 イベントの設定

関連リンク

- 15.7.1 イベント通知の設定をする手順

15.7.1 イベント通知の設定をする手順

特定のイベントが発生したときに、イベントの発生をメールで通知するように設定できます。

イベント通知の設定をするには：

1. 設定画面を表示します。
2. メニューエリアで [イベント] - [イベント通知の設定] を選択します。
3. 「メールで受け取りたいイベントの、重大度と種類を設定してください。」で、メールで通知したいイベントのカテゴリをチェックします。
4. 「メールの通知先を選択してください。」で、イベントを通知するユーザー ID をチェックします。
ユーザー ID をチェックすると、対応するメールアドレスを編集できます。

通知対象のイベントと、通知先が設定されます。

なお、特定のイベントを通知の対象外にしたい場合は、「通知の対象外とするイベントを選択してください。」で、[追加] ボタンをクリックしてください。[通知の対象外とするイベントの追加] ダイアログで、メール通知しないイベントを指定できます。

ポイント

ユーザー ID をチェックすると、メールアドレスを編集できます。メールアドレスが設定されていない場合はメールアドレスを入力することもできます。なお、ここで設定したメールアドレスは設定画面の [ユーザー管理] - [ユーザーアカウントの管理] 画面のユーザーアカウントにも反映されます。

ポイント

通知対象に設定したイベントは、通知先のユーザー ID に設定した業務分掌に関係なくすべて通知されます。ただし、イベント通知のメールに記載された URL については、通知先のユーザー ID に URL のリンク先の業務分掌を設定してある場合にだけ参照できます。リンク先の業務分掌を設定していないユーザー ID の場合、リンクをクリックすると自動的にホーム画面に移動します。

関連リンク

- 15.8.1 メールサーバを設定する手順
- 4. ユーザーアカウントを管理する

15.8 他システムとの接続情報の設定

JP1/IT Desktop Management 2 がほかのシステムと接続するための次の接続情報を設定できます。

- JP1/IT Desktop Management 2 がメール通知するときに使用するメールサーバの情報
- 探索対象とする Active Directory のドメイン情報
- 最新の更新プログラム情報を取得するサポートサービスサイトへの接続情報
- スマートデバイスを管理するために必要な、MDM システムとの接続情報

関連リンク

- [15.8.1 メールサーバを設定する手順](#)
- [15.8.2 Active Directory と接続するための情報を設定する手順](#)
- [15.8.3 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](#)
- [15.8.4 MDM システムと連携するための情報を設定する手順](#)

15.8.1 メールサーバを設定する手順

探索の完了、ダイジェストレポートの作成、イベントの発生などのメールを受け取るためには、JP1/IT Desktop Management 2 がメール通知するときに使用するメールサーバの情報を設定する必要があります。

メールサーバを設定するには：

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] - [メールサーバの設定] を選択します。
3. インフォメーションエリアで、メールサーバの情報を設定します。
[テストメールを送信] ボタンをクリックすると、設定したメールサーバを使用してテストメールを送信できます。メールが正しく送信されるか確認してください。なお、テストメールはログインユーザーのユーザーアカウントに設定されたメールアドレスに送信されます。
4. [適用] ボタンをクリックします。

設定したメールサーバを使用して、メールが送信されるようになります。

ポイント

メール通知を利用すると、JP1/IT Desktop Management 2 の操作画面を頻繁に確認しなくても、管理状況を把握できるようになります。メール通知を利用できるのは次の機能です。

- 探索結果の通知

- ダイジェストレポートの通知
- イベント発生のお知らせ

関連リンク

- [15.2.1 探索条件を設定する手順（ネットワークの探索）](#)
- [15.2.2 探索条件を設定する手順（Active Directory の探索）](#)
- [15.6.2 ダイジェストレポートの送付先を設定する手順](#)
- [15.7.1 イベント通知の設定をする手順](#)

15.8.2 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 JP1/IT Desktop Management 2 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、部署の情報を反映する」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

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

15.8.3 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、最新の更新プログラム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、updatesupportinfo コマンドを利用して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

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

15.8.4 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 JP1/IT Desktop Management 2 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、JP1/IT Desktop Management 2 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 製品または MDM サービスのサーバ証明書入手します。

1. Web ブラウザで MDM 製品または MDM サービス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。

JP1/IT Desktop Management 2 - Manager のインストール先フォルダ¥mgr¥uCPSB¥jdk¥jre¥bin¥keytool.exe -import -keystore JP1/IT Desktop Management 2 - Manager 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. JP1/IT Desktop Management 2 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。

なお、MobileIron と連携する場合、[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。

また、JP1 スマートデバイス管理サービスと連携する場合、[MDM 連携の設定] で指定するユーザー ID は管理者権限を持つユーザー ID を指定する必要があります。

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かった場合、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

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

16

データベースを管理する

ここでは、データベースマネージャを使ってデータベースを管理する方法について説明します。

16.1 データベースマネージャを起動する手順

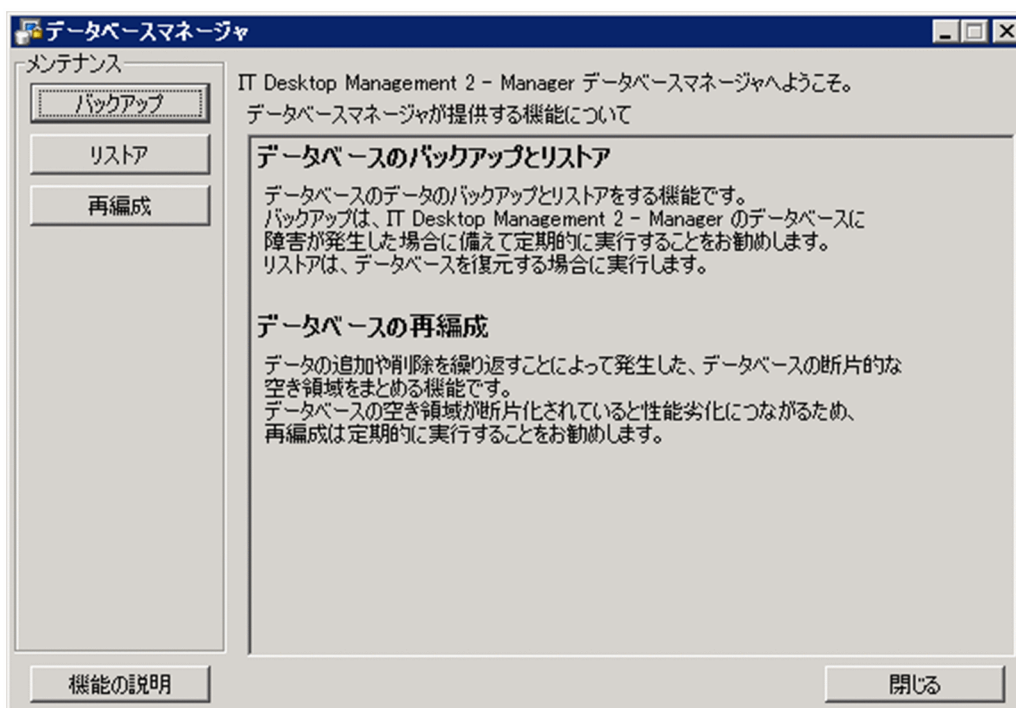
データベースマネージャは管理用サーバから起動できます。

なお、データベースマネージャは、JP1_ITDM2_DB Service のサービスが起動しているときだけ実行できます。

データベースマネージャを起動するには：

1. Administrator 権限を持つユーザーで OS 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] - [JP1_IT Desktop Management 2 - Manager] - [ツール] - [データベースマネージャ] を選択します。

データベースマネージャが起動して、機能説明の画面が表示されます。



3. ダイアログの左側の [メンテナンス] から、実行したい機能のボタンをクリックします。

選択した機能に応じた画面が表示されます。

[機能の説明] ボタンをクリックすると、データベースマネージャの初期画面に戻ります。

注意事項

[機能の説明] ボタンをクリックして初期画面を表示した場合、それまで設定した内容はクリアされます。

[閉じる] ボタンをクリックすると、データベースマネージャを終了します。

関連リンク

- [16.2 データベースをバックアップする](#)
- [16.3 データベースをリストアする](#)
- [16.4 データベースを再編成する](#)

16.2 データベースをバックアップする

データベースマネージャを使用して、データベースをバックアップする手順について説明します。

ポイント

データベースをバックアップするためには、管理用サーバを停止する必要があります。このため、管理用サーバを使用しない曜日、時間などを考慮して実施してください。

ポイント

データベースのバックアップに掛かる時間は、ディスク性能に依存します。進捗状況は、処理中を示すダイアログに経過時間が表示されるので、この時間を目安にしてください。

注意事項

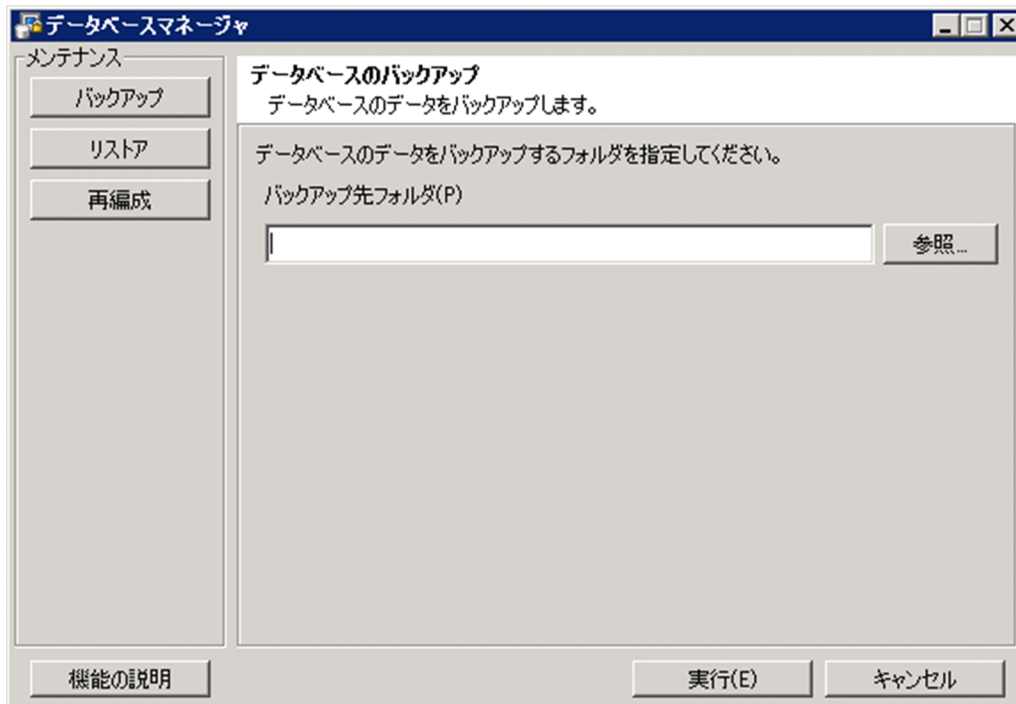
コンピュータが Windows 8.1、Windows 8 および Windows Server 2012 の場合、[バックアップ先フォルダ] に次のフォルダを指定しないでください。

- 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

1. データベースマネージャの [メンテナンス] にある [バックアップ] ボタンをクリックします。

2. [データベースのバックアップ] 画面でバックアップファイルを格納するフォルダを指定します。

[バックアップ先フォルダ] にバックアップファイルの格納先を指定します。ローカルドライブ上のフォルダを指定してください。バックアップファイルの容量は運用内容や JP1/IT Desktop Management 2 の利用期間によって異なります。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。



注意事項

【バックアップ先フォルダ】にネットワークドライブ上のフォルダを指定すると、バックアップに失敗します。

以前にデータベースをバックアップした場合、前回指定したバックアップファイルの格納先が表示されます。なお、格納先に同名のバックアップファイルが存在する場合は、上書きされます。上書きに失敗しても、前回取得したバックアップファイルはそのまま残ります。

バックアップ先フォルダを直接指定するときは、150 文字以内で半角英数字、半角スペース、および次に示す半角記号を使用してください。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

3. [実行] ボタンをクリックします。

バックアップが完了するまで、進捗状況を示すダイアログが表示されます。

バックアップが完了すると、次に示すファイルが出力されます。

- jdnexport.info
- jdnexportdata.bak
- table.テーブル名.exp.bin

関連リンク

- 16.1 データベースマネージャを起動する手順

16.3 データベースをリストアする

データベースマネージャを使用して、データベースをリストアする手順について説明します。

ポイント

データベースをリストアするためには、管理用サーバを停止する必要があります。このため、管理用サーバを使用しない曜日、時間などを考慮して実施してください。

ポイント

データベースのリストアに掛かる時間は、ディスク性能に依存します。進捗状況は、処理中を示すダイアログに経過時間が表示されるので、この時間を目安にしてください。

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、[バックアップ先フォルダ] に次のフォルダを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

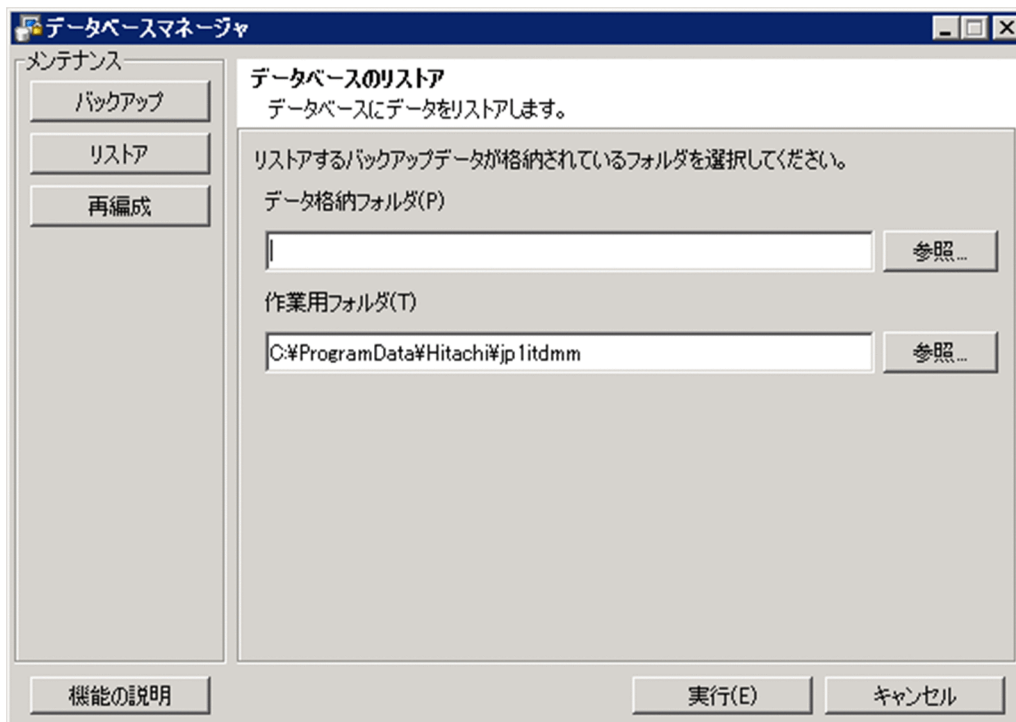
Asset Console を使用している場合は、事前に次の操作を実施してください。

- ・ World Wide Web Publishing Service または World Wide Web Publishing サービスを停止する。
- ・ JP1/IT Desktop Management 2 - Manager からの情報取得コマンド (jamTakeITDM2Info.exe) を実行中のときは、停止する。
- ・ タスク「ITDM2 - Manager 管理情報の取得 (Asset Console)」を Windows のタスクスケジューラに登録しているときは、無効にする。

データベースのリストア完了後に必ず Asset Console で、JP1/IT Desktop Management 2 - Manager の管理情報の取得コマンド (jamTakeITDM2Info.exe) を実行してください。情報取得が完了してから、サービス、コマンドおよびタスクを再開してください。

1. データベースマネージャの [メンテナンス] にある [リストア] ボタンをクリックします。
2. [データベースのリストア] 画面でバックアップファイルが格納されているフォルダを指定します。

[データ格納フォルダ] にバックアップファイルの格納先を指定します。



注意事項

[データ格納フォルダ] にネットワークドライブ上のフォルダを指定すると、リストアに失敗します。

以前にデータベースをバックアップした場合、前回指定したバックアップファイルの格納先が表示されます。

データ格納フォルダを直接指定するときは、150 文字以内で半角英数字、半角スペース、および次に示す半角記号を使用してください。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

3. 作業用フォルダを指定します。

[作業用フォルダ] にデータベースのリストアで使用する作業用フォルダを指定します。

注意事項

[作業用フォルダ] には、10,000 台の機器を管理する場合は 10 ギガバイト以上の空き容量があるローカルドライブ上のフォルダを指定してください。また、ネットワークドライブ上のフォルダを指定すると、リストアに失敗します。

以前にデータベースをリストアした場合、前回指定した作業用フォルダが表示されます。

作業用フォルダを直接指定するときは、150 文字以内で半角英数字、半角スペース、および次に示す半角記号を使用してください。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

デフォルトは、次に示すフォルダが設定されています。

All User プロファイルのアプリケーションデータフォルダ¥Hitachi¥jp¥ltd¥mm

4. [実行] ボタンをクリックします。

リストアが完了するまで、進捗状況を示すダイアログが表示されます。

リストアが完了します。

関連リンク

- [16.1 データベースマネージャを起動する手順](#)

16.4 データベースを再編成する

データベースマネージャを使用して、データベースを再編成する手順について説明します。

ポイント

データベースを再編成するためには、管理用サーバを停止する必要があります。このため、管理用サーバを使用しない曜日、時間などを考慮して実施してください。

ポイント

データベースの再編成に掛かる時間は、ディスク性能に依存します。進捗状況は、処理中を示すダイアログに経過時間が表示されるので、この時間を目安にしてください。

注意事項

コンピュータが Windows 8.1 および Windows 8 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

1. データベースマネージャの [メンテナンス] にある [再編成] ボタンをクリックします。

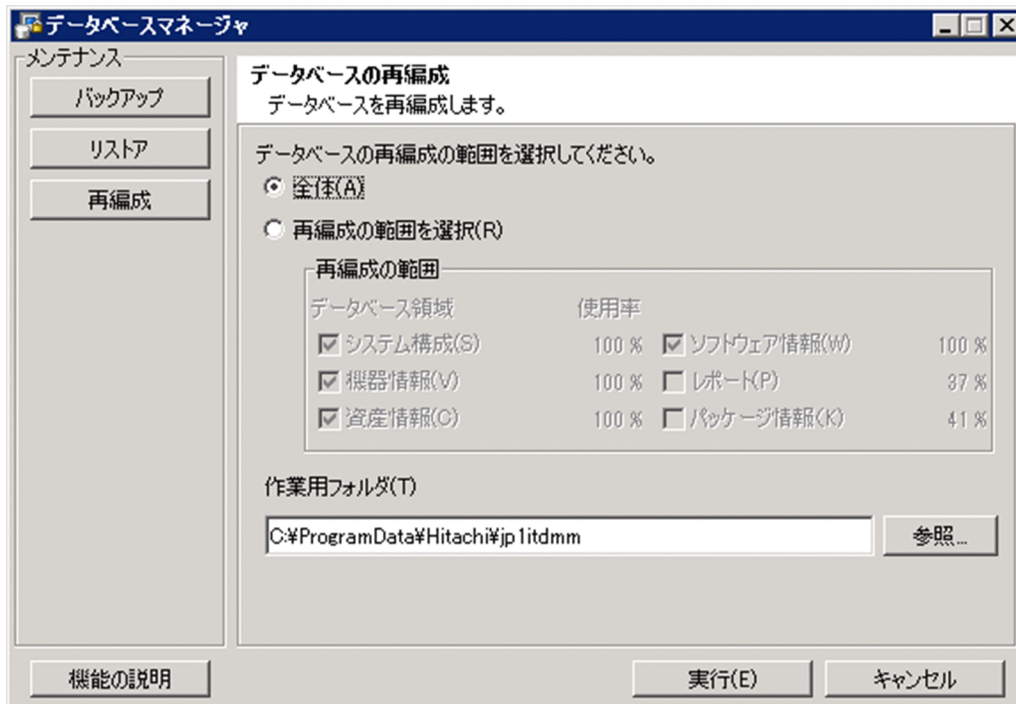
2. [データベースの再編成] 画面で再編成する範囲を選択します。

[全体] を選択した場合

データベースが保持しているすべての情報が再編成の対象になります。

[再編成の範囲を選択] を選択した場合

再編成したい項目をチェックしてください。各項目別にデータベース領域の使用率が表示されます。なお、使用率が 80%以上の項目は、自動的にチェックされます。



3. 作業用フォルダを指定します。

[作業用フォルダ] にデータベースの再編成で使用する作業用フォルダを指定します。

注意事項

[作業用フォルダ] には、10,000 台の機器を管理する場合は 30 ギガバイト以上の空き容量があるローカルドライブ上のフォルダを指定してください。ネットワークドライブ上のフォルダを指定すると、再編成に失敗します。また、クラスタ構成の場合は、共有ディスクのフォルダを指定してください。

以前にデータベースを再編成した場合、前回指定した作業用フォルダが表示されます。

作業用フォルダを直接指定するときは、150 文字以内で半角英数字、半角スペース、および次に示す半角記号を使用してください。

「#」、「(」、「)」、「.」(ピリオド)、「@」、「¥」

デフォルトは、次に示すフォルダが設定されています。

All User プロファイルのアプリケーションデータフォルダ¥Hitachi¥jp1tdmm

4. [実行] ボタンをクリックします。

再編成が完了するまで、進捗状況を示すダイアログが表示されます。

再編成が完了します。

■ ポイント

データベースの再編成は、`reorgdb` コマンドでも実行できます。`reorgdb` コマンドについては、「[17.22 reorgdb \(データベースの再編成\)](#)」を参照してください。

関連リンク

- [16.1 データベースマネージャを起動する手順](#)

17

コマンド

ここでは、JP1/IT Desktop Management 2 のコマンドについて説明します。

17.1 コマンドを実行する手順

JP1/IT Desktop Management 2 のコマンドは、専用のコマンドプロンプト ([JP1ITDM2 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、[JP1ITDM2 Utility Console] を利用すると便利です。
[JP1ITDM2 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。[JP1ITDM2 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、Windows Server 2008、または Windows Vista の場合で、ユーザーアカウント制御 (UAC) が有効なときは、[JP1ITDM2 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] - [JP1_IT Desktop Management 2 - Manager] - [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、JP1/IT Desktop Management 2 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、JP1/IT Desktop Management 2 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
- [JP1ITDM2 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

17.2 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。

17.3 コマンド一覧

JP1/IT Desktop Management 2 で使用できるコマンドの一覧を次の表に示します。

コマンド名	機能	実行できるシステム
ioutils exportasset	ハードウェア資産情報をエクスポートします。	管理用サーバ
ioutils importasset	ハードウェア資産情報をインポートします。	管理用サーバ
ioutils exportfield	追加管理項目の設定をエクスポートします。	管理用サーバ
ioutils importfield	追加管理項目の設定をインポートします。	管理用サーバ
ioutils exporttemplate	資産情報をインポートする際に使用する、項目名の対応づけのテンプレートをエクスポートします。	管理用サーバ
ioutils importtemplate	資産情報をインポートする際に使用する、項目名の対応づけのテンプレートをインポートします。	管理用サーバ
ioutils exportdevice	機器情報をエクスポートします。	管理用サーバ
ioutils exportdevicedetail	詳細な機器情報をエクスポートします。	管理用サーバ
ioutils exportpolicy	セキュリティポリシーの設定をエクスポートします。	管理用サーバ
ioutils importpolicy	セキュリティポリシーの設定をインポートします。	管理用サーバ
ioutils exportupdategroup	更新プログラムグループの設定をエクスポートします。	管理用サーバ
ioutils importupdategroup	更新プログラムグループの設定をインポートします。	管理用サーバ
ioutils exportoplog	管理用サーバに格納されている操作ログをエクスポートします。	管理用サーバ
ioutils exportfilter	フィルタの設定をエクスポートします。	管理用サーバ
ioutils importfilter	フィルタの設定をインポートします。	管理用サーバ
updatesupportinfo	サポートサービスサイトからダウンロードしたサポート情報を登録します。	管理用サーバ
exportdb	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。	管理用サーバ
importdb	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。	管理用サーバ
reorgdb	データベースを再編成します。	管理用サーバ
stopservice	管理用サーバのサービスを停止します。	管理用サーバ
startservice	管理用サーバのサービスを開始します。	管理用サーバ
getlogs	管理用サーバのトラブルシュート用情報を取得します。	- 管理用サーバ - リモートインストールマネージャを導入したコンピュータ
getinstlogs	インストール時のトラブルシュート用情報を取得します。	管理用サーバ

コマンド名	機能	実行できるシステム
getinstlogs	インストール時のトラブルシュート用情報を取得します。	リモートインストールマネージャを導入したコンピュータ
addfwlist.bat	Windows ファイアウォールの例外許可に JP1/IT Desktop Management 2 を設定します。	- 管理用サーバ - リモートインストールマネージャを導入したコンピュータ
resetnid.vbs	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) をリセットします。	エージェント
getinv.vbs	オフライン管理のコンピュータの機器情報を収集します。	エージェント
ioassetsfieldutil export	共通管理項目と追加管理項目の定義をエクスポートします。	管理用サーバ
ioassetsfieldutil import	共通管理項目と追加管理項目の定義をインポートします。	管理用サーバ

17.4 ioutils exportasset (ハードウェア資産情報のエクスポート)

機能

CSV ファイルにハードウェア資産情報をエクスポートします。

資産画面で「-」と表示されている項目は、空の値が出力されます。これは、エクスポートしたデータをそのままインポートした場合に、エラーにならないようにしているためです。なお、エクスポート対象となる情報が 0 件の場合でも、ファイルが出力されます。

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

```
ioutils△exportasset△-export△エクスポートするファイル名 [△-filter△フィルタ名][△-encoding△文字コードの種別][△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする CSV ファイル名を、259 バイト以内の絶対パスで指定します。

-filter△フィルタ名

フィルタを使用してハードウェア資産情報をエクスポートする場合、操作画面のメニューエリアに表示されるフィルタ名を指定します。

-encoding△文字コードの種別

エクスポートするハードウェア資産情報の文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 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

戻り値

ioutils exportasset 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
70	指定されたフィルタが存在しません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

ハードウェア資産情報を C:\temp\hardwareexpo.csv にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportasset -export C:\temp\hardwareexpo.csv -encoding UTF-8 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.5 ioutils importasset (ハードウェア資産情報のインポート)

機能

CSV ファイルを利用してハードウェア資産情報をインポートします。ハードウェア資産情報の項目と CSV ファイルの記述形式については、マニュアル「JP1 Version 10 JP1/IT Desktop Management 2 導入・設計ガイド」を参照してください。

CSV ファイルをインポートすると、ハードウェア資産情報は CSV ファイルに設定された値で更新されます。ただし、CSV ファイルで値が空になっている（ダブルクォーテーション (") だけで値がない）項目は、インポートしても更新されません（空の値には上書きされません）。

ポイント

値にダブルクォーテーション (") で囲んだ半角スペースが設定されている場合は、条件によって値は次のようになります。

- 項目が [部署] または [設置場所] のとき：[不明] に更新される
- 項目のデータ型が [テキスト型] のとき：空白に更新される
- 項目のデータ型が [選択型] または [階層型] のとき：更新されない

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

```
ioutils△importasset△-import△インポートするファイル名△-template△テンプレート名 [△-encoding△文字コードの種別]
```

引数

-import△インポートするファイル名

インポートする CSV ファイル名を、259 バイト以内の絶対パスで指定します。

-template△テンプレート名

インポート時に使用するテンプレート名を指定します。

テンプレートで対応づけが設定されている項目だけがインポートされます。

テンプレートで対応づけが設定されている項目がインポートするファイルに存在しない場合、次のようにインポートされます。

- 存在しない項目は、項目が省略されたと扱われ、インポート後の資産情報の項目に省略時の値が設定されます。なお、インポートによって資産情報が上書きされる場合、省略された項目は上書きされません。
- マッピングキーに対応する列が存在しない場合は、エラーとなりインポートできません。

-encoding△文字コードの種別

インポートするハードウェア資産情報の文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils importasset 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	指定されたフォルダが不正、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
72	指定されたテンプレートが存在しません。
80	インポートするファイルの形式が不正です。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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¥にエクスポート済みのハードウェア資産情報「hardwareexpo.csv」を、「ハードウェア資産情報インポート用」テンプレートを使用してインポートする場合のコマンドの使用例を次に示します。

ioutils importasset -import C:¥temp¥hardwareexpo.csv -template ハードウェア資産情報インポート用 -encoding UTF-8

関連リンク

- [17.1 コマンドを実行する手順](#)

17.6 ioutils exportfield (追加管理項目の設定のエクスポート)

機能

XML ファイルに追加管理項目の設定をエクスポートします。次の項目を 1 つ以上指定できます。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 契約情報

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

```
ioutils△exportfield△-export△エクスポートするファイル名△-fieldtype△追加管理項目の種別  
[△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-fieldtype△追加管理項目の種別

エクスポートする追加管理項目の種別を指定します。追加管理項目の種別は次のとおりです。

- hardware：ハードウェア資産情報の追加管理項目
- license：ソフトウェアライセンス情報の追加管理項目
- contract：契約情報の追加管理項目

複数の種別を指定できます。複数種別の追加管理項目をエクスポートする場合、「,」（コンマ）区切りで指定します。

-s

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 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

戻り値

ioutils exportfield 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。

戻り値	説明
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
101	メモリ不足、またはその他のほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
150	その他のエラーでコマンドの実行が中断しました。

使用例

ハードウェア資産情報とソフトウェアライセンス情報の追加管理項目を、「C:¥temp¥hardexportfield.xml」にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportfield -export C:¥temp¥hardexportfield.xml -fieldtype hardware,license -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.7 ioutils importfield (追加管理項目の設定のインポート)

機能

XML ファイルから追加管理項目をインポートします。インポートできるファイルは、追加管理項目をエクスポートしたファイルです。

このコマンドでは、インポートによる項目の追加だけができます。項目の変更または削除はできません。エクスポートによってバックアップしていた追加管理項目を、障害対応や環境移行でリストアするときに使用してください。

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

```
ioutils△importfield△-import△インポートするファイル名
```

引数

-import△インポートするファイル名

インポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils importfield 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	追加管理項目のインポートは正常終了しましたが、一部のサービスが開始されていません。
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、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
80	インポートするファイルの形式が不正です。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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¥にエクスポートした hardexportfield.xml をインポートする場合のコマンドの使用例を示します。

```
ioutils importfield -import C:¥temp¥hardexportfield.xml
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.8 ioutils exporttemplate (テンプレートのエクスポート)

資産情報をインポートする際に、項目の対応づけを定義したテンプレートを使用できます。このテンプレートをエクスポートする `ioutils exporttemplate` コマンドについて説明します。

機能

指定された種別と名称のテンプレートをエクスポートします。次の項目のうち 1 つ指定できます。

- ハードウェア資産情報
- ソフトウェアライセンス情報
- 管理ソフトウェア情報
- 契約情報
- 契約会社リスト

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、ある管理用サーバで作成したテンプレートをほかの管理用サーバに流用できます。

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

```
ioutils△exporttemplate△-export△エクスポートするファイル名△-templatetype△テンプレートの種別△-name△テンプレート名 [△-s]
```

引数

`-export△`エクスポートするファイル名

エクスポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

`-templatetype△`テンプレートの種別

エクスポートするテンプレートの種別を指定します。テンプレートの種別は次のとおりです。

- `assetImport` : ハードウェア資産情報インポート時のテンプレート
- `licenseImport` : ソフトウェアライセンス情報インポート時のテンプレート
- `softwareImport` : 管理ソフトウェア情報インポート時のテンプレート
- `contractImport` : 契約情報インポート時のテンプレート
- `vendorCatalogImport` : 契約会社リスト情報インポート時のテンプレート

`-name△`テンプレート名

エクスポートするテンプレートの名称を指定します。

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 exportupdategroup
 - ioutils importasset
 - ioutils importfield
 - ioutils importfilter
 - ioutils importpolicy
 - ioutils importtemplate
 - ioutils importupdategroup

- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils exporttemplate 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
72	指定されたテンプレートがありません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

ハードウェア資産情報インポート時のテンプレート「ハードウェア資産情報テンプレート 1」を、「C:¥temp ¥assetexport.xml」にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exporttemplate -export C:¥temp¥assetexport.xml -templatetype assetImport -name ハードウェア資産情報テンプレート 1 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.9 ioutils importtemplate (テンプレートのインポート)

資産情報をインポートする際に、項目の対応づけを定義したテンプレートを使用できます。このテンプレートをインポートする `ioutils importtemplate` コマンドについて説明します。

機能

エクスポートしたテンプレートをインポートします。なお、インポートできるファイルは、テンプレートをエクスポートしたファイルだけです。テンプレート名を指定した場合、指定した名称で登録されます。テンプレート名を指定しなかった場合、エクスポート時の名称で登録されます。

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、ある管理用サーバで作成したテンプレートをほかの管理用サーバに流用できます。

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

```
ioutils△importtemplate△-import△インポートするファイル名[△-name△テンプレート名][△-s]
```

引数

`-import△インポートするファイル名`

インポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

`-name△テンプレート名`

インポートするテンプレートの名称を指定します。引数を省略した場合、エクスポート時のテンプレート名で登録されます。

`-s`

同じ名称のテンプレートがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のテンプレートが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて入力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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
- ioassetsfielddutil export
- ioassetsfielddutil 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 importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils importtemplate 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	指定されたフォルダが不正、ディスク容量が不足、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。
51	コマンドの実行権限がありません。

戻り値	説明
54	管理用サーバがセットアップされていません。
74	指定されたテンプレート名に誤りがあります。
80	インポートするファイルの形式が不正です。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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¥にエクスポート済みのハードウェア資産情報インポート時のテンプレート「assetexport.xml」を、「ハードウェア資産情報テンプレート 1」としてインポートする場合のコマンドの使用例を次に示します。

```
ioutils importtemplate -import C:¥temp¥assetexport.xml -name ハードウェア資産情報テンプレート 1 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.10 ioutils exportdevice (機器情報のエクスポート)

機器情報をエクスポートする `ioutils exportdevice` コマンドについて説明します。

機能

CSV ファイルに機器情報をエクスポートします。なお、エクスポート対象となる情報が 0 件の場合でも、ファイルが出力されます。

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、あるシステムの機器情報をほかのシステムに流用できます。

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

```
ioutils△exportdevice△-export△エクスポートするファイル名[△-filter△フィルタ名][△-encoding△文字コードの種別][△-s]
```

引数

`-export△エクスポートするファイル名`

エクスポートする CSV ファイル名を、259 バイト以内の絶対パスで指定します。

`-filter△フィルタ名`

フィルタを使用して機器情報をエクスポートする場合、操作画面のメニューエリアに表示されるフィルタ名を指定します。

`-encoding△文字コードの種別`

エクスポートする機器情報の文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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
 - importdb
 - ioassetsfieldutil export
 - ioassetsfieldutil import
 - ioutils exportasset
 - 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

ioutils exportdevice 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
70	指定されたフィルタがありません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

機器情報を C:\temp¥deviceexpo.csv にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportdevice -export C:\temp¥deviceexpo.csv -encoding UTF-8 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.11 ioutils exportdevicedetail (詳細な機器情報のエクスポート)

詳細な機器情報をエクスポートする `ioutils exportdevicedetail` コマンドについて説明します。

機能

CSV ファイルに詳細な機器情報をエクスポートします。なお、エクスポート対象となる情報が 0 件の場合でも、ファイルが出力されます。

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、あるシステムの機器情報をほかのシステムに流用できます。

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

```
ioutils△exportdevicedetail△-export△エクスポートするファイル名[△-template△テンプレート名][△-filter△フィルタ名][△-encoding△文字コードの種別][△-s]
```

引数

`-export△エクスポートするファイル名`

エクスポートする CSV ファイル名を、259 バイト以内の絶対パスで指定します。

`-template△テンプレート名`

エクスポート時に使用するテンプレート名を指定します。テンプレートに設定されている項目を、設定されている文字コードでエクスポートします。

`-filter△フィルタ名`

フィルタを使用して機器情報をエクスポートする場合、操作画面のメニューエリアに表示されるフィルタ名を指定します。

`-encoding△文字コードの種別`

エクスポートする機器情報の文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、テンプレートを指定するとテンプレートに設定された文字コードが指定されます。テンプレートを指定しないと、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932

- Shift-JIS
- EUC-JP
- JIS

-S

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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
 - importdb
 - ioassetsfieldutil export
 - ioassetsfieldutil import
 - ioutils exportasset
 - ioutils exportdevice
 - 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

ioutils exportdevicedetail 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
70	指定されたフィルタがありません。
72	指定されたテンプレートが存在しません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

機器情報を C:\temp¥devicedetailexpo.csv にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportdevicedetail -export C:\temp¥devicedetailexpo.csv -encoding UTF-8 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.12 ioutils exportpolicy (セキュリティポリシーの設定のエクスポート)

機能

セキュリティポリシーの設定情報を、指定したファイルにエクスポートします。

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、ある管理用サーバで作成したセキュリティポリシーをほかの管理用サーバに流用できます。

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

```
ioutils△exportpolicy△-export△エクスポートするファイル名△-name△セキュリティポリシー名  
[△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-name△セキュリティポリシー名

エクスポートするセキュリティポリシーの名称を指定します。

-s

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 exporttemplate
 - ioutils exportupdategroup
 - ioutils importasset
 - ioutils importfield
 - ioutils importfilter
 - ioutils importpolicy
 - ioutils importtemplate
 - ioutils importupdategroup
 - reorgdb
 - startservice
 - stopservice
 - updatesupportinfo
- セキュリティポリシーの使用必須ソフトウェアの自動対策でパッケージを指定している場合、そのセキュリティポリシーはエクスポートできません。

戻り値

ioutils exportpolicy 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
75	指定されたセキュリティポリシーはありません。

戻り値	説明
85	パッケージがあります。
101	メモリ不足、またはその他の要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
150	その他のエラーでコマンドの実行が中断しました。

使用例

セキュリティポリシーの設定情報「開発部用ポリシー」を「C:\temp¥exportpolicy.xml」にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportpolicy -export C:\temp¥exportpolicy.xml -name 開発部用ポリシー -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.13 ioutils importpolicy (セキュリティポリシーの設定のインポート)

機能

エクスポートしたセキュリティポリシーをインポートします。インポートできるファイルは、事前にエクスポートしたファイルだけです。セキュリティポリシー名を指定しなかった場合、エクスポート時の名称で登録されます。

複数の JP1/IT Desktop Management 2 システムを構築している場合、このコマンドを利用することで、ある管理用サーバで作成したセキュリティポリシーをほかの管理用サーバに流用できます。

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

```
ioutils△importpolicy△-import△インポートするファイル名[△-name△セキュリティポリシー名]  
[△-applygroup△適用する更新プログラムグループ名][△-excludegroup△除外する更新プログラムグループ名][△-s]
```

引数

-import△インポートするファイル名

インポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-name△セキュリティポリシー名

インポートするセキュリティポリシーの名称を指定します。引数を省略した場合、エクスポート時のセキュリティポリシー名で登録されます。

-applygroup△適用する更新プログラムグループ名

適用する更新プログラムグループ名を指定します。引数を省略した場合、エクスポート時の適用更新プログラムグループ名を割り当てられます。

-excludegroup△除外する更新プログラムグループ名

除外する更新プログラムグループ名を指定します。引数を省略した場合、エクスポート時の除外更新プログラムグループ名を割り当てられます。

-s

同じ名称のセキュリティポリシーがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のセキュリティポリシーが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて入力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 importtemplate`
 - `ioutils importupdategroup`
 - `reorgdb`
 - `startservice`
 - `stopservice`
 - `updatesupportinfo`
- タスクが指定されているセキュリティポリシーをエクスポートしたデータをインポートする場合、インポート先に同じタスク名が存在するかどうかチェックされます。同じタスクが存在するとき、タスク名の先頭に `imp_N_` (N は 1 以上の整数) が付与されてインポートされます。なお、タスク名が最大サイズを超えるときは、超過したタスク名の後ろの部分が省略されます。

戻り値

ioutils importpolicy 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	指定されたフォルダが不正、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
76	指定されたセキュリティポリシー名が不正です。
80	インポートするファイルの形式が不正です。
83	該当する更新プログラムグループがありません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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¥にエクスポート済みのセキュリティポリシーの設定情報「exportpolicy.xml」を、「開発部用ポリシー」としてインポートする場合のコマンドの使用例を次に示します。除外する更新プログラムグループ名を、「Windows XP 用除外プログラム」とします。

```
ioutils importpolicy -import C:¥temp¥exportpolicy.xml -name 開発部用ポリシー -excludegroup "Windows XP 用除外プログラム" -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.14 ioutils exportupdategroup (更新プログラムグループの設定のエクスポート)

機能

更新プログラムグループの設定情報を、指定したファイルにエクスポートします。

複数の JP1/IT Desktop Management 2 システムを構築している場合、あるシステムの更新プログラムグループの設定をほかのシステムに流用できます。

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

```
ioutils△exportupdategroup△-export△エクスポートするファイル名△-name△更新プログラムグループ名△[△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-name△更新プログラムグループ名

設定をエクスポートする更新プログラムグループ名を指定します。

-s

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 importasset
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils exportupdategroup 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
83	該当する更新プログラムグループがありません。

戻り値	説明
101	メモリ不足、またはその他の要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
150	その他のエラーでコマンドの実行が中断しました。

使用例

更新プログラムグループ「本社用除外グループ」の設定を「C:¥temp¥updategroup.xml」にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportupdategroup -export C:¥temp¥updategroup.xml -name 本社用除外グループ -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.15 ioutils importupdategroup (更新プログラムグループの設定のインポート)

機能

エクスポートした更新プログラムグループの設定情報を、インポートします。インポートできるファイルは、更新プログラムグループをエクスポートしたファイルだけです。

複数の JP1/IT Desktop Management 2 システムを構築している場合、あるシステムの更新プログラムグループの設定をほかのシステムに流用できます。

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

```
ioutils△importupdategroup△-import△インポートするファイル名[△-name△更新プログラムグループ名][△-s]
```

引数

-import△インポートするファイル名

インポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-name△更新プログラムグループ名

インポートする更新プログラムグループ名を指定します。引数を省略した場合、エクスポート時の更新プログラムグループ名で登録されます。

-s

同じ名称の更新プログラムグループがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称の更新プログラムグループが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて入力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils importupdategroup 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	指定されたフォルダが不正、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。

戻り値	説明
79	指定された更新プログラムグループ名が不正です。
80	インポートするファイルの形式が不正です。
101	メモリ不足、またはその他の要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
150	その他のエラーでコマンドの実行が中断しました。

使用例

C:¥temp¥にエクスポート済みの更新プログラムグループの設定「updategroup.xml」を、「本社用除外グループ」としてインポートする場合のコマンドの使用例を次に示します。

```
ioutils importupdategroup -import C:¥temp¥updategroup.xml -name 本社用除外グループ -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.16 ioutils exportoplog (操作ログのエクスポート)

機能

管理用サーバに格納されている操作ログを、指定した期間分だけ CSV ファイルにエクスポートします。

エクスポートするファイルのサイズが 2 ギガバイトを超える場合、ファイルを分割して出力します。分割されたファイルは、ファイル名の拡張子の前に連番が付与されます。

エクスポート対象となる情報が 0 件の場合でも、ファイルが出力されます。

エクスポートするファイルの出力形式については、「[付録 A.4 エクスポートした操作ログの出力形式](#)」を参照してください。

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

```
ioutils△exportoplog△-export△エクスポートするファイル名{△-range△エクスポートする期間 |  
△-within△エクスポートする日数}[△-encoding△文字コードの種別][△-filter△フィルタ名][△-  
line△エクスポートする行数][△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする CSV ファイルを、259 バイト以内の絶対パスで指定します。

-range△エクスポートする期間

エクスポートする期間を YYYY-MM-DD*の形式で指定します。開始日と終了日は、「,」（コンマ）で区切って指定します。

注※ YYYY：年、MM：月、DD：日

この引数は、-within と同時には指定できません。

-within△エクスポートする日数

エクスポートする日数を指定します。指定できる日数は 1～500 です。

この引数は、-range と同時には指定できません。

-encoding△文字コードの種別

エクスポートする操作ログの文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16

- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-filter△フィルタ名

フィルタを使用して特定の操作ログをエクスポートする場合、フィルタ名を指定します。

指定するフィルタ名のフィルタ条件には、[操作日時（Web ブラウザのロケール）] を含めないでください。[操作日時（Web ブラウザのロケール）] をフィルタ条件に含んだフィルタ名を指定すると、正しくフィルタリングされないことがあります。

-line△エクスポートする行数

1 ファイルにエクスポートする行数を指定します。指定できる行数は 1～4294967295 です。省略した場合、1 ファイルには 2 ギガバイト分の操作ログが出力されます。

-s

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils importasset
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils exporttoplog 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
70	指定されたフィルタがありません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

エクスポートする日数を「25」、フィルタ名を「ファイルコピー操作」の条件で、操作ログを「C:¥temp¥exportoplog.csv」としてエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportoplog -export C:¥temp¥exportoplog.csv -within 25 -encoding UTF-8 -filter ファイル  
コピー操作 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.17 ioutils exportfilter (フィルタの設定のエクスポート)

機能

指定されたフィルタ情報条件をエクスポートします。次に示す画面のメニューエリアに定義されているフィルタのうち 1 つ指定できます。

- ハードウェア資産
- ソフトウェアライセンス
- 管理ソフトウェア
- 契約
- 機器情報
- ソフトウェア情報
- 機器のセキュリティ状態
- 操作ログ
- 更新プログラム
- イベント一覧
- パッケージ
- タスク
- ネットワーク制御リスト※

注※ 設定画面－[ネットワーク制御]－[ネットワーク制御リストの設定] 画面のインフォメーションエリアで設定するフィルタです。

複数の JP1/IT Desktop Management 2 システムを構築している場合、あるシステムのフィルタをほかのシステムに流用できます。

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

```
ioutils△exportfilter△-export△エクスポートするファイル名△-filtertype△フィルタの種別△-name△エクスポートするフィルタ名[△-s]
```

引数

-export△エクスポートするファイル名

エクスポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-filtertype△フィルタの種別

エクスポートするフィルタの種別を指定します。フィルタの種別は次のとおりです。

- asset：ハードウェア資産
- license：ソフトウェアライセンス
- mngsoft：管理ソフトウェア
- contract：契約
- device：機器情報
- inssoft：ソフトウェア情報
- secdevice：機器のセキュリティ状態
- oplog：操作ログ
- update：更新プログラム
- event：イベント一覧
- package：パッケージ
- task：タスク
- netctl：ネットワーク制御リスト

-name△エクスポートするフィルタ名

エクスポートするフィルタ名を指定します。

-s

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 exporttoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils importasset
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

エクスポートできないフィルタの条件を次の表に示します。

項目	エクスポートできないフィルタの条件
機器種別	フィルタにユーザーが任意に追加した項目（機器種別や資産状態など）が含まれている場合
資産種別	
予定資産状態	
ライセンス種類	
ライセンス状態	
予定ライセンス状態	
ライセンス種類	
契約種別	
契約状態	
部署	部署の項目が含まれている場合
設置場所	設置場所の項目が含まれている場合

戻り値

ioutils exportfilter 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
70	指定されたフィルタがありません。
86	エクスポートできない項目があります。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

ハードウェア資産のフィルタ「低スペックな PC」を、「C:¥temp¥exportfilter.xml」にエクスポートする場合のコマンドの使用例を次に示します。

```
ioutils exportfilter -export C:¥temp¥exportfilter.xml -filtertype asset -name 低スペックな PC -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.18 ioutils importfilter (フィルタの設定のインポート)

機能

エクスポートしたフィルタをインポートします。インポートできるファイルは、フィルタをエクスポートしたファイルだけです。

複数の JP1/IT Desktop Management 2 システムを構築している場合、あるシステムのフィルタをほかのシステムに流用できます。

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

```
ioutils△importfilter△-import△インポートするファイル名[△-name△フィルタ名][△-s]
```

引数

-import△インポートするファイル名

インポートする XML ファイル名を、259 バイト以内の絶対パスで指定します。

-name△フィルタ名

インポートするフィルタ名を指定します。フィルタ名を省略した場合、エクスポート時のフィルタ名で登録されます。

-s

同じ名称のフィルタがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のフィルタが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて入力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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開始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 importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

戻り値

ioutils importfilter 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	指定されたフォルダが不正、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
77	指定されたフィルタ名が不正です。
80	インポートするファイルの形式が不正です。

戻り値	説明
84	エクスポート元とインポート先の追加資産管理項目が不整合です。
101	メモリ不足、またはその他の要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
150	その他のエラーでコマンドの実行が中断しました。

使用例

C:¥temp¥にエクスポート済みのハードウェア資産のフィルタ「exportfilter.xml」を、「滅却予定の PC」
としてインポートする場合のコマンドの使用例を次に示します。

```
ioutils importfilter -import C:¥temp¥exportfilter.xml -name 滅却予定の PC -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.19 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

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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

- [17.1 コマンドを実行する手順](#)

17.20 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 JP1/IT Desktop Management 2 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)、「@」、「¥」

JP1/IT Desktop Management 2 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
JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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

- [17.1 コマンドを実行する手順](#)

17.21 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）、「@」、「¥」

JP1/IT Desktop Management 2 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。

JP1/IT Desktop Management 2 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、10,000 台の機器を管理する場合は 10 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)、「@」、「¥」

JP1/IT Desktop Management 2 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。

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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

- [17.1 コマンドを実行する手順](#)

17.22 reorgdb (データベースの再編成)

機能

データベースを再編成します。データベースのパフォーマンスの効率を上げるため、システム管理者は定期的にこのコマンドを実行することをお勧めします。

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

```
reorgdb[△-s][△-w△作業用フォルダ名]
```

引数

-s

管理用サーバのサービスの停止 (stopservice コマンド)、データベースの再編成 (reorgdb 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。

-w△作業用フォルダ名

データベースの再編成処理時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、10,000 台の機器を管理する場合は 30 ギガバイト以上の空き容量が必要です。また、クラスタ構成の場合は、共有ディスクのフォルダを指定します。

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、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)、「@」、「¥」

JP1/IT Desktop Management 2 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。

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥temp

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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
 - 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
 - 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

reorgdb 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	データベースの再編成に成功しましたが、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。

戻り値	説明
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。
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	デフォルトの作業用フォルダが使用できません。
101	データベースの再編成に失敗しました。
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

管理用サーバのサービスの停止、データベースの再編成、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ときのコマンドの使用例を示します。

reorgdb -s

関連リンク

- [17.1 コマンドを実行する手順](#)

17.23 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

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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

- [17.1 コマンドを実行する手順](#)

17.24 startservice (サービス開始)

機能

管理用サーバの関連サービスを起動し、管理用サーバを起動状態にします。

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

```
startservice
```

引数

引数はありません。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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
- stopservice
- updatesupportinfo

戻り値

startservice 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開始しています。
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開始に失敗しました。
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。

使用例

管理用サーバのサービスを開始するコマンドの使用例を次に示します。

```
startservice
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.25 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またはリモートインストールマネージャを導入したコンピュータ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次に示すフォルダに格納されます。

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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

- [17.1 コマンドを実行する手順](#)

17.26 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）

JP1/IT Desktop Management 2 - Manager または Remote Install Manager 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 JP1/IT Desktop Management 2 - Manager または Remote Install Manager 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またはリモートインストールマネージャを導入したコンピュータ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

JP1/IT Desktop Management 2 の提供媒体のルート¥_PPDIR¥P064274A¥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。

戻り値	説明
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

- [17.1 コマンドを実行する手順](#)

17.27 addfwlist.bat (Windows ファイアウォールの例外許可設定)

Windows ファイアウォールが有効なコンピュータに JP1/IT Desktop Management 2 - Manager または Remote Install Manager をインストールすると、自動的に例外許可が設定されます。ただし、Windows ファイアウォールが無効なコンピュータの場合、例外許可は設定されません。このため、JP1/IT Desktop Management 2 - Manager または Remote Install Manager をインストールしたあとで、Windows ファイアウォールを無効から有効に変更する場合は、このコマンドで Windows ファイアウォールの例外許可設定を行ってください。

機能

JP1/IT Desktop Management 2 - Manager または Remote Install Manager を Windows ファイアウォールの例外対象に設定します。

なお、このコマンドは管理用サーバまたはリモートインストールマネージャを導入したコンピュータで実行してください。

形式

```
addfwlist.bat
```

引数

引数はありません。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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、Windows ファイアウォールのサービスが開始している状態で実行してください。

戻り値

addfwlist.bat 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	コマンドが異常終了しました。

使用例

Windows ファイアウォールの例外許可設定を行うコマンドの使用例を次に示します。

addfwlist.bat

関連リンク

- [17.1 コマンドを実行する手順](#)

17.28 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 JP1/IT Desktop Management 2 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 JP1/IT Desktop Management 2 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 [基本設定] - [上位システムとの通信のタイミング] 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)]
- ポーリングの設定で指定した間隔

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¥jpltdma」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¥jpltdma¥bin"
```

```
start /wait Cscript.exe resetnid.vbs /nodeid
```

```
echo %errorlevel%
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.29 getinv.vbs (オフライン管理の情報収集)

機能

オフライン管理のコンピュータに対して、情報収集用ツールの設定に従って次に示す処理を実行したあとで、機器情報を収集します。

- [利用者情報の入力] 画面の表示の制御
- ソフトウェア検索条件に従ったソフトウェア検索
- 最新のウイルス対策製品の情報収集

このコマンドの前提条件を次に示します。

- エージェントのサービスが開始している
- エージェントのバージョンが 10-01 以降である
- 機器情報の収集処理が実行されていない
- [利用者情報の入力] 画面が表示されていない
- このコマンドが格納されているフォルダがローカルドライブである
- このコマンドが格納されているフォルダのフルパスが 128 文字以内である

なお、このコマンドは、外部記憶媒体に格納して、オフライン管理のコンピュータ上で直接実行してください。

形式

```
getinv.vbs[△/u][△/s][△/silent]
```

引数

/u

[利用者情報の入力] 画面を、利用者のコンピュータに表示しません。引数「/silent」を指定した場合は、引数「/u」の指定とは関係なく [利用者情報の入力] 画面を表示しません。

/s

設定画面の [ソフトウェア検索条件の設定] 画面で設定したインストールソフトウェア情報を、取得しません。

/silent

利用者のコンピュータに、画面を表示しません。

格納先

情報収集用ツール（解凍後）の格納先

注意事項

次に示す場合は、情報収集用ツールを再作成したあとで、機器情報を収集する必要があります。

- セキュリティポリシーでの判定対象のウィルス対策製品を変更した場合
- 追加管理項目の設定を変更した場合

戻り値

getinv.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、収集処理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。
10031	情報収集用ツールを使用した情報の収集は、すでに実行されています。
10032	一時的なエラーが発生しました。
10033	バックグラウンドで情報の収集が実行されています。
10034	【利用者情報の入力】画面が表示されています。
10051	格納フォルダのパスが長過ぎるため、処理を中止しました。
10052	情報収集用ツールがローカルディスク上にありません。
10101	情報の収集に失敗しました。
10102	このコマンドが格納されているフォルダに、読み込みおよび書き込みの権限がありません。
10103	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せん。
10104	コンピュータにインストールされているエージェントは、オフライン管理に対応していないバージョンです。
10105	情報収集用ツールが壊れていることが考えられます。
10106	エージェントの環境が壊れています。

使用例

【利用者情報の入力】画面を利用者のコンピュータに表示しないで機器情報を収集する場合のコマンドの使用例を次に示します。

getinv.vbs /u

17.30 ioassetsfieldutil export (共通管理項目と追加管理項目の定義のエクスポート)

共通管理項目と追加管理項目の定義をエクスポートする `ioassetsfieldutil export` コマンドについて説明します。

機能

CSV ファイルに共通管理項目と追加管理項目の定義をエクスポートします。

エクスポートできる定義は、次の共通管理項目と追加管理項目のうち、データ型が階層型と選択型のものです。

- ハードウェア資産情報と機器情報の共通管理項目
- ハードウェア資産情報の追加管理項目
- ソフトウェアライセンス情報の追加管理項目
- 契約情報の追加管理項目

なお、このコマンドは管理用サーバで実行してください。また、管理用サーバのセットアップが完了し、かつ管理用サーバのサービスが開始している状態で実行してください。

形式

```
ioassetsfieldutil△export△-field△エクスポートするファイル名[△-encoding△文字コードの種別][△-s]
```

引数

`-field△`エクスポートするファイル名

エクスポートする CSV ファイル名を、255 バイト以内の絶対パス名で指定します。

`-encoding△`文字コードの種別

エクスポートする CSV ファイルの文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932

- Shift-JIS
- EUC-JP
- JIS

-S

エクスポート先に同じ名称のファイルがすでに存在しても、確認しないで上書きします。引数を省略した場合、同じ名称のファイルが存在すると、上書き確認のメッセージを出力し、管理者の応答に応じて出力を中止または上書きします。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

JP1/IT Desktop Management 2 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、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 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

戻り値

ioassetsfieldutil export 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	指定されたフォルダが不正、ディスク容量が不足、またはフォルダがありません。
15	ファイル出力時のファイルのアクセスエラー、または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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
101	メモリ不足、またはそのほかの要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。
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

共通管理項目と追加管理項目の定義を C:¥temp¥common.csv にエクスポートする場合のコマンドの使用例を次に示します。

```
ioassetsfieldutil export -field C:¥temp¥common.csv -encoding UTF-8 -s
```

関連リンク

- [17.1 コマンドを実行する手順](#)

17.31 ioassetsfieldutil import (共通管理項目と追加管理項目の定義のインポート)

共通管理項目と追加管理項目の定義をインポートする `ioassetsfieldutil import` コマンドについて説明します。

機能

CSV ファイルに共通管理項目と追加管理項目の定義をインポートします。このコマンドを利用することで、共通管理項目と追加管理項目の定義を一括して追加、更新、および削除できます。

CSV ファイルの記述形式の誤りが原因でインポートに失敗した場合、インポートログファイルが出力されます。CSV ファイルの記述形式の誤りは、100 件まで検出されます。CSV ファイルの記述形式の誤りが原因でインポートに失敗した場合の対処方法については、「[18.6 共通管理項目と追加管理項目の定義のインポートに失敗した場合のトラブルシューティング](#)」を参照してください。

`ioassetsfieldutil import` コマンドで部署の定義を移動した場合、次の情報が移動後の部署に引き継がれます。

- 移動した部署に割り当たっているセキュリティポリシー
- 移動した部署に割り当たっているエージェント設定
- 移動した部署に関連づいているレポートのデータ

なお、このコマンドは管理用サーバで実行してください。また、管理用サーバのセットアップが完了し、かつ管理用サーバのサービスが開始している状態で実行してください。

形式

```
ioassetsfieldutil△import△-field△インポートするファイル名[△-agentupdate△利用者の入力開始のタイミング][△-encoding△文字コードの種別][△-c]
```

引数

`-field△インポートするファイル名`

インポートする CSV ファイル名を、255 バイト以内の絶対パス名で指定します。

`-agentupdate△利用者の入力開始のタイミング`

利用者の入力開始のタイミングを指定します。引数を省略した場合、設定画面の「資産管理」－「資産管理項目の設定」－「利用者情報の入力開始日時」に表示されている設定のままコマンドを実行します。指定できる値を次に示します。

now

コマンドを実行したタイミングで、利用者のコンピュータに情報入力を促すメッセージを表示します。

"YYYY-MM-DD△HH:MM"※

指定した入力開始日時（利用者のコンピュータのローカルタイム）から、利用者のコンピュータに情報入力を促すメッセージを表示します。

注※ YYYY：年、MM：月、DD：日、HH：時、MM：分

-encoding△文字コードの種別

インポートする CSV ファイルの文字コードを指定します。文字コードの種別は次のとおりです。引数を省略した場合、UTF-8 が指定されます。

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-C

インポートする CSV ファイルの形式のチェックだけを実施する場合に指定します。

格納先

JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥bin¥

注意事項

- 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
 - 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
- 配布の実行中にはこのコマンドを実行しないでください。このコマンドを実行すると、サービス (JP1_ITDM2_Agent Control) の処理が一時中断されるため、配布が遅れることがあります。

戻り値

ioassetsfieldutil import 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	インポートに成功しましたが、エージェント制御サービスの再開始に失敗しました。
11	コマンド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、ディスク容量が不足、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。
51	コマンドの実行権限がありません。
54	管理用サーバがセットアップされていません。
80	インポートするファイルの形式が不正です。
87	インポートデータのデータベース反映に失敗しました。
101	メモリ不足、またはその他の要因でコマンド実行に失敗しました。
120	データベースのアクセスエラーです。

使用例

C:¥temp¥にエクスポート済みの共通管理項目と追加管理項目の定義「common.csv」をインポートする場合のコマンドの使用例を次に示します。

```
ioassetsfieldutil import -field C:¥temp¥common.csv
```

関連リンク

- [17.1 コマンドを実行する手順](#)

18

トラブルシューティング

ここでは、JP1/IT Desktop Management 2 の運用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。

18.1 運用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運用時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。

管理用サーバでトラブルが発生した場合

1. エラーメッセージを確認する

次に示す方法で、エラーメッセージを確認してください。

- エラーの発生時に表示されるダイアログから、エラー内容を確認してください。
- 出力されたログファイルから、エラー内容を確認してください。
- ホーム画面またはイベント画面から、イベントのメッセージを確認してください。

2. トラブルの要因および対処方法を確認して、対処する

メッセージに従ってトラブルの要因および対処方法を確認して、対処してください。

エージェントでトラブルが発生した場合

エージェントでトラブルが発生した場合は、管理者が対処してください。

1. エラーメッセージを確認する

ホーム画面またはイベント画面から、イベントのメッセージを確認してください。

2. イベントのメッセージから判断および対処する

必要に応じてトラブルシュート用情報を採取してください。

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。

- KDEXnnnnn-Z メッセージテキスト
- KFPHnnnnnn-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

JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 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。JP1/IT Desktop Management 2 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があるメッセージを示します。

18.2 機器が発見されない場合の対処方法

機器の探索を実行した際に、機器が発見されない場合の対処方法について説明します。

次に示す条件に当てはまる機器は発見できません。これらの条件に一致する機器がある場合は、条件に一致しなくなるよう対処してから再度探索を実行してください。

- 探索条件の探索範囲に含まれていない
- 探索条件の認証情報（ID またはコミュニティ名）に誤りがある
- 機器の電源が OFF になっている
- 機器がネットワークに接続されていない
- NAPT を利用している
- Windows のファイアウォールの設定やルータの設定によって ICMP が通信できない
- 仮想 PC の場合に IP アドレスを共有している
- 仮想 PC の場合にプライベートネットワークを共有している

18.3 認証エラー発生時の対処方法

機器の探索を実行した際に、エージェントレスのコンピュータで認証エラーが発生した場合の対処方法について説明します。

管理用サーバでの対処方法

次に示す内容を確認し、誤りなどがある場合は対処してください。

探索範囲の設定

探索範囲が正しく設定されているかどうかを確認してください。探索範囲の設定方法については、「[15.2 機器の探索の設定](#)」を参照してください。

認証情報の登録

認証情報の登録（Windows 認証または SNMP 認証）が正しく設定されているかどうかを確認してください。なお、ユーザーアカウント制御（UAC）がサポートされている Windows を探索する場合は、そのコンピュータのビルトインユーザーの認証情報を設定する必要があります。認証情報の登録方法については、「[15.2 機器の探索の設定](#)」を参照してください。

認証情報の割り当て

認証情報の割り当てが正しく設定されているかどうかを確認してください。認証情報の割り当て方法については、「[15.2 機器の探索の設定](#)」を参照してください。

利用者のコンピュータでの対処方法

次に示す内容を確認し、誤りなどがある場合は対処してください。

SNMP 認証

- コミュニティ名が正しく設定されているかどうかを確認してください。
- SNMP エージェントのサービスが正しく動作しているかどうかを確認してください。

Windows 認証について

- ファイル共有の追加設定をしてください。
- 管理共有が無効になっている場合は、有効にしてください。管理共有は、Windows の `net share` コマンドで確認できます。このコマンドを実行した結果、「admin\$」が表示されれば管理共有が有効になっています。
- 認証情報には、Administrator 権限を持ち、アカウントが有効なユーザーを設定してください。
- Windows 8.1、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、または Windows Vista の場合で、ユーザーアカウント制御（UAC）が有効なときは、Administrator 権限を持つビルトインユーザーを利用するか、Administrator 権限を持つユーザーでかつ UAC を無効にしてください。
- Windows Server 2008、Windows Vista、または Windows XP の場合で、ファイアウォールが有効なときは、外部のサーバからのファイル共有を許可してください。

- Windows XP の場合、簡易ファイル共有を無効にしてください。

18.4 情報収集用ツールで収集した機器情報の通知に失敗した場合のトラブルシューティング

機器情報の通知に失敗した場合は、通知失敗リスト（result_failed.txt）の情報を基に機器情報を収集し直したあと、再通知してください。

通知失敗リストは、通知に失敗したコンピュータがある場合に生成されます。通知失敗リストには、機器情報の通知に失敗したコンピュータのホスト名の一覧が出力されます。

生成先

機器情報を通知するときに表示された、[通知情報の格納先の指定] ダイアログで指定した「Data」フォルダ

出力形式

YYYY/MM/DD△hh:mm:ss△ホスト名※

注※ YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

出力例

2012/10/11 14:15:16 Host1

2012/10/11 14:15:18 Host2

2012/10/11 14:15:19 Host3

18.5 CSV ファイルが正しく表示されないときの対処方法

インポートまたはエクスポートする場合、ご利用の環境によっては CSV ファイルが正しく表示されないことがあります。ここでは、CSV ファイルが正しく表示されないときの対処方法を説明します。

インポートする場合

資産情報をインポートする場合に、[データの項目名を対応づける] 画面でデータが正しく表示されないときは、1 つ前の [インポートファイルを読み込む] 画面に戻って、[文字エンコーディング] でインポートする CSV ファイルの文字コードを変更してください。

エクスポートした場合

エクスポートした CSV ファイルを表計算ソフトウェアなどで参照する場合に、データが正しく表示されないときは、[エクスポートする項目の選択] ダイアログの [文字エンコーディング] で、エクスポートする CSV ファイルの文字コードを変更してください。

ポイント

エクスポートした資産情報を編集してインポートする場合は、エクスポート時に選択した文字コードをインポート時にも指定してください。

18.6 共通管理項目と追加管理項目の定義のインポートに失敗した場合のトラブルシューティング

インポートした CSV ファイルの記述形式の誤りが原因で、共通管理項目と追加管理項目の定義のインポートに失敗した場合は、`ioassetsfieldutil import` コマンド実行時に出力されるインポートログファイル（インポートするファイル名.log）の情報を基に CSV ファイルを修正してから、`ioassetsfieldutil import` コマンドを再実行してください。

インポートログファイルは、インポートした CSV ファイルの記述形式の誤りが原因でインポートに失敗したときだけ生成されます。

`ioassetsfieldutil import` コマンドは、インポートする CSV ファイルをすべて読み込んだあと、次に示す順に行を並び変えてからインポートを実行します。そのため、インポートログファイルも次に示す順に出力されます。

1. 更新区分が「A」（追加）の定義で、階層が浅い定義から深い定義の順
2. 更新区分が「U」（更新）の定義（インポートする CSV ファイルと同じ順）
3. 更新区分が「D」（削除）の定義で、階層が深い定義から浅い定義の順

生成先

インポートした CSV ファイルを格納しているフォルダ

出力形式

メッセージ ID△※インポートした CSV ファイルの行番号:インポートした CSV ファイルの情報

注※ メッセージ ID は、インポートに失敗した定義の行だけに出力されます。

出力例

```
8:a,common,ja,部署,ja,,開発部/開発C課,,,,  
KDEX4388-E 3:u,common,ja,部署,ja,営業部/営業1課err,営業部/営業課,,,,  
4:d,common,ja,部署,ja,営業部/営業2課,,,,
```

出力例では、インポートした CSV ファイルの 3 行目に記載している定義の更新に失敗しています。コマンドプロンプトに表示される KDEX4388-E のメッセージを参考にインポートした CSV ファイルの 3 行目を修正し、`ioassetsfieldutil import` コマンドを再実行する必要があります。

関連リンク

- [17.31 ioassetsfieldutil import（共通管理項目と追加管理項目の定義のインポート）](#)

18.7 ディスクの空き容量が少ないときの対処方法

JP1/IT Desktop Management 2 のデータベースの格納先、操作ログの保管先、および保存用の変更履歴の出力先のディスクの空き容量が不足すると、新規にデータを追加できなくなり、正しい情報で管理できなくなってしまいます。

このような事態を避けるためには、JP1/IT Desktop Management 2 が使用するディスクの空き容量を監視して、空き容量が少なくなってきたときに対処する必要があります。

JP1/IT Desktop Management 2 が使用するディスクの空き容量は、ホーム画面の [データベースとディスクの状況] パネルで確認できます。

ディスクの空き容量が少なくなってくると、[通知事項] パネルに警告またはエラーのメッセージが表示されます。これらのメッセージが表示された場合は、空き容量を増やすために対処してください。対処の例を次に示します。

- ディスク内の不要なデータを削除する
- 論理ドライブを利用している場合、ディスク増設などで容量を追加する

ディスクの空き容量を確保できない場合は、セットアップで各フォルダのパスを変更したり、管理用サーバをリプレースして対処してください。

18.8 フェールオーバー発生後の対処方法

クラスタシステムで運用中にフェールオーバーが発生した場合の、実行中の処理に応じた対処方法を次の表に示します。

実行中の処理	フェールオーバー後の対処方法
操作画面の参照中	通信またはデータベースアクセスのエラーメッセージが出力されたあとで、いったんログアウトしてからログインし直してください。
パッケージ登録中	通信またはデータベースアクセスのエラーメッセージが出力されたあとで、いったんログアウトしてからログインし直してください。 パッケージの登録が完了していない場合は、パッケージを再登録してください。
資産情報などのインポート中	通信またはデータベースアクセスのエラーメッセージが出力されたあとで、いったんログアウトしてログインし直してから、インポートを再実行してください。
資産情報などのエクスポート中	通信またはデータベースアクセスのエラーメッセージが出力されたあとで、いったんログアウトしてログインし直してから、エクスポートを再実行してください。
データベースマネージャ実行中	実行中だった処理を再実行してください。
セットアップ実行中	クラスタグループの所有者をフェールオーバー前のノードに移したあと、セットアップを再実行してください。
コンポーネントの登録中	コンポーネントを再登録してください。
USB デバイスの登録中	USB デバイスを再登録してください。
コマンド実行中	コマンドを再実行してください。 また、実行していたコマンドに応じて、次に示す対処をしてください。 • ioutils exportasset（ハードウェア資産情報のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportfield（追加管理項目の設定のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exporttemplate（テンプレートのエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportdevice（機器情報のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportdevicedetail（詳細な機器情報のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportpolicy（セキュリティポリシーの設定のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportupdategroup（更新プログラムグループの設定のエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportoplog（操作ログのエクスポート） エクスポートされたファイルを削除してください。 • ioutils exportfilter（フィルタの設定のエクスポート） エクスポートされたファイルを削除してください。 • ioassetsfieldutil export（共通管理項目と追加管理項目の定義のエクスポート）

実行中の処理	フェールオーバー後の対処方法
コマンド実行中	エクスポートされたファイルを削除してください。 • exportdb（バックアップの取得） バックアップ先フォルダを削除してください。 • getlogs（管理用サーバのトラブルシュート用情報の取得） トラブルシュート用情報格納先フォルダを削除しないでください。サポートサービスに問い合わせるときに必要なことがあります。 • getinstlogs（インストール時のトラブルシュート用情報の取得） トラブルシュート用情報格納先フォルダを削除しないでください。サポートサービスに問い合わせるときに必要なことがあります。

18.9 管理用サーバのトラブルシューティング

障害発生時には、JP1/IT Desktop Management 2 の画面にメッセージが表示されます。このメッセージに従ってトラブルの要因および対処方法を確認して、対処してください。

イベント画面で対処が必要なイベントを確認した場合は、イベントのメッセージを確認して対処してください。

また、エラーが発生するとログファイルが出力されます。ログファイルからエラーの要因や対処方法を確認してください。

対処が必要なイベントの要因と対処を次の表に示します。

イベント番号	種類	メッセージ	要因	対処
002	設定	機器の状態が管理対象外に変更されました。	機器が管理対象外に変更されました。	設定画面の [機器の探索] - [除外対象機器] 画面を確認してください。
004	設定	ライセンス数を超過したため管理対象の機器として登録できませんでした。	ライセンス超過を検知しました。	管理台数分のライセンスを購入し、設定画面の [製品ライセンス] - [製品ライセンスの設定] 画面でライセンスを追加してください。
005	設定	エージェントがアンインストールされました。	エージェントのアンインストールを検知しました。	エージェントのアンインストールを許可した機器かどうかを確認してください。
019	エラー	機能名で詳細情報を取得できませんでした。	機器の探索や機器情報の収集が失敗しました。	認証情報や探索範囲などの設定内容、サービス (JP1_ITDM2_Agent Control) の稼働状況を確認してください。または、対象機器の状態を確認してください。確認完了後、機器の探索や機器情報の収集を再実行してください。 それでも解決できない場合は、 <code>getlogs</code> コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
050	セキュリティ	機器のセキュリティ状態を判定しました。判定結果は 危険 レベルです。	セキュリティ判定の結果、対象のコンピュータが危険と判定されました。	対象のコンピュータに対して、セキュリティ対策を実施してください。
051	セキュリティ	機器のセキュリティ状態を判定しました。判定結果は 危険 レベルです。	セキュリティ判定の結果、対象のコンピュータが警告または注意と判定されました。	対象のコンピュータに対して、セキュリティ対策を実施してください。

イベント番号	種類	メッセージ	要因	対処
055	エラー	管理者へのメール通知に失敗しました。	• 要因 1 管理者にメールアドレスが設定されていません。または、メールアドレスに誤りがあります。 • 要因 2 メールサーバの設定に誤りがあります。または、メールサーバが稼働していません。 • 要因 3 メールサーバの接続に必要な認証の設定に誤りがあります。	要因ごとに次に示す対策を実施してください。 • 要因 1 設定画面の [ユーザー管理] – [ユーザーアカウントの管理] 画面で、管理者にメールアドレスを設定してください。または、正しいメールアドレスに変更してください。 • 要因 2 設定画面の [他システムとの接続] – [メールサーバの設定] 画面で、メールサーバの設定を修正してください。または、メールサーバの管理者へ連絡してください。 • 要因 3 設定画面の [他システムとの接続] – [メールサーバの設定] 画面で、メールサーバで使用する認証の設定を修正してください。
057	エラー	利用者へのメッセージ通知に失敗しました。	管理用サーバとコンピュータ間のネットワークなどの障害により、メッセージの通知に失敗しました。	getlogs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
074	エラー	セキュリティ対策の実施に失敗しました。	セキュリティ対策が失敗しました。	getlogs コマンドでトラブルシュート用情報を取得し、エラー要因を取り除いたあと、セキュリティ対策を実施してください。また、メッセージ通知などにより、利用者にセキュリティ対策を依頼してください。
078	エラー	印刷操作の抑止を解除できませんでした。	印刷抑止の解除が失敗しました。	失敗したのが印刷抑止の解除を許可した利用者かどうかを確認し、許可した利用者の場合は、正しい印刷抑止解除パスワードを連絡してください。許可していない利用者の場合は、必要に応じて印刷を抑止していることを連絡してください。
081	エラー	当該機器にすでに適用されているグループポリシーと異なるため、セキュリティ対策を実施できませんでした。	セキュリティ対策を実施しようとしたが、すでに適用されているセキュリティポリシーと異なっていました。	適用済みのセキュリティポリシーおよびセキュリティ対策の内容を確認してください。

イベント番号	種類	メッセージ	要因	対処
200	エラー	サービス (JP1_ITDM2_Service) でエラーが発生しました。サービス (JP1_ITDM2_Service) を停止します。	サービス (JP1_ITDM2_Service) の内部で致命的なエラーが発生しました。	getlogs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
203	エラー	製品更新情報の取得に失敗しました。サポートサービスの設定情報が不正です。	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] 画面の設定に誤りがあります。	サポートサービスサイトと接続するための情報を確認し、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] 画面の設定を修正してください。[接続テスト] ボタンをクリックすると、サポートサービスに接続できるか確認できます。
206	エラー	Active Directory サーバとの接続に失敗しました。Active Directory の設定情報が不正です。	Active Directory サーバが稼働していません。または、設定画面の [他システムとの接続] - [Active Directory の設定] 画面の設定に誤りがあります。	Active Directory サーバの稼働状況を確認してください。Active Directory サーバが稼働している場合は、設定画面の [他システムとの接続] - [Active Directory の設定] 画面の設定を修正してください。[接続テスト] ボタンをクリックすると、Active Directory サーバに接続できるか確認できます。
208	エラー	受信ファイルの更新処理でエラーが発生しました。	エージェントからの情報の受信に失敗しました。	管理用サーバの環境でリソースが不足しているおそれがあります。このエラーが頻発するときは、管理用サーバの環境を見直してください。
209	エラー	機能名でエラーが発生しました。	マネージャサービスの内部処理でエラーが発生しました。	設定画面の [機器の探索] 画面や [エージェント] 画面、または機器画面を確認したあと、探索またはエージェントの配信を再実行してください。 繰り返し発生する場合は、getlogs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
210	エラー	受信ファイルの更新処理でエラーが発生したため、更新できませんでした。	エージェントからの情報の受信に失敗し、回復が見込めないため更新処理を中止しました。	管理用サーバの環境でリソースが不足している可能性があります。管理用サーバの環境を見直したあと、情報を再取得してください。

イベント番号	種類	メッセージ	要因	対処
211	エラー	フォーマットが不正なファイルを受信したため、更新できませんでした。	フォーマットが不正なファイルを受信しました。	取得元のデータに特殊文字（制御コードなど）が含まれているおそれがあります。取得元のデータが編集できれば、特殊文字を取り除いて再度情報を取得してください。 繰り返し発生する場合は、 getlogs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
1003	設定	エージェントの環境が壊れました。	エージェントのファイルが削除されたなどして、エージェントの実行環境が壊れています。	エージェント側でアップデートを実施し、環境を修復してください。
1004	機器	新しいソフトウェアが発見されました。	新しいソフトウェアを検知しました。	機器画面の [ソフトウェア情報] 画面で、問題のないソフトウェアかどうか確認してください。
1006	エラー	使用禁止サービスを停止できませんでした。	使用禁止サービスを停止しようとしたのですが、停止できませんでした。	エージェントの状態を確認してください。
1016	配布	使用必須ソフトウェアを配布します。	使用必須ソフトウェアがインストールされていないことを検知しました。	自動対策が実施されるので、配布（ITDM 互換）画面でタスクの実行結果を確認してください。
1017	配布	使用禁止ソフトウェアを削除します。	使用禁止ソフトウェアがインストールされていることを検知しました。	自動対策が実施されるので、配布（ITDM 互換）画面でタスクの実行結果を確認してください。
1018	配布	パッケージ配布タスクがエラー終了しました。	インストールが何らかの要因によって失敗しました。	イベント詳細でエラーの要因を確認して、問題を解決したあと、再実行してください。
1019	配布	アンインストールタスクがエラー終了しました。	アンインストールが何らかの要因によって失敗しました。	イベント詳細でエラーの要因を確認して、問題を解決したあと、再実行してください。
1021	配布	管理者が実行するタスク（タスク名）が完了しました。	管理者が実行するタスクが完了しました。	配布（ITDM 互換）画面でタスクの実行結果を確認してください。
1022	資産	未確認のハードウェア資産（機器種別）が登録されました。	管理対象機器の追加、USB デバイスの登録が実行されました。	資産画面で、資産状態が [未確認] のハードウェア資産情報を編集してください。
1028	設定	ネットワークの探索が終了しました。	ネットワークの探索が終了しました。	設定画面の [探索履歴の確認] 画面で、探索結果を確認してください。

イベント番号	種類	メッセージ	要因	対処
1029	設定	Active Directory との同期が完了しました。	Active Directory の探索が終了しました。	設定画面の [探索履歴の確認] 画面で、探索結果を確認してください。
1032	エラー	操作ログの保管でエラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しているおそれがあります。	要因ごとに次に示す対策を実施してください。 • 要因 1 get logs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 セットアップで指定したローカルデータフォルダの空き容量を増やすか、ローカルデータフォルダを十分な空き容量のあるディスクに変更してください。 • 要因 3 セットアップで指定した操作ログの保管先フォルダが存在し、接続できるか確認してください。 • 要因 4 セットアップで指定したユーザー名とパスワードを確認してください。 • 要因 5 セットアップで指定した操作ログの保管先フォルダの空き容量を増やすか、操作ログの保管先フォルダを十分な空き容量のあるディスクに変更してください。
1034	エラー	操作ログの手動取り込みの処理で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4	要因ごとに次に示す対策を実施してください。 • 要因 1 get logs コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 セットアップで指定したローカルデータフォルダの空き容量を増やすか、ローカルデータフォルダを十分な空き容量

イベント番号	種類	メッセージ	要因	対処
1034	エラー	操作ログの手動取り込みの処理で、エラーが発生しました。	操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しているおそれがあります。 • 要因 6 操作ログの保管先フォルダにバックアップファイルがありません。 • 要因 7 操作ログの保管先フォルダのバックアップファイルが壊れています。	のあるディスクに変更してください。 • 要因 3 セットアップで指定した操作ログの保管先フォルダが存在し、接続できるか確認してください。 • 要因 4 セットアップで指定したユーザー名とパスワードを確認してください。 • 要因 5 セットアップで指定した操作ログの保管先フォルダの空き容量を増やすか、操作ログの保管先フォルダを十分な空き容量のあるディスクに変更してください。 • 要因 6 バックアップファイルを別のフォルダに退避している場合は、操作ログの保管先フォルダにバックアップファイルを戻したあとで、操作ログのリストアを再実行してください。 • 要因 7 操作ログの保管先フォルダの中にある詳細情報に表示されたファイルを削除してください。
1035	セキュリティ	操作ログの取り込みで、一部のデータの取り込みをスキップしました。	操作ログの保管先フォルダに、該当日のバックアップファイルがありません。	該当日のバックアップファイルを別のフォルダに退避している場合は、操作ログの保管先フォルダにバックアップファイルを戻したあとで、操作ログのリストアを再実行してください。
1036	エラー	操作ログのデータベースの拡張に失敗しました。	操作ログのデータベース格納フォルダの空き容量がありません。	不要なファイルを移動または削除したりして、ディスクの空き容量を確保してから、サービスを再起動してください。 ディスクの空き容量が十分あるにも関わらず、繰り返し発生する場合は、<code>get logs</code> コマンドでトラブルシューティング用情報を取得したあと、サポートサービスへ連絡してください。

イベント番号	種類	メッセージ	要因	対処
1037	エラー	Active Directory サーバからの機器情報および組織情報の取得に失敗しました。	• 要因 1 Active Directory サーバとの接続に失敗しました。 • 要因 2 Active Directory サーバとの認証に失敗しました。 • 要因 3 指定されたドメインが見つかりませんでした。 • 要因 4 Active Directory サーバに指定された OU 情報が見つかりませんでした。 • 要因 5 Active Directory サーバとの暗号化通信に失敗しました。	要因ごとに次に示す対策を実施してください。 • 要因 1 設定画面の【他システムとの接続】－【Active Directory の設定】画面で設定したホスト名とポート番号を確認してください。または、Active Directory サーバの稼働状況を確認してください。 • 要因 2 設定画面の【他システムとの接続】－【Active Directory の設定】画面で設定したユーザー ID とパスワードを確認してください。 • 要因 3 設定画面の【他システムとの接続】－【Active Directory の設定】画面で設定したドメイン名を確認してください。 • 要因 4 設定画面の【他システムとの接続】－【Active Directory の設定】画面で設定したルート OU を確認してください。 • 要因 5 設定画面の【他システムとの接続】－【Active Directory の設定】画面で設定したポート番号を確認してください。または、Active Directory サーバに証明書がインストールされているか確認してください。 [接続テスト] ボタンをクリックすると、Active Directory サーバに接続できるか確認できます。
1048	不審操作	添付ファイル付きメールの送信操作を検出しました。	添付ファイル付きメールの送信を、不審な操作として検知しました。	操作に問題がないか確認してください。
1049	不審操作	Web/FTP サーバへのファイルのアップロード操作を検出しました。	Web サーバ/FTP サーバへのファイルのアップロードを、不審な操作として検知しました。	操作に問題がないか確認してください。

イベント番号	種類	メッセージ	要因	対処
1050	不審操作	リムーバブルドライブへのファイルのコピー、移動操作を検出しました。	リムーバブルドライブへのファイルのコピーまたは移動を、不審な操作として検知しました。	操作に問題がないか確認してください。
1051	不審操作	プリンタへの大量印刷操作を検出しました。	プリンタへの大量印刷を、不審な操作として検知しました。	操作に問題がないか確認してください。
1055	エラー	サポートサービスへの接続でエラーが発生しました。	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] 画面の設定に誤りがあります。	サポートサービスサイトと接続するための情報を確認し、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] 画面の設定を修正してください。 [接続テスト] ボタンをクリックすると、サポートサービスに接続できるか確認できます。
1056	エラー	管理者へのメール通知に失敗しました。	• 要因 1 管理者にメールアドレスが設定されていません。または、メールアドレスに誤りがあります。 • 要因 2 メールサーバの設定に誤りがあります。または、メールサーバが稼働していません。 • 要因 3 メールサーバの接続に必要な認証の設定に誤りがあります。	要因ごとに次に示す対策を実施してください。 • 要因 1 設定画面の [ユーザー管理] – [ユーザーアカウントの管理] 画面で、管理者にメールアドレスを設定してください。または、正しいメールアドレスに変更してください。 • 要因 2 設定画面の [他システムとの接続] – [メールサーバの設定] 画面で、メールサーバの設定を修正してください。または、メールサーバの管理者へ連絡してください。 • 要因 3 設定画面の [他システムとの接続] – [メールサーバの設定] 画面で、メールサーバで使用する認証の設定を修正してください。
1057	エラー	ディスクの空き容量が少なくなっています。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	ディスクの空き容量が、環境情報の各ディスクの警告しきい値より少なくなりました。	ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
1058	エラー	ディスクの空き容量が非常に少なくなっています。ディスクの空き容量が不足すると、管理用サーバでデータベース	ディスクの空き容量が、環境情報の各ディスクのエラーしきい値より少なくなりました。	ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。

イベント番号	種類	メッセージ	要因	対処
1058	エラー	障害が発生するおそれがあります。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	ディスクの空き容量が、環境情報の各ディスクのエラーしきい値より少なくなりました。	ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
1059	設定	ライセンスの有効期限が近づいています。	ライセンスの有効期限が近づいていることを検知しました。	製品版のライセンスを購入してください。
1064	エラー	アカウント（ アカウント名 ）のセキュリティ対策の実施に失敗しました。	セキュリティ対策が失敗しました。	getlogs コマンドでトラブルシュート用情報を取得し、エラー要因を取り除いたあと、セキュリティ対策を実施してください。また、メッセージ通知などにより、利用者にセキュリティ対策を依頼してください。
1065	エラー	該当する機器にすでに適用されているグループポリシーと異なるため、アカウント（ アカウント名 ）のセキュリティ対策を実施できませんでした。ポリシーおよびセキュリティ対策内容を確認してください。	セキュリティ対策を実施しようとしたが、すでに適用されているグループポリシーと異なっていました。	適用済みのセキュリティポリシーおよびセキュリティ対策の内容を確認してください。
1071	エラー	セキュリティ対策の実施に失敗しました。管理者がトラブルシュート情報収集コマンドでトラブルシュート情報を採取しエラー要因を取り除いたあと、セキュリティ対策を実施してください。	セキュリティ対策が失敗しました。	getlogs コマンドでトラブルシュート用情報を取得し、エラー要因を取り除いたあと、セキュリティ対策を実施してください。また、メッセージ通知などにより、利用者にセキュリティ対策を依頼してください。
1072	エラー	該当する機器にすでに適用されているグループポリシーと異なるため、セキュリティ対策を実施できませんでした。セキュリティポリシーおよびセキュリティ対策内容を確認してください。	セキュリティ対策を実施しようとしたが、すでに適用されているグループポリシーと異なっていました。	適用済みのセキュリティポリシーおよびセキュリティ対策の内容を確認してください。
1076	セキュリティ	操作ログを破棄しました。	- 要因 1 エージェントの日付と時刻の設定に誤りがあります。 - 要因 2 エージェントが管理用サーバに長期間接続できませんでした。	要因ごとに次に示す対策を実施してください。 - 要因 1 エージェントの日付と時刻の設定を確認してください。 - 要因 2

イベント番号	種類	メッセージ	要因	対処
1076	セキュリティ	操作ログを破棄しました。	• 要因 1 エージェントの日付と時刻の設定に誤りがあります。 • 要因 2 エージェントが管理用サーバに長期間接続できませんでした。	エージェントが管理用サーバに定期的に接続できるか確認してください。
1085	設定	ネットワークモニタの有効化に失敗しました。	ネットワークモニタの有効化に失敗しました。	インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\JDNINMA\JDNINS01.log」に出力されます。
1086	設定	ネットワークモニタの無効化に失敗しました。	ネットワークモニタの無効化に失敗しました。	インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\JDNINMA\JDNINS01.log」に出力されます。
1088	エラー	認証に失敗したため、AMT による電源制御ができませんでした。	設定された AMT の admin パスワードで AMT にアクセスした際に、認証エラーとなりました。	AMT の設定の画面の設定内容を見直すか、以下の URL にアクセスして AMT の認証情報を変更してください。 http://ホスト名:16992
1089	エラー	認証に失敗したため、AMT の設定ができませんでした。	設定された AMT の admin パスワードで AMT にアクセスした際に、認証エラーとなりました。	[AMT の設定]画面の[admin パスワード]の設定内容を見直すか、以下の URL にアクセスして AMT の認証情報を変更してください。 http://ホスト名:16992
1090	エラー	操作ログのデータフォルダのディスク空き容量が少なくなっています。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	サイトサーバの操作ログ格納用のディスク空き容量が少なくなっています。	ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。

イベント番号	種類	メッセージ	要因	対処
1091	エラー	操作ログのデータフォルダのディスク空き容量が非常に少なくなっているため、操作ログを取得するサービスを停止しました。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	サイトサーバの操作ログ格納用のディスク空き容量が非常に少なくなっています。	ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
1094	エラー	データフォルダのディスク空き容量が少なくなっています。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	サイトサーバのデータフォルダの空き容量が少なくなっています。	ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
1095	エラー	データフォルダのディスク空き容量が非常に少なくなっているため、パッケージをサイトサーバにダウンロードできません。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。	サイトサーバのデータフォルダの空き容量が非常に少なくなっています。	ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
1100	エラー	サイトサーバプログラムのインストールに失敗しました。	サイトサーバプログラムのインストールに失敗しました。	インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\JDNINST\JDNINS01.log」に出力されます。 それでも解決できない場合は、トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
1101	エラー	サイトサーバプログラムのアンインストールに失敗しました。	サイトサーバプログラムのアンインストールに失敗しました。	インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\JDNINST

イベント番号	種類	メッセージ	要因	対処
1101	エラー	サイトサーバプログラムのアンインストールに失敗しました。	サイトサーバプログラムのアンインストールに失敗しました。	¥[JDNINS01.log] に出力されます。 それでも解決できない場合は、トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
1103	エラー	サイトサーバで、データベースへのアクセスエラーが発生しています。	データベースのサービス (JP1_ITDM2_DB Service) が開始されていないことが考えられます。	サイトサーバ上でデータベースのサービス (JP1_ITDM2_DB Service) を開始してください。
1105	設定	ネットワークモニタの有効化に失敗しました。	• 要因 1 併存できない製品がインストールされています。 • 要因 2 インストーラの実行中です。 • 要因 3 ネットワークモニタエージェントのインストール先フォルダ配下の、フォルダまたはファイルが使用中です。	要因ごとに次に示す対策を実施してください。 • 要因 1 併存できない製品をアンインストールしたあとで、インストールを再実行してください。 • 要因 2 しばらく時間をおいてから [操作メニュー] の [ネットワークモニタを有効にする] を選択して有効化を再実行してください。それでも解決できない場合は、トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 3 インストール先フォルダ配下のフォルダまたはファイルを閉じたあとで、[操作メニュー] の [ネットワークモニタを有効にする] を選択して有効化を再実行してください。
1106	エラー	サイトサーバプログラムのインストールに失敗しました。	• 要因 1 併存できない製品がインストールされています。 • 要因 2 インストーラの実行中です。 • 要因 3 サイトサーバプログラムのインストール先フォルダ配下の、	要因ごとに次に示す対策を実施してください。 • 要因 1 併存できない製品をアンインストールしたあとで、インストールを再実行してください。 • 要因 2 しばらく時間をおいてから [操作メニュー] の [サイト

イベント番号	種類	メッセージ	要因	対処
1106	エラー	サイトサーバプログラムのインストールに失敗しました。	フォルダまたはファイルが使用中です。 • 要因 4 インストール先フォルダの空き容量が不足しています。 • 要因 5 データベースフォルダの空き容量が不足しています。 • 要因 6 サポート対象外の OS です。	サーバプログラムをインストールする]を選択してインストールを再実行してください。それでも解決できない場合は、トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 3 サイトサーバのインストール先フォルダ配下の、フォルダまたはファイルが使用中です。次に示すタイミングで、[操作メニュー] の [サイトサーバプログラムをインストールする] を選択してインストールを再実行してください。 • インストール先フォルダ配下のフォルダまたはファイルを閉じたあと • サイトサーバで実行中のコマンド、プログラム、またはセットアップが終了したあと • 要因 4 インストール先フォルダの空き容量を増やしたあとで、[操作メニュー] の [サイトサーバプログラムをインストールする] を選択してインストールを再実行してください。 • 要因 5 データベースフォルダの空き容量を増やしたあとで、[操作メニュー] の [サイトサーバプログラムをインストールする] を選択してインストールを再実行してください。 • 要因 6 サポートされている OS でインストールを実行してください。
1111	エラー	スマートデバイスのロックに失敗しました。	• 要因 1	要因ごとに次に示す対策を実施してください。

イベント番号	種類	メッセージ	要因	対処
1111	エラー	スマートデバイスのロックに失敗しました。	MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4 MDM システムの管理下に、管理対象のスマートデバイスが存在しません。 • 要因 5 MDM 連携でエラーが発生しました。 • 要因 6 MDM サーバの設定情報の取得中にエラーが発生しました。	• 要因 1 MDM 連携の設定に指定した MDM サーバおよびプロキシサーバのホスト名、IP アドレス、ポート番号を確認してください。また、MDM サーバの稼働状況を確認してください。 • 要因 2 MDM 連携の設定に指定した MDM サーバのユーザー ID、パスワードを確認してください。 • 要因 3 MDM 連携の設定に指定したプロキシサーバのユーザー ID、パスワード、IP アドレス、ポート番号を確認してください。 • 要因 4 MDM サーバにスマートデバイスを登録して、情報を取得してください。 • 要因 5 トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 6 設定画面の [MDM 連携の設定] 画面で、MDM 連携の設定情報が削除されていないか確認してください。
1113	エラー	スマートデバイスのパスコードのリセットに失敗しました。	• 要因 1 MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4	要因ごとに次に示す対策を実施してください。 • 要因 1 MDM 連携の設定に指定した MDM サーバおよびプロキシサーバのホスト名、IP アドレス、ポート番号を確認してください。また、MDM サーバの稼働状況を確認してください。 • 要因 2

イベント番号	種類	メッセージ	要因	対処
1113	エラー	スマートデバイスのパスコードのリセットに失敗しました。	MDM システムの管理下に、管理対象のスマートデバイスが存在しません。 • 要因 5 MDM 連携でエラーが発生しました。 • 要因 6 MDM サーバの設定情報の取得中にエラーが発生しました。	MDM 連携の設定に指定した MDM サーバのユーザー ID、パスワードを確認してください。 • 要因 3 MDM 連携の設定に指定したプロキシサーバのユーザー ID、パスワード、IP アドレス、ポート番号を確認してください。 • 要因 4 MDM サーバにスマートデバイスを登録して、情報を取得してください。 • 要因 5 トラブルシュート用情報を取得し、サポートサービスへ連絡してください。 • 要因 6 設定画面の [MDM 連携の設定] 画面で、MDM 連携の設定情報が削除されていないか確認してください。
1115	エラー	スマートデバイスの初期化に失敗しました。	• 要因 1 MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4 MDM システムの管理下に、管理対象のスマートデバイスが存在しません。 • 要因 5 MDM 連携でエラーが発生しました。 • 要因 6 MDM サーバの設定情報の取得中にエラーが発生しました。	要因ごとに次に示す対策を実施してください。 • 要因 1 MDM 連携の設定に指定した MDM サーバのホスト名とポート番号、およびプロキシサーバのホスト名とポート番号を確認してください。また、MDM サーバの稼働状況を確認してください。 • 要因 2 MDM 連携の設定に指定した MDM サーバのユーザー ID、パスワードを確認してください。 • 要因 3 MDM 連携の設定に指定したプロキシサーバのユーザー ID、パスワード、IP アドレス、ポート番号を確認してください。 • 要因 4

イベント番号	種類	メッセージ	要因	対処
1115	エラー	スマートデバイスの初期化に失敗しました。	• 要因 1 MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4 MDM システムの管理下に、管理対象のスマートデバイスが存在しません。 • 要因 5 MDM 連携でエラーが発生しました。 • 要因 6 MDM サーバの設定情報の取得中にエラーが発生しました。	MDM サーバにスマートデバイスを登録して、情報を取得してください。 • 要因 5 トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 6 設定画面の [MDM 連携の設定] 画面で、MDM 連携の設定情報が削除されていないか確認してください。
1116	エラー	スマートデバイスの削除に失敗しました。	データベースへのアクセスエラーが発生した可能性があります。	設定画面の [管理対象機器] 画面から削除する機器を選択して、削除を実行してください。
1118	エラー	MDM システム（製品名）との機器情報の同期に失敗しました。	• 要因 1 MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4 MDM 連携でエラーが発生しました。 • 要因 5 MDM サーバの設定情報の取得中にエラーが発生しました。	要因ごとに次に示す対策を実施してください。 • 要因 1 MDM 連携の設定に指定した MDM サーバおよびプロキシサーバのホスト名、IP アドレス、ポート番号を確認してください。また、MDM サーバの稼働状況を確認してください。 • 要因 2 MDM 連携の設定に指定した MDM サーバのユーザー ID、パスワードを確認してください。 • 要因 3 MDM 連携の設定に指定したプロキシサーバのユーザー ID、パスワード、IP アドレス、ポート番号を確認してください。 • 要因 4

イベント番号	種類	メッセージ	要因	対処
1118	エラー	MDM システム（製品名）との機器情報の同期に失敗しました。	• 要因 1 MDM サーバ、およびプロキシサーバとの接続に失敗しました。 • 要因 2 MDM サーバとの認証に失敗しました。 • 要因 3 プロキシサーバとの認証に失敗しました。 • 要因 4 MDM 連携でエラーが発生しました。 • 要因 5 MDM サーバの設定情報の取得中にエラーが発生しました。	トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 5 設定画面の [MDM 連携の設定] 画面で、MDM 連携の設定情報が削除されていないか確認してください。
1132	エラー	変更履歴の取得中に致命的なエラーが発生しました。	内部エラーが発生しました。	トラブルシュート用情報を取得し、サポートサービスへ連絡します。
1133	エラー	保存用の変更履歴のファイル出力に失敗しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 変更履歴の保管先が存在しない、または接続できません。 • 要因 3 変更履歴の保管先に接続するためのユーザー名、またはパスワードが間違っています。 • 要因 4 変更履歴の保管先のディスク容量が不足している可能性があります。	要因ごとに次に示す対策を実施してください。 • 要因 1 トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 変更履歴の保管先が存在し、接続できるか確認してください。 • 要因 3 セットアップで指定したユーザー名、パスワードを確認してください。 • 要因 4 セットアップで指定した変更履歴の保管先の空き容量を増やすか、変更履歴の保管先を十分な空き容量のあるディスクに変更してください。
1138	エラー	操作ログを定期的にエクスポートする処理で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2	要因ごとに次に示す対策を実施してください。 • 要因 1

イベント番号	種類	メッセージ	要因	対処
1138	エラー	操作ログを定期的にエクスポートする処理で、エラーが発生しました。	ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しています。	<code>get logs</code> コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 セットアップで指定したローカルデータフォルダの空き容量を増やすか、ローカルデータフォルダを十分な空き容量のあるディスクに変更してください。 • 要因 3 セットアップで指定した操作ログの保管先フォルダが存在し、接続できるか確認してください。 • 要因 4 セットアップで指定したユーザー名とパスワードを確認してください。 • 要因 5 セットアップで指定した操作ログの保管先フォルダの空き容量を増やすか、操作ログの保管先フォルダを十分な空き容量のあるディスクに変更してください。
1139	エラー	操作ログの自動取り込み処理で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しています。	要因ごとに次に示す対策を実施してください。 • 要因 1 <code>get logs</code> コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 セットアップで指定したローカルデータフォルダの空き容量を増やすか、ローカルデータフォルダを十分な空き容量のあるディスクに変更してください。 • 要因 3 セットアップで指定した操作ログの保管先フォルダが存在し、接続できるか確認してください。

イベント番号	種類	メッセージ	要因	対処
1139	エラー	操作ログの自動取り込み処理で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しています。	• 要因 4 セットアップで指定したユーザー名とパスワードを確認してください。 • 要因 5 セットアップで指定した操作ログの保管先フォルダの空き容量を増やすか、操作ログの保管先フォルダを十分な空き容量のあるディスクに変更してください。
1140	エラー	操作ログの日付情報の更新で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しています。	要因ごとに次に示す対策を実施してください。 • 要因 1 <code>get logs</code> コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 • 要因 2 セットアップで指定したローカルデータフォルダの空き容量を増やすか、ローカルデータフォルダを十分な空き容量のあるディスクに変更してください。 • 要因 3 セットアップで指定した操作ログの保管先フォルダが存在し、接続できるか確認してください。 • 要因 4 セットアップで指定したユーザー名とパスワードを確認してください。 • 要因 5 セットアップで指定した操作ログの保管先フォルダの空き容量を増やすか、操作ログの保管先フォルダを十分な空き

イベント番号	種類	メッセージ	要因	対処
1140	エラー	操作ログの日付情報の更新で、エラーが発生しました。	• 要因 1 内部エラーが発生しました。 • 要因 2 ローカルデータフォルダのディスク容量が不足しているおそれがあります。 • 要因 3 操作ログの保管先フォルダが存在しない、または接続できません。 • 要因 4 操作ログの保管先フォルダに接続するためのユーザー名、またはパスワードが間違っています。 • 要因 5 操作ログの保管先フォルダのディスク容量が不足しています。	容量のあるディスクに変更してください。

エラー発生時に出力されるログファイルを次の表に示します。

ログの種類	出力先	ファイル名	説明
公開メッセージログファイル	JP1/IT Desktop Management 2 のインストール先フォルダ¥mgr¥log	JDNMAINn.log※ (n=1～9)	JP1/IT Desktop Management 2 の動作状況を確認できる情報が出力されます。
イベントログ	OS のイベントログ	—	JP1/IT Desktop Management 2 の起動と停止、および致命的エラーが出力されます。致命的エラーには、公開メッセージログファイルに出力されない情報が含まれます。イベントログは、OS のイベントビューアで確認してください。

(凡例) —：該当なし

注※ 世代管理されています。ログのファイルサイズの上限を超えた場合、番号を 1 つ繰り上げたファイルが作成されます。番号は 1 から開始されます。番号が 9 になった場合は 1 に戻ります。

必要に応じて、`getlogs` コマンドでトラブルシューティング用情報を取得してください。`getlogs` コマンドについては、「[17.25 getlogs \(トラブルシューティング用情報の取得\)](#)」を参照してください。

関連リンク

- [13.1 イベントの詳細を確認する手順](#)

18.10 エージェントのトラブルシューティング手順

エージェントでトラブルが発生した場合の対処方法、およびトラブルシュート用情報の採取方法について説明します。

なお、JP1/IT Desktop Management 2 - Agent を配信してインストールしたときのエラー内容については、イベント画面で確認してください。

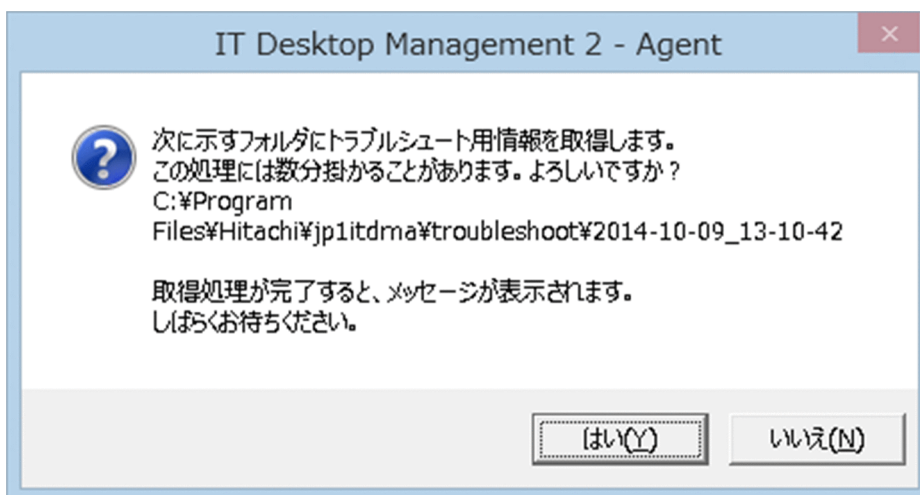
エージェントのトラブルシュート用情報を採取するには：

トラブルシュート用情報の採取は、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。

オフライン管理用のエージェントがインストールされているコンピュータでトラブルが発生した場合は、次に示す手順で採取できる情報のほかに、情報収集用ツールで生成された「Data」フォルダ以下のファイルも採取してください。

1.getlogs.vbs をダブルクリックする

トラブルシュート用情報の取得を確認するダイアログが表示されます。

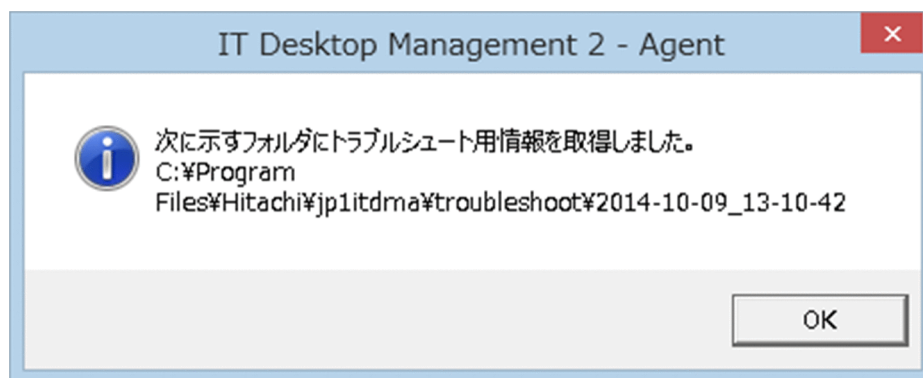


getlogs.vbs の格納場所を次に示します。

JP1/IT Desktop Management 2 - Agent のインストール先フォルダ¥bin

2. [はい] ボタンをクリックする

トラブルシュート用情報の採取が開始されます。トラブルシュート用情報の採取が終了すると、トラブルシュート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。このダイアログには、トラブルシュート用情報の格納先が表示されます。



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。

JP1/IT Desktop Management 2 - 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	JP1/IT Desktop Management 2 - Agent 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 - ファイル情報 JP1/IT Desktop Management 2 - Agent 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

セキュリティの自動対策で変更した設定を元に戻すには：

セキュリティポリシーの適用やセキュリティの自動対策で変更した、管理対象コンピュータのセキュリティ設定項目を、変更前の状態に戻す手順を次の表に示します。

セキュリティ設定項目	対処方法
更新プログラム	次の 2 点を実施してください。 - 該当のコンピュータで、手動で更新プログラムをアンインストールする。 - Windows のコントロールパネルで「自動更新」を起動し、元の設定に戻す。

セキュリティ設定項目	対処方法
使用ソフトウェア	次の2点を実施してください。 • 必須ソフトウェアをインストールした場合、必要に応じてアンインストールする。 • 使用禁止ソフトウェアをアンインストールした場合、必要に応じてインストールする。
サービスのセキュリティ設定	Windows のコントロールパネルで [管理ツール] を起動し、[サービス] をダブルクリックします。禁止したサービスの設定を元に戻してください。
OS のセキュリティ設定	次の設定内容を確認して、変更してください。なお、具体的な変更方法は設定内容や OS によって異なります。 • [マイコンピュータ] の [プロパティ] の設定 • [画面のプロパティ] の設定 • [コントロールパネル] の [管理ツール] の設定 • エクスプローラの設定 • レジストリエディタでの編集内容
禁止操作（使用抑止と起動抑止の設定）	エージェントのプログラムをアンインストールします。

18.11 リモートコントロール時のトラブルシューティング

コントローラ側でコンピュータの画面が表示されない

Java2 で作成されたアプリケーションを接続先のコンピュータで起動した場合、Direct Draw を使用して描画するため、コントローラ側でコンピュータの画面が表示されないことがあります。

対処方法

コンピュータで Java2 起動時に次のオプションを指定して、Direct Draw を使用しないようにします。

```
-Dsun.java2d.noddraw=true
```

エージェントのインストール後に Windows 7、Windows Server 2008、Windows Vista、Windows Server 2003、または Windows XP が起動しない

他社のリモートコントロール製品がインストールされている場合、エージェントをインストールしたあとで Windows 7、Windows Server 2008、Windows Vista、Windows Server 2003、または Windows XP が起動しなくなることがあります。

対処方法

他社のリモートコントロール製品をアンインストールしてから、エージェントを再インストールする手順を次に示します。

1. OS をセーフモードで起動してから、エージェントをアンインストールします。
2. コンピュータを再起動します。
3. 他社のリモートコントロール製品がインストールされている場合は、アンインストールします。
4. コンピュータを再起動します。
5. エージェントを再度インストールします。

コンピュータをセーフモードで起動する手順を次に示します。

1. コンピュータを再起動します。
2. 画面のいちばん下に、[F8] キーを押して起動オプションを表示するように求めるメッセージが表示されたら、[F8] キーを押します。
3. 方向キーを使用して、[セーフモード] を選択し、[Enter] キーを押します。
4. 方向キーを使用して、起動する OS を選択します。

18.12 ネットワーク制御時のトラブルシューティング

遮断した機器のネットワーク接続を許可したが、すぐにネットワークに接続できない

ネットワーク接続が遮断された機器に対して、機器画面から手動でネットワーク接続を許可しても、ネットワークに接続できるようになるまで数分掛かることがあります。

対処方法

ネットワークに接続できるようになるまで、しばらくお待ちください。それでもネットワークに接続できない場合は、利用者のコンピュータを再起動してください。

すべての機器がネットワークに接続できない

ホワイトリスト方式を利用する場合、ルータのネットワーク接続を許可しないと、ネットワークが利用できなくなります。

対処方法

ルータが遮断されると管理用サーバとの通信ができないため、ネットワークモニタ設定を変更できません。この場合、ネットワークモニタを有効にしたコンピュータで、Windows の [コントロールパネル] - [管理ツール] - [サービス] のサービス「JP1_ITDM2_Network Monitor」（サービス表示名：NXNetMonitor）を停止してください。そのあと、管理用サーバと接続して、ネットワーク制御リストの設定を変更してください。なお、ルータによっては再起動が必要になる場合があります。

関連リンク

- [8.7.2 ネットワーク制御リストの機器を編集する手順](#)

18.13 Active Directory 連携時のトラブルシューティング手順

Active Directory 連携時に、セキュリティポリシーでセキュリティ設定を自動対策しても、「該当する機器にすでに適用されているグループポリシーと異なるため、自動対策が失敗した」旨のイベントが発生することがあります。

対処方法

この場合は、Active Directory のグループポリシーの設定と JP1/IT Desktop Management 2 のセキュリティポリシーの設定が相反しているおそれがあります。JP1/IT Desktop Management 2 よりも Active Directory の設定が優先されるため、必要に応じて Active Directory のグループポリシーの設定を変更してください。

Active Directory のグループポリシーの設定を確認するには：

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. [名前] に「gpedit.msc」と入力します。
3. 起動したグループポリシーで [ローカル コンピュータ ポリシー] - [コンピュータの構成] - [Windows の設定] - [セキュリティの設定] の順に選択します。

Active Directory のグループポリシーが表示されます。設定を確認してください。

18.14 MDM 連携時のトラブルシューティング

スマートデバイスの情報が更新されない

接続先の MDM システムの認証情報が正しく設定されていない場合、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「1108」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。

18.15 JP1/IM 連携時のトラブルシューティング

JP1/IM 連携構成システム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。

JP1/IM にイベントが通知されない

JP1/IT Desktop Management 2 と JP1/Base とが通信できていない場合、JP1/IM にイベントは通知されません。

対処方法

イベント番号「1120」のイベント、またはメッセージ ID「KDEX6511-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、構築手順を確認して設定を見直してください。

18.16 データベース障害のトラブルシューティング

データベース接続エラーが発生する

データベース接続エラーが発生する場合、次の原因が考えられます。

1. データベースが停止状態または開始中の状態である。
2. データベースが閉塞状態である。

対処方法

- 1.の場合は、`stopservice` コマンドおよび`startservice` コマンドを使用して、管理用サーバのサービスを開始してください。
- 2.の場合は、JP1/IT Desktop Management 2 セットアップで、データベースを初期化してください。

データベースのバックアップ、リストア、再編成に失敗する

データベースのバックアップ、リストア、再編成に失敗する場合、次の原因が考えられます。

1. データベースの格納フォルダに対するアクセス権限がない。
2. I/O エラーが発生した。

対処方法

- 1.の場合は、データベースの格納フォルダに対するアクセス権限を確認してください。
- 2.の場合は、ディスク障害が発生していないことを確認してください。

関連リンク

- [17.23 stopservice \(サービス停止\)](#)
- [17.24 startservice \(サービス開始\)](#)

19

イベント

ここでは、JP1/IT Desktop Management 2 のイベントを一覧で説明します。

19.1 イベント一覧

イベント番号	重要度	イベントの内容
0	情報	機器が発見されました。 機器種別 = 機種種別 機種種別で表示される内容を、次に示します。 • PC • サーバ • ネットワーク装置 • プリンタ • スマートデバイス • ストレージ • USB デバイス • ディスプレイ • 周辺装置 • その他 • 不明な機器 • (ユーザー定義)
1	情報	機器が管理対象として追加されました。 機器種別 = 機種種別 機種種別で表示される内容を、次に示します。 • PC • サーバ • ネットワーク装置 • プリンタ • スマートデバイス • ストレージ • USB デバイス • ディスプレイ • 周辺装置 • その他 • 不明な機器 • (ユーザー定義)
2	情報	機器の状態が管理対象外に変更されました。
3	情報	機器が削除されました。
4	警戒	ライセンス数を超過したため管理対象の機器として登録できませんでした。 管理台数分のライセンスを購入してください。 機器種別 = 機種種別

イベント番号	重要度	イベントの内容
4	警戒	機種種別で表示される内容を、次に示します。 • PC • サーバ • ネットワーク装置 • プリンタ • スマートデバイス • ストレージ • USB デバイス • ディスプレイ • 周辺装置 • その他 • 不明な機器 • (ユーザー定義)
5	警戒	エージェントがアンインストールされました。 該当する機器のエージェントをアンインストールしてもよいかどうかを確認してください。
6	情報	エージェント設定の内容が更新されました。 エージェント設定名 = エージェント設定名
7	情報	メモリ容量が変更されました。 変更前 = メモリ容量 変更後 = メモリ容量
8	情報	ハードウェアが追加されました。 インタフェース種別 = インタフェース種別 モデル名 = モデル名 容量 = 容量
9	情報	ハードウェアが削除されました。 インタフェース種別 = インタフェース種別 モデル名 = モデル名 容量 = 容量
19	警戒	機能名で詳細情報を取得できませんでした。 認証情報、探索範囲などの設定内容、サービス (JP1_ITDM2_Agent Control) の稼働状況を確認してください。または、対象機器 (クライアント) の状態を確認してください。確認完了後、機器の探索や機器情報の収集を再実行してください。それでも解決できない場合は、トラブルシューティング情報収集コマンドでトラブルシューティング情報を収集したあと、サポートサービスへ連絡してください。 エラー要因 = エラー要因 IP アドレス = IP アドレス 機能名で表示される内容を、次に示します。 • 機器の探索

イベント番号	重要度	イベントの内容
19	警戒	・ インベントリ収集 ・ オンデマンドのインベントリ収集 エラー要因で表示される内容を、次に示します。 ・ ユーザ認証に失敗しました ・ 管理共有に接続できませんでした ・ 管理共有にアクセス中にエラーが発生しました ・ クライアントに接続できませんでした ・ 通信エラーが発生しました ・ クライアントでエラーが発生しました ・ 機器探索用のプログラムが現在実行中です ・ 機器探索用のプログラムが終了しませんでした
22	情報	エージェントのインストーラを起動しました。 形名 = 形名 バージョン = バージョン IP アドレス = IP アドレス
56	情報	利用者へメッセージ通知しました。
57	警戒	利用者へのメッセージ通知に失敗しました。 トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
58	情報	ネットワークへの接続を拒否しました。
60	情報	ネットワークへの接続を許可しました。
62	情報	ウィルス対策製品のセキュリティポリシーの設定が変更されました。 製品名 = 製品名 ウィルス対策製品のバージョン = エンジンバージョン 定義ファイルバージョン = 定義ファイルバージョン
63	情報	更新プログラム情報を追加しました。 更新プログラム情報 = 更新プログラム情報
69	情報	セキュリティポリシーが追加されました。 セキュリティポリシー名 = セキュリティポリシー名
70	情報	セキュリティポリシーの内容が更新されました。 セキュリティポリシー名 = セキュリティポリシー名
71	情報	セキュリティポリシーが削除されました。 セキュリティポリシー名 = セキュリティポリシー名

イベント番号	重要度	イベントの内容
72	情報	セキュリティポリシーの割り当てが変更されました。 セキュリティポリシー名 = セキュリティポリシー名 割り当てグループ = 割り当てグループ
75	情報	ソフトウェアの起動を抑止しました。 実行アカウント名 = 実行アカウント名 ログオンアカウント名 = ログインユーザー名 製品名 = 製品名 製品バージョン = バージョン ファイル名 = ファイル名
76	情報	印刷操作を抑止しました。 ログオンアカウント名 = ログオンユーザー名 プリンタ名 = プリンタ名 印刷ドキュメント名 = 印刷ドキュメント名
77	情報	印刷操作の抑止を解除しました。 ログオンアカウント名 = ログオンユーザー名
78	警戒	印刷操作の抑止を解除できませんでした。 正しいパスワードを確認し、印刷操作の抑止を解除してください。 ログオンアカウント名 = ログオンユーザー名
200※	緊急	サービス (JP1_ITDM2_Service) でエラーが発生しました。サービス (JP1_ITDM2_Service) を停止します。 トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。 エラーコード=エラーコード
208	警戒	受信ファイルの更新処理で、一時的なエラーが発生しました。更新処理をリトライします。
209	警戒	機能名でエラーが発生しました。 機能名処理で内部エラーが発生しました。エラーが繰り返し発生する場合は、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。 エラーコード = エラーコード IP アドレス = IP アドレス 機能名で表示される内容を、次に示します。 - 機器の探索 - インベントリ収集 - オンデマンドのインベントリ収集 - エージェントの配信
210	警戒	受信ファイルの更新処理でエラーが発生したため、更新できませんでした。 受信ファイルの更新に失敗し、回復が見込めないため、更新処理を行いませんでした。リソースが不足が発生しているおそれがあります。

イベント番号	重要度	イベントの内容
210	警戒	エラーが繰り返し発生する場合は、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
211	警戒	フォーマットが不正なファイルを受信したため、更新できませんでした。 不正なファイルを受信したため、情報を更新できませんでした。 取得元のデータに特殊文字（制御コードなど）が含まれているおそれがあります。取得元のデータの特殊文字を取り除いて情報を再取得してください。 エラーが繰り返し発生する場合は、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
212	警戒	受信ファイルのサイズがデータベースの更新可能サイズをオーバーしたため、更新できませんでした。 受信ファイルのサイズがデータベースの更新可能サイズを超えたため、更新できませんでした。 エラーが繰り返し発生する場合は、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
1003	警戒	エージェントの環境が壊れました。 エージェントのファイル削除など、エージェント実行環境が壊れています。利用者による意図的な削除などが考えられます。
1004	情報	新しいソフトウェアが発見されました。 ソフトウェア名称 = ソフトウェア名称 バージョン = バージョン
1006	警戒	使用禁止サービスを停止できませんでした。 サービス名 = サービス名
1007	情報	ウィルス対策製品の情報が追加されました。
1008	情報	エージェントのバージョンを更新しました。 エージェントバージョン = エージェントバージョン
1009	情報	マネージャの動作定義ファイルを更新しました。
1011	情報	操作の抑止対象のデバイスを切断しました。 ログオンアカウント名 = ログオンアカウント名 ドライブ名 = ドライブ名 ドライブ種別 = ドライブ種別 デバイス名 = デバイス名 デバイスインスタンス ID = デバイスインスタンス ID デバイス区分 = デバイス区分 ドライブ種別で表示される内容を、次に示します。 • 不明 • ローカルディスク • ネットワークドライブ

イベント番号	重要度	イベントの内容
1011	情報	・ リムーバブルディスク ・ CD-ROM ドライブ ・ RAM ディスク デバイス区分で表示される内容を、次に示します。 ・ 不明 ・ USB デバイス ・ 内蔵 CD/DVD ドライブ ・ 内蔵 FD ドライブ ・ IEEE1394 デバイス ・ 内蔵 SD カード ・ Bluetooth デバイス ・ イメージングデバイス ・ Windows ポータブルデバイス
1016	情報	使用必須ソフトウェアを配布します。 使用必須ソフトウェアがインストールされていない管理機器に対して、セキュリティポリシーの設定に従ってソフトウェアの配布処理を開始しました。タスクの実行状況はポリシーベースタスク名で確認できます。
1017	情報	使用禁止ソフトウェアを削除します。 使用禁止ソフトウェアを発見したため、セキュリティポリシーの設定に従ってソフトウェアを削除します。タスクの実行状況はポリシーベースタスク名で確認できます。
1018	警戒	パッケージ配布タスクがエラー終了しました。 エージェント対象エージェントホスト名へのタスクタスク名称がエラー終了しました。 エラー要因：エラー要因 エラー要因で表示される内容を、次に示します。 ・ ディスクの空き容量が不足しています。 ・ フォルダまたはファイルにアクセスできません。 ・ 指定した機器が、タスクの実行対象から外れました。 ・ 内部エラーが発生しました ・ パッケージに登録された ZIP ファイルの解凍に失敗しました。 ・ コマンドが起動しません。 ・ コマンドの処理を中止しました。 ・ コマンドが異常終了しました
1019	警戒	アンインストールタスクがエラー終了しました。 エージェント対象エージェントホスト名へのタスクタスク名称がエラー終了しました。 エラー要因：エラー要因 エラー要因で表示される内容を、次に示します。 ・ ディスクの空き容量が不足しています。

イベント番号	重要度	イベントの内容
1019	警戒	- フォルダまたはファイルにアクセスできません。 - 指定した機器が、タスクの実行対象から外れました。 - 内部エラーが発生しました - コマンドが起動しません。 - コマンドの処理を中止しました。 - コマンドが異常終了しました
1020	情報	タスクタスク名称が実行スケジュールにしたがって実行されました。 スケジュール設定されていたタスクタスク名称が実施時刻実行開始時刻になったため、処理を開始しました。
1021	情報	管理者が実行するタスクタスク名称が完了しました。 管理者が実行するタスクタスク名称が完了しました。結果を確認してください。 エラー数 = エラーノード数
1022	情報	未確認のハードウェア資産(機器種別)が登録されました。 未確認のハードウェア資産(機器種別)が登録されました。資産登録を行ってください。 機器種別で表示される内容を、次に示します。 - PC - サーバ - ネットワーク装置 - プリンタ - スマートデバイス - ストレージ - USB デバイス - ディスプレイ - 周辺装置 - その他 - 不明な機器 (ユーザー定義)
1028	情報	ネットワークの探索が終了しました。
1029	情報	Active Directory との同期が完了しました。
1032※	警戒	操作ログの保管でエラーが発生しました。 エラー要因 エラー要因で表示される内容を、次に示します。 - 内部エラーが発生しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。 - データフォルダまたはローカルデータフォルダで I/O エラーが発生しました。データフォルダまたはローカルデータフォルダにアクセスできること、および空き容量が不足していないことを確認してください。

イベント番号	重要度	イベントの内容
1032※	警戒	- 操作ログの保管先フォルダに接続できませんでした。セットアップで指定した操作ログの保管先フォルダが存在し、接続できることを確認してください。 - 操作ログの保管先フォルダへの認証に失敗しました。セットアップで指定したユーザー名およびパスワードで、操作ログの保管先フォルダに接続できることを確認してください。 - 操作ログの保管先フォルダで I/O エラーが発生しました。操作ログの保管先フォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに保管されたファイルが存在しません。保管されたファイルをほかのフォルダに退避している場合は、操作ログの保管先フォルダに保管されたファイルを戻したあと、操作ログの取り込みを再実行してください。 - セットアップで操作ログの保管先フォルダが設定されていることを確認してください。 - 管理用サーバで、共有フォルダに対する匿名アクセスが制限されているため、操作ログの保管先フォルダに接続できません。セットアップで指定したユーザー名とパスワードに対応するユーザアカウントを、管理用サーバで作成してください。
1033	情報	操作ログの手動取り込みが終了しました。 手動取り込み期間：取り込み期間開始日時～取り込み期間終了日時
1034	警戒	操作ログの手動取り込みの処理で、エラーが発生しました。 エラー要因 詳細情報 = 詳細情報 エラー要因で表示される内容を、次に示します。 - 内部エラーが発生しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。 - データフォルダまたはローカルデータフォルダで I/O エラーが発生しました。データフォルダまたはローカルデータフォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに接続できませんでした。セットアップで指定した操作ログの保管先フォルダが存在し、接続できることを確認してください。 - 操作ログの保管先フォルダへの認証に失敗しました。セットアップで指定したユーザー名およびパスワードで、操作ログの保管先フォルダに接続できることを確認してください。 - 操作ログの保管先フォルダで I/O エラーが発生しました。操作ログの保管先フォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに保管されたファイルが存在しません。保管されたファイルをほかのフォルダに退避している場合は、操作ログの保管先フォルダに保管されたファイルを戻したあと、操作ログの取り込みを再実行してください。 - セットアップで操作ログの保管先フォルダが設定されていることを確認してください。

イベント番号	重要度	イベントの内容
1034	警戒	- 管理用サーバで、共有フォルダに対する匿名アクセスが制限されているため、操作ログの保管先フォルダに接続できません。セットアップで指定したユーザー名とパスワードに対応するユーザアカウントを、管理用サーバで作成してください。 - 詳細情報に示す操作ログファイルが壊れているため、該当する操作ログファイルをデータベースに取り込めません。詳細情報に表示されている操作ログファイルを削除してください。 エラー要因がファイルの破損の場合、詳細情報には、ファイル名が表示されます。
1036※	緊急	操作ログのデータベースの拡張に失敗しました。 操作ログのデータベースの空き容量がありません。 空き容量を確保して、サービスを再起動してください。空き容量が十分ある場合で、エラーが繰り返し発生するときは、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
1037※	警戒	Active Directory サーバからの機器情報および組織情報の取得に失敗しました。 要因 [Active Directory の設定] 画面の接続テスト機能を使用して、設定を見直してください。 エラーコード=エラーコード Active Directory サーバのホスト名=ホスト名 Active Directory サーバのポート番号=ポート番号 ユーザー ID=接続アカウント ルート OU=取り込みルートパス 要因には、状況に応じてエラーの要因が表示されます。
1038	情報	エージェントの動作定義ファイルを更新しました。
1039	情報	更新プログラムを配布します。 更新プログラムが適用されていない管理対象の機器に、セキュリティポリシーの設定に従って更新プログラムを配布するタスクを開始しました。タスクの実行状況はタスク名で確認できます。
1041	警戒	更新プログラムの配布タスクでエラーが発生したため、タスクを終了しました。 エラー要因 タスク名 = タスク名 エラー要因で表示される内容を、次に示します。 - 更新プログラムを登録したパッケージが登録されていません。 - 更新プログラムのダウンロードに失敗しました。
1048	警戒	添付ファイル付きメールの送信操作を検出しました。 ログオンアカウント名 = ログオンユーザー名 持ち出しファイル数 = 持ち出しファイル数 ファイルの持ち出し先情報 = 出力先情報（あて先メールアドレス）

イベント番号	重要度	イベントの内容
1049	警戒	Web/FTP サーバへのファイルのアップロード操作を検出しました。 ログオンアカウント名 = ログオンユーザー名 持ち出しファイル数 = 持ち出しファイル数 ファイルの持ち出し先情報 = 出力先情報（送信先 URL、サーバ名）
1050	警戒	リムーバブルドライブへのファイルのコピー、移動操作を検出しました。 ログオンアカウント名 = ログオンユーザー名 持ち出しファイル数 = 持ち出しファイル数 ファイルの持ち出し先情報 = 出力先情報（ファイルパス）
1051	警戒	プリンタへの大量印刷操作を検出しました。 ログオンアカウント名 = ログオンユーザー名 印刷ページ数 = 印刷ページ数
1055※	警戒	サポートサービスへの接続でエラーが発生しました。 サポートサービスへの接続でエラーが発生しました。 エラー要因 [サポートサービスの設定] 画面の接続テスト機能を使用して、設定を見直してください。 エラー要因 には、状況に応じてエラーの要因が表示されます。
1056※	緊急	管理者へのメール通知に失敗しました。 エラー要因 [メールサーバの設定] 画面のテストメール送信機能を使用して、設定を見直してください。 エラー要因 には、状況に応じてエラーの要因が表示されます。
1057※	警戒	ディスクの空き容量が少なくなっています。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 フォルダ種別（フォルダ種別のフォルダのパス） ディスクの空き容量=フォルダ種別のフォルダの空きディスク容量
1058※	緊急	ディスクの空き容量が非常に少なくなっています。ディスクの空き容量が不足すると、管理用サーバでデータベース障害が発生するおそれがあります。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 フォルダ種別（フォルダ種別のフォルダのパス） ディスクの空き容量=フォルダ種別のフォルダの空きディスク容量
1059	警戒	製品ライセンスの有効期限が近づいています。 期限：期限日時 製品ライセンスを購入してください。
1060	情報	ソフトウェアが追加されました。 ソフトウェア = ソフトウェア名称 バージョン
1061	情報	ソフトウェアが削除されたか、ソフトウェア検索条件が変更されました。 ソフトウェア = ソフトウェア名称 バージョン

イベント番号	重要度	イベントの内容
1062	情報	ソフトウェアが更新されました。 変更前 ソフトウェア = ソフトウェア名称 バージョン 変更後 ソフトウェア = ソフトウェア名称 バージョン
1063	情報	アカウント(アカウント名)のセキュリティ対策を実施しました。 項目名 = 項目名 項目名で表示される内容を、次に示します。 - 無期限パスワードを無効にする - スクリーンセーバーのパスワード保護を有効にする - スクリーンセーバーの起動待ち時間を設定する
1064	情報	アカウント(アカウント名)のセキュリティ対策の実施に失敗しました。 項目名 = 項目名 項目名で表示される内容を、次に示します。 - 無期限パスワードを無効にする - スクリーンセーバーのパスワード保護を有効にする - スクリーンセーバーの起動待ち時間を設定する
1065	警戒	該当する機器にすでに適用されているグループポリシーと異なるため、アカウント(アカウント名)のセキュリティ対策を実施できませんでした。ポリシーおよびセキュリティ対策内容を確認してください。 項目名 = 項目名 項目名で表示される内容を、次に示します。 - 無期限パスワードを無効にする - スクリーンセーバーのパスワード保護を有効にする - スクリーンセーバーの起動待ち時間を設定する
1066	情報	セキュリティ設定が変更されました。 項目 = 項目名 変更前 = 値 変更後 = 値 項目名で表示される内容を、次に示します。 - パワーオンパスワード - Guest アカウント - 自動ログオン - 共有フォルダ - 管理共有 - DCOM - 匿名接続による情報取得の制限 - Windows ファイアウォールの設定 - Windows 自動更新 - リモートデスクトップ 値で表示される内容を、次に示します。

イベント番号	重要度	イベントの内容
1066	情報	• 無効 • 有効 • なし • あり • 不明 • 許可する • 許可しない
1067	情報	コンピュータのアカウント(アカウント名)が追加されました。 パスワード更新からの経過日数 = 経過日数日 脆弱パスワード = 脆弱パスワード パスワード無期限設定 = パスワード無期限設定 スクリーンセーバーの設定 = スクリーンセーバー設定 スクリーンセーバーのパスワード設定 = スクリーンセーバーのパスワード設定 スクリーンセーバーの起動までの待ち時間 = スクリーンセーバー起動までの待ち時間 脆弱パスワードで表示される内容を、次に示します。 • 高い • 低い パスワード無期限設定、スクリーンセーバー設定、スクリーンセーバーのパスワード設定で表示される内容を、次に示します。 • 無効 • 有効 スクリーンセーバー起動までの待ち時間には、待ち時間(秒)が表示されます。
1068	情報	コンピュータのアカウント(アカウント名)が削除されました。 パスワード更新からの経過日数 = 経過日数日 脆弱パスワード = 脆弱パスワード パスワード無期限設定 = パスワード無期限設定 スクリーンセーバーの設定 = スクリーンセーバー設定 スクリーンセーバーのパスワード設定 = スクリーンセーバーのパスワード設定 スクリーンセーバーの起動までの待ち時間 = スクリーンセーバー起動までの待ち時間 脆弱パスワードで表示される内容を、次に示します。 • 高い • 低い パスワード無期限設定、スクリーンセーバー設定、スクリーンセーバーのパスワード設定で表示される内容を、次に示します。 • 無効 • 有効 スクリーンセーバー起動までの待ち時間には、待ち時間(秒)が表示されます。

イベント番号	重要度	イベントの内容
1069	情報	コンピュータのアカウント(アカウント名)が変更されました。 項目 = 項目名 変更前 = 変更前の値 変更後 = 変更後の値 項目名で表示される内容を、次に示します。 - パスワードの安全性 - 無期限パスワード - スクリーンセーバーの設定 - スクリーンセーバーのパスワード保護 - スクリーンセーバーの起動待ち時間 変更前の値、変更後の値で表示される内容を、次に示します。 - パスワードの安全性 - 高い - 低い - 無期限パスワード、スクリーンセーバーの設定、スクリーンセーバーのパスワード保護 - 無効 - 有効 - スクリーンセーバーの起動待ち時間 - 待ち時間（秒）が表示されます。
1070	情報	セキュリティ対策を実施しました。 項目名 = 項目名 項目名で表示される内容を、次に示します。 - Guest アカウントを無効にする - 無期限パスワードを無効にする - 自動ログオンを無効にする - 共有フォルダを無効にする - 匿名接続を無効にする - Windows ファイアウォールを有効にする - Windows 自動更新を有効にする - 管理共有を無効にする - DCOM を無効にする - リモートデスクトップを無効にする - Windows 自動更新を実行する - サービスを停止して無効化する
1071	警戒	セキュリティ対策の実施に失敗しました。管理者がトラブルシューティング情報収集コマンドでトラブルシューティング情報を採取しエラー要因を取り除いたあと、セキュリティ対策を実施してください。 項目名 = 項目名 項目名で表示される内容を、次に示します。

イベント番号	重要度	イベントの内容
1071	警戒	• Guest アカウントを無効にする • 無期限パスワードを無効にする • 自動ログオンを無効にする • 共有フォルダを無効にする • 匿名接続を無効にする • Windows ファイアウォールを有効にする • Windows 自動更新を有効にする • 管理共有を無効にする • DCOM を無効にする • リモートデスクトップを無効にする • Windows 自動更新を実行する • サービスを停止して無効化する
1072	警戒	該当する機器にすでに適用されているグループポリシーと異なるため、セキュリティ対策を実施できませんでした。セキュリティポリシーおよびセキュリティ対策内容を確認してください。 項目名 = 項目名 項目名で表示される内容を、次に示します。 • Windows ファイアウォールを有効にする • Windows 自動更新を有効にする • Windows 自動更新を実行する • リモートデスクトップを無効にする
1073	情報	使用禁止サービスの起動を検知しました。 サービス名 = サービス名
1074	情報	使用禁止サービスの停止を検知しました。 サービス名 = サービス名
1075	情報	ソフトウェア辞書にエントリを追加しました。
1076	警戒	操作ログを破棄しました。 操作ログの保管期間を超えたデータを受信したため、操作ログを破棄しました。機器の日付と時刻の設定に誤りがあることが考えられます。
1077	情報	ネットワークモニタを有効化しました。 ネットワークアドレス = ネットワークアドレス
1078	情報	ネットワークモニタを無効化しました。 ネットワークアドレス = ネットワークアドレス
1079※	警戒	機器のネットワークへの接続が遮断されました。 MAC アドレス = MAC アドレス IP アドレス = IP アドレス

イベント番号	重要度	イベントの内容
1081	情報	ネットワークモニタの処理を開始しました。
1082※	警戒	ネットワークモニタの処理を停止しました。
1085	警戒	ネットワークモニタの有効化に失敗しました。 インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\%JDINMA%\JDININS01.log」に出力されます。 ネットワークアドレス=ネットワークアドレス
1086	警戒	ネットワークモニタの無効化に失敗しました。 インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\%JDINMA%\JDININS01.log」に出力されます。 ネットワークアドレス=ネットワークアドレス
1087	情報	資産情報のインポートが正常に終了しました。 資産種別 = 資産種別 追加した件数 = 件数 更新した件数 = 件数 エラー件数 = 件数
1088	警戒	認証に失敗したため、AMT による電源制御ができませんでした。 AMT の設定の画面の設定内容を見直すか、以下の URL にアクセスして AMT の認証情報を変更してください。 http://ホスト名:16992
1089	警戒	認証に失敗したため、AMT の設定ができませんでした。 [AMT の設定]画面の[admin パスワード]の設定内容を見直すか、以下の URL にアクセスして AMT の認証情報を変更してください。 http://ホスト名:16992
1090	警戒	操作ログのデータフォルダのディスク空き容量が少なくなっています。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 空きディスク容量=空きディスク容量 MB
1091※	緊急	操作ログのデータフォルダのディスク空き容量が非常に少なくなっているため、操作ログを取得するサービスを停止しました。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 空きディスク容量=空きディスク容量 MB
1092	警戒	サイトサーバのデータベースの空き容量が少なくなっています。 データベース使用率=データベース使用率%

イベント番号	重要度	イベントの内容
1093※	緊急	サイトサーバのデータベースの空き容量が非常に少なくなっているため、操作ログ収集サービスを停止しました。 データベース使用率=データベース使用率%
1094	警戒	データフォルダのディスク空き容量が少なくなっています。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 空きディスク容量=空きディスク容量 MB
1095※	緊急	データフォルダのディスク空き容量が非常に少なくなっているため、パッケージをサイトサーバにダウンロードできません。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。 空きディスク容量=空きディスク容量 MB
1096	情報	サイトサーバプログラムがインストールされました。
1097	情報	サイトサーバプログラムがアンインストールされました。
1098	情報	サイトサーバのサービスが開始されました。
1099	情報	サイトサーバのサービスが停止されました。
1100	緊急	サイトサーバプログラムのインストールに失敗しました。 インストーラートレースログファイルに出力されているエラーメッセージを確認し、そのエラーメッセージに従って対処してください。 インストーラートレースログファイルは発生元の「%WINDIR%\Temp\%JDNINST%\JDNINS01.log」に出力されます。 それでも解決できない場合は、トラブルシュート用情報の取得コマンドでトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。
1101	緊急	サイトサーバプログラムのアンインストールに失敗しました。
1103※	緊急	サイトサーバで、データベースへのアクセスエラーが発生しています。 データベースのサービス (JP1_ITDM2_DB Service) が開始されていないことが考えられます。サイトサーバ上でデータベースのサービスの状態を確認し、停止している場合は開始してください。 それでも解決できない場合は、サイトサーバ上でトラブルシュート用情報の取得コマンドを実行してトラブルシュート用情報を取得したあと、サポートサービスへ連絡してください。 要因=DBMS の詳細情報
1104※	緊急	サイトサーバで致命的なエラーが発生しています。 サイトサーバの環境が壊れているおそれがあります。 サイトサーバ上でトラブルシュート情報収集コマンドを実行してトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。

イベント番号	重要度	イベントの内容
1104※	緊急	エラーコード=内部エラーコード
1105	警戒	ネットワークモニタの有効化に失敗しました。 エラー要因 ネットワークアドレス=ネットワークアドレス エラー要因には、状況に応じてエラーの要因が表示されます。
1106	緊急	サイトサーバプログラムのインストールに失敗しました。 エラー要因 エラー要因には、状況に応じてエラーの要因が表示されます。
1110	情報	スマートデバイスをロックしました。 MDM 設定名=MDM 設定名
1111	警戒	スマートデバイスのロックに失敗しました。 要因=エラー要因 MDM 設定名=MDM 設定名 MDM サーバのホスト名=ホスト名 MDM サーバのポート番号=ポート番号 MDM サーバのユーザー ID=ユーザー ID プロキシサーバの IP アドレス=IP アドレス プロキシサーバのポート番号=ポート番号 プロキシサーバのユーザー ID=ユーザー ID
1112	情報	スマートデバイスのパスコードをリセットしました。 MDM 設定名=MDM 設定名
1113	警戒	スマートデバイスのパスコードのリセットに失敗しました。 要因=エラー要因 MDM 設定名=MDM 設定名 MDM サーバのホスト名=ホスト名 MDM サーバのポート番号=ポート番号 MDM サーバのユーザー ID=ユーザー ID プロキシサーバの IP アドレス=IP アドレス プロキシサーバのポート番号=ポート番号 プロキシサーバのユーザー ID=ユーザー ID
1114	情報	スマートデバイスを初期化しました。 MDM 設定名=MDM 設定名
1115	警戒	スマートデバイスの初期化に失敗しました。 要因=エラー要因 MDM 設定名=MDM 設定名 MDM サーバのホスト名=ホスト名 MDM サーバのポート番号=ポート番号

イベント番号	重要度	イベントの内容
1115	警戒	MDM サーバのユーザー ID=ユーザー ID プロキシサーバの IP アドレス=IP アドレス プロキシサーバのポート番号=ポート番号 プロキシサーバのユーザー ID=ユーザー ID
1116	警戒	スマートデバイスの削除に失敗しました。 データベースへのアクセスエラーが発生したことが考えられます。 設定画面の [機器の探索] - [探索履歴の確認] - [管理対象機器] で削除したい機器を選択して、削除してください。 エラーコード=内部エラーコード
1117	情報	MDM システム (製品名) との機器情報の同期が完了しました。 MDM 設定名=設定名
1118※	警戒	MDM システム (製品名) との機器情報の同期に失敗しました。 要因=要因 MDM 設定名=MDM 設定名 MDM サーバのホスト名=サーバのホスト名 MDM サーバのポート番号=サーバのポート番号 ユーザー ID=ユーザー ID プロキシサーバの IP アドレス=プロキシサーバの IP アドレス プロキシサーバのポート番号=プロキシサーバのポート番号 プロキシサーバのユーザー ID=プロキシサーバのユーザー ID 要因には、状況に応じてエラーの要因が表示されます。
1120	警戒	JP1/IM へのイベント通知に失敗しました。 JP1/IM 連携の前提ソフトウェアである JP1/Base がインストールされているかを確認してください。 インストールされている場合は、JP1/Base の設定が正しいかを確認してください。 それでも解決できない場合は、トラブルシューティング情報の取得コマンドでトラブルシューティング情報を取得したあと、サポートサービスへ連絡してください。 エラーコード=内部エラーコード
1122	警戒	最大値を超えるインベントリを受信しました。
1123	警戒	Active Directory サーバからの機器情報および組織情報の取得に失敗しました。 Active Directory サーバからの機器情報および組織情報の取得でエラーが発生しました。 トラブルシューティング情報の取得コマンドでトラブルシューティング情報を取得したあと、サポートサービスへ連絡してください。 エラーコード=エラーコード
1124	情報	SAMAC 辞書の情報を更新しました。

イベント番号	重要度	イベントの内容
1127	緊急	機器のセキュリティ状態を判定しました。判定結果は危険レベルです。 セキュリティポリシー名=セキュリティポリシー名 更新プログラム=更新プログラムの危険レベル ウィルス対策製品=ウィルス対策製品の危険レベル 使用禁止ソフトウェア=使用禁止ソフトウェアの危険レベル 使用必須ソフトウェア=必須ソフトウェアの危険レベル 使用禁止サービス=使用禁止サービスの危険レベル OS のセキュリティ設定=セキュリティ設定の危険レベル ユーザー定義のセキュリティ設定=ユーザー定義のセキュリティ設定の危険レベル 危険レベルについて、次に示します。 • 危険 • 警告 • 注意 • 安全 • 不明 • 対象外 危険レベルの対象項目について、次に示します。 • Guest アカウント設定 • 脆弱なパスワード • 無期限パスワード • パスワード更新経過日数 • 自動ログオンの設定 • パワーオンパスワード設定 • 共有フォルダの設定 • 匿名接続による制限 • 不要サービスの稼働 • Windows ファイアウォールの設定 • Windows 自動更新の設定 • スクリーンセーバーのパスワードによる保護 • スクリーンセーバーの待ち時間の設定 • 管理共有フォルダの設定 • DCOM の設定 • リモートデスクトップの設定
1128	警戒	機器のセキュリティ状態を判定しました。判定結果は危険レベルです。 セキュリティポリシー名=セキュリティポリシー名 更新プログラム=更新プログラムの危険レベル ウィルス対策製品=ウィルス対策製品の危険レベル 使用禁止ソフトウェア=使用禁止ソフトウェアの危険レベル 使用必須ソフトウェア=必須ソフトウェアの危険レベル

イベント番号	重要度	イベントの内容
1128	警戒	使用禁止サービス=使用禁止サービスの危険レベル OS のセキュリティ設定=セキュリティ設定の危険レベル ユーザー定義のセキュリティ設定=ユーザー定義のセキュリティ設定の危険レベル 危険レベルについて、次に示します。 • 危険 • 警告 • 注意 • 安全 • 不明 • 対象外 危険レベルの対象項目について、次に示します。 • Guest アカウント設定 • 脆弱なパスワード • 無期限パスワード • パスワード更新経過日数 • 自動ログオンの設定 • パワーオンパスワード設定 • 共有フォルダの設定 • 匿名接続による制限 • 不要サービスの稼働 • Windows ファイアウォールの設定 • Windows 自動更新の設定 • スクリーンセーバーのパスワードによる保護 • スクリーンセーバーの待ち時間の設定 • 管理共有フォルダの設定 • DCOM の設定 • リモートデスクトップの設定
1129	情報	機器のセキュリティ状態を判定しました。判定結果は危険レベルです。 セキュリティポリシー名=セキュリティポリシー名 更新プログラム=更新プログラムの危険レベル ウィルス対策製品=ウィルス対策製品の危険レベル 使用禁止ソフトウェア=使用禁止ソフトウェアの危険レベル 使用必須ソフトウェア=必須ソフトウェアの危険レベル 使用禁止サービス=使用禁止サービスの危険レベル OS のセキュリティ設定=セキュリティ設定の危険レベル ユーザー定義のセキュリティ設定=ユーザー定義のセキュリティ設定の危険レベル 危険レベルについて、次に示します。 • 危険 • 警告

イベント番号	重要度	イベントの内容
1129	情報	• 注意 • 安全 • 不明 • 対象外 危険レベルの対象項目について、次に示します。 • Guest アカウント設定 • 脆弱なパスワード • 無期限パスワード • パスワード更新経過日数 • 自動ログオンの設定 • パワーオンパスワード設定 • 共有フォルダの設定 • 匿名接続による制限 • 不要サービスの稼働 • Windows ファイアウォールの設定 • Windows 自動更新の設定 • スクリーンセーバーのパスワードによる保護 • スクリーンセーバーの待ち時間の設定 • 管理共有フォルダの設定 • DCOM の設定 • リモートデスクトップの設定
1130	情報	変更履歴の取得処理を開始しました。
1131	情報	変更履歴の取得処理が完了しました。
1132※	警戒	変更履歴の取得中に致命的なエラーが発生しました。 トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。
1133※	警戒	保存用の変更履歴のファイル出力に失敗しました。 エラー要因 エラー要因には、状況に応じてエラーの要因が表示されます。
1134	情報	ネットワークへの接続を許可する処理を、JP1/NETM/NM - Manager に要求しました。
1135※	警戒	ネットワークへの接続を拒否する処理を、JP1/NETM/NM - Manager に要求しました。
1136※	警戒	ネットワークへの接続拒否に失敗しました。 エラー要因 エラー要因で表示される内容を次に示します。

イベント番号	重要度	イベントの内容
1136※	警戒	- JP1/NETM/NM - Manager がインストールされていません。管理用サーバに JP1/NETM/NM - Manager がインストールされているかを確認してください。 - JP1/NETM/NM - Manager のサービスが開始されていません。管理用サーバで JP1/NETM/NM - Manager のサービスが開始されているかを確認してください。 - 内部エラーが発生したため処理を中止しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。
1137※	警戒	ネットワークへの接続許可に失敗しました。 エラー要因 エラー要因で表示される内容を次に示します。 - JP1/NETM/NM - Manager がインストールされていません。管理用サーバに JP1/NETM/NM - Manager がインストールされているかを確認してください。 - JP1/NETM/NM - Manager のサービスが開始されていません。管理用サーバで JP1/NETM/NM - Manager のサービスが開始されているかを確認してください。 - 内部エラーが発生したため処理を中止しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。
1138	警戒	操作ログを定期的にエクスポートする処理で、エラーが発生しました。 エラー要因 エラー要因で表示される内容を、次に示します。 - 内部エラーが発生しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。 - データフォルダまたはローカルデータフォルダで I/O エラーが発生しました。データフォルダまたはローカルデータフォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに接続できませんでした。セットアップで指定した操作ログの保管先フォルダが存在し、接続できることを確認してください。 - 操作ログの保管先フォルダへの認証に失敗しました。セットアップで指定したユーザー名およびパスワードで、操作ログの保管先フォルダに接続できることを確認してください。 - 操作ログの保管先フォルダで I/O エラーが発生しました。操作ログの保管先フォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに保管されたファイルが存在しません。保管されたファイルをほかのフォルダに退避している場合は、操作ログの保管先フォルダに保管されたファイルを戻したあと、操作ログの取り込みを再実行してください。 - セットアップで操作ログの保管先フォルダが設定されていることを確認してください。 - 管理用サーバで、共有フォルダに対する匿名アクセスが制限されているため、操作ログの保管先フォルダに接続できません。セットアップで指定した

イベント番号	重要度	イベントの内容
1138	警戒	ユーザー名とパスワードに対応するユーザアカウントを、管理用サーバで作成してください。
1139	警戒	操作ログの自動取り込み処理で、エラーが発生しました。 エラー要因 エラー要因で表示される内容を、次に示します。 - 内部エラーが発生しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。 - データフォルダまたはローカルデータフォルダで I/O エラーが発生しました。データフォルダまたはローカルデータフォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに接続できませんでした。セットアップで指定した操作ログの保管先フォルダが存在し、接続できることを確認してください。 - 操作ログの保管先フォルダへの認証に失敗しました。セットアップで指定したユーザー名およびパスワードで、操作ログの保管先フォルダに接続できることを確認してください。 - 操作ログの保管先フォルダで I/O エラーが発生しました。操作ログの保管先フォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに保管されたファイルが存在しません。保管されたファイルをほかのフォルダに退避している場合は、操作ログの保管先フォルダに保管されたファイルを戻したあと、操作ログの取り込みを再実行してください。 - セットアップで操作ログの保管先フォルダが設定されていることを確認してください。 - 管理用サーバで、共有フォルダに対する匿名アクセスが制限されているため、操作ログの保管先フォルダに接続できません。セットアップで指定したユーザー名とパスワードに対応するユーザアカウントを、管理用サーバで作成してください。
1140	警戒	操作ログの日付情報の更新で、エラーが発生しました。 エラー要因 エラー要因で表示される内容を、次に示します。 - 内部エラーが発生しました。エラーが繰り返し発生する場合は、サポートサービスに連絡してください。 - データフォルダまたはローカルデータフォルダで I/O エラーが発生しました。データフォルダまたはローカルデータフォルダにアクセスできること、および空き容量が不足していないことを確認してください。 - 操作ログの保管先フォルダに接続できませんでした。セットアップで指定した操作ログの保管先フォルダが存在し、接続できることを確認してください。 - 操作ログの保管先フォルダへの認証に失敗しました。セットアップで指定したユーザー名およびパスワードで、操作ログの保管先フォルダに接続できることを確認してください。 - 操作ログの保管先フォルダで I/O エラーが発生しました。操作ログの保管先フォルダにアクセスできること、および空き容量が不足していないことを確認してください。

イベント番号	重要度	イベントの内容
1140	警戒	• 操作ログの保管先フォルダに保管されたファイルが存在しません。保管されたファイルをほかのフォルダに退避している場合は、操作ログの保管先フォルダに保管されたファイルを戻したあと、操作ログの取り込みを再実行してください。 • セットアップで操作ログの保管先フォルダが設定されていることを確認してください。 • 管理用サーバで、共有フォルダに対する匿名アクセスが制限されているため、操作ログの保管先フォルダに接続できません。セットアップで指定したユーザー名とパスワードに対応するユーザアカウントを、管理用サーバで作成してください。

注※ JP1/IM と連携する場合に、JP1 イベントとして JP1/IM に出力されます。

19.2 JP1 イベントの属性

JP1 イベントの属性には、基本属性と拡張属性があります。基本属性にはイベント ID とメッセージの項目が、拡張属性には共通情報（重大度やユーザー名など）と固有情報（メッセージ詳細）があります。

JP1 イベントの属性を次の表に示します。以降の表中では、凡例を次のとおり表記しています。

（凡例）－：該当なし

イベント番号が 200 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	－	00006902
		メッセージ	－	サービス (JP1_ITDM2_Service) でエラーが発生しました。サービス (JP1_ITDM2_Service) を停止します。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	－	トラブルシューティング情報収集コマンドでトラブルシューティング情報を収集したあと、サポートサービスへ連絡してください。 エラーコード=エラーコード

イベント番号が 1032 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	－	00006901
		メッセージ	－	操作ログの保管でエラーが発生しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	－	エラー要因 エラー要因には、状況に応じてエラーの要因が表示されます。

イベント番号が 1036 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006905
		メッセージ	—	操作ログのデータベースの拡張に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	操作ログのデータベースの空き容量がありません。空き容量を確保して、サービスを再起動してください。空き容量が十分ある場合で、エラーが繰り返し発生するときは、トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。

イベント番号が 1037 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006906
		メッセージ	—	Active Directory サーバからの機器情報および組織情報の取得に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	要因 [Active Directory の設定] 画面の接続テスト機能を使用して、設定を見直してください。 エラーコード=エラーコード Active Directory サーバのホスト名=ホスト名 Active Directory サーバのポート番号=ポート番号 ユーザー ID=接続アカウント ルート OU=取り込みルートパス

属性種別		項目	属性名	内容
拡張属性	固有情報	メッセージ詳細	—	要因には、状況に応じてエラーの要因が表示されます。

イベント番号が 1055 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006907
		メッセージ	—	サポートサービスへの接続でエラーが発生しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	サポートサービスへの接続でエラーが発生しました。 エラー要因 [サポートサービスの設定] 画面の接続テスト機能を使用して、設定を見直してください。 エラー要因 には、状況に応じてエラーの要因が表示されます。

イベント番号が 1056 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006908
		メッセージ	—	管理者へのメール通知に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	エラー要因 [メールサーバの設定] 画面のテストメール送信機能を使用して、設定を見直してください。 エラー要因 には、状況に応じてエラーの要因が表示されます。

イベント番号が 1057 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006909
		メッセージ	—	ディスクの空き容量が少なくなっています。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	フォルダ種別（フォルダ種別のフォルダのパス） ディスクの空き容量=フォルダ種別のフォルダの空きディスク容量

イベント番号が 1058 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690A
		メッセージ	—	ディスクの空き容量が非常に少なくなっています。ディスクの空き容量が不足すると、管理用サーバでデータベース障害が発生するおそれがあります。ディスクの空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	フォルダ種別（フォルダ種別のフォルダのパス） ディスクの空き容量=フォルダ種別のフォルダの空きディスク容量

イベント番号が 1079 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006913

属性種別		項目	属性名	内容
基本属性		メッセージ	—	機器のネットワークへの接続が遮断されました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	設定なし
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_SECURITY
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	MAC アドレス=MAC アドレス IP アドレス=IP アドレス

イベント番号が 1082 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006914
		メッセージ	—	ネットワークモニタの処理を停止しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	NM ホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_SECURITY
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	—

イベント番号が 1091 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690B
		メッセージ	—	操作ログのデータフォルダのディスク空き容量が非常に少なくなっているため、操作ログを取得するサービスを停止しました。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生したサイトサーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2

属性種別		項目	属性名	内容
拡張属性	共通情報	オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	空きディスク容量=空きディスク容量 MB

イベント番号が 1093 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690C
		メッセージ	—	サイトサーバのデータベースの空き容量が非常に少なくなっているため、操作ログ収集サービスを停止しました。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生したサイトサーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	データベース使用率=データベース使用率%

イベント番号が 1095 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690D
		メッセージ	—	データフォルダのディスク空き容量が非常に少なくなっているため、パッケージをサイトサーバにダウンロードできません。ディスク空き容量を増やすか、十分な空き容量のあるディスクに変更してください。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生したサイトサーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時

属性種別		項目	属性名	内容
拡張属性	固有情報	メッセージ 詳細	—	空きディスク容量=空きディスク容量 MB

イベント番号が 1103 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690E
		メッセージ	—	サイトサーバで、データベースへのアクセスエラーが発生しています。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生したサイトサーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクト タイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ 詳細	—	データベースのサービス（JP1_ITDM2_DB Service）が開始されていないことが考えられます。サイトサーバ上でデータベースのサービスの状態を確認し、停止している場合は開始してください。 それでも解決できない場合は、サイトサーバ上でトラブルシューティング情報の取得コマンドを実行してトラブルシューティング情報を取得したあと、サポートサービスへ連絡してください。 要因=DBMS の詳細情報

イベント番号が 1104 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	0000690F
		メッセージ	—	サイトサーバで致命的なエラーが発生しています。
拡張属性	共通情報	重大度	SERVERITY	Emergency
		発生ホスト名	JP1_SOURCEHOST	イベントが発生したサイトサーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクト タイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ 詳細	—	サイトサーバの環境が壊れているおそれがあります。

属性種別		項目	属性名	内容
拡張属性	固有情報	メッセージ 詳細	—	サイトサーバ上でトラブルシュート情報収集コマンドを実行してトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。 エラーコード=内部エラーコード

イベント番号が 1118 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006912
		メッセージ	—	MDM システム（MDM の製品名または MDM のサービス名）との機器情報の同期に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	イベントが発生した管理用サーバのホスト名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクト タイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ 詳細	—	要因=要因 MDM 設定名=MDM 設定名 MDM サーバのホスト名=サーバのホスト名 MDM サーバのポート番号=サーバのポート番号 ユーザー ID=ユーザー ID プロキシサーバの IP アドレス=プロキシサーバの IP アドレス プロキシサーバのポート番号=プロキシサーバのポート番号 プロキシサーバのユーザー ID=プロキシサーバのユーザー ID 要因には、状況に応じてエラーの要因が表示されます。

イベント番号が 1132 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006915
		メッセージ	—	変更履歴の取得中に致命的なエラーが発生しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	対象サーバ名

属性種別		項目	属性名	内容
拡張属性	共通情報	プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	トラブルシュート情報収集コマンドでトラブルシュート情報を収集したあと、サポートサービスへ連絡してください。

イベント番号が 1133 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006916
		メッセージ	—	保存用の変更履歴のファイル出力に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	対象サーバ名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	エラー要因 エラー要因には、状況に応じてエラーの要因が表示されます。

イベント番号が 1135 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006917
		メッセージ	—	ネットワークへの接続を拒否する処理を、JP1/NETM/NM - Manager に要求しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	対象サーバ名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_SECURITY
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	—

イベント番号が 1136 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006918
		メッセージ	—	ネットワークへの接続拒否に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	対象サーバ名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	エラー要因 エラー要因 には、状況に応じてエラーの要因が表示されます。

イベント番号が 1137 の場合

属性種別		項目	属性名	内容
基本属性		イベント ID	—	00006919
		メッセージ	—	ネットワークへの接続許可に失敗しました。
拡張属性	共通情報	重大度	SERVERITY	Alert
		発生ホスト名	JP1_SOURCEHOST	対象サーバ名
		プロダクト名	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		オブジェクトタイプ	OBJECT_TYPE	ITDM2_ERR
		開始時刻	START_TIME	イベント発生日時
	固有情報	メッセージ詳細	—	エラー要因 エラー要因 には、状況に応じてエラーの要因が表示されます。

付録

付録 A 参考情報

ここでは、JP1/IT Desktop Management 2 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

JP1/IT Desktop Management 2 で使用するポート番号について説明します。

JP1/IT Desktop Management 2 - Manager 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。 管理者のコンピュータにインストールされたり リモートインストールマネージャ、パッケージから 管理用サーバへの通信でも使用されます。
31000	←	エージェントまた は中継システム [ephemeral]	TCP	エージェントまたは中継システムから管理用サー バへの通信に使用されます。
ephemeral	→	エージェントまた は中継システム [31001]	TCP	リモートインストールマネージャを使用した配布 をする場合に、管理用サーバからエージェント、 中継システムへの通信に使用されます。
31006～31009、 31011、31012	なし	なし	TCP	JP1/IT Desktop Management 2 の内部処理に 使用されます。
31010	←	- リモートインス トールマネー ジャ [ephemeral] - Asset Console (jamTakeITD M2Info.exe) [ephemeral]	TCP	リモートインストールマネージャ、Asset Console から管理用サーバへの通信や内部処理に 使用されます。
ephemeral	→	エージェントまた は中継システム [31014]	TCP	マルチキャスト配布をする場合に管理用サーバか らエージェントまたは中継システムへの通信に使 用されます。
31015	←	エージェントまた は中継システム [ephemeral]	TCP	マルチキャスト配布の再送要求をする場合にエー ジェントまたは中継システムから管理用サーバへ の通信に使用されます。

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
31021	←	- リモートインストールマネージャ [ephemeral] - エージェント [ephemeral] - 中継システム [ephemeral] - パッケージ [ephemeral]	TCP	リモートインストールマネージャを使用した配布をする場合にリモートインストールマネージャ、エージェント、中継システムおよびパッケージから管理用サーバへ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 JP1/IT Desktop Management 2 - Manager 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）。

管理者のコンピュータ（リモートインストールマネージャ）

管理者のコン ピュータのポート 番号	接続方向	接続対象 [ポート 番号]	プロトコル	用途
ephemeral	→	管理用サーバ [31010、31021]	TCP	リモートインストールマネージャを使用した配布をする場合に、リモートインストールマネージャから管理用サーバへの通信に使用されます。
ephemeral※	← →	管理用サーバ [ephemeral※]	TCP	リモートインストールマネージャの内部処理に使用されます。

注※ データベースのエージェント接続で使用するポート番号を固定する手順を次に示します。

管理用サーバ(接続先)のポート番号を固定する場合

1. stopservice コマンドを実行し、管理用サーバのサービスを停止します。
2. JP1/IT Desktop Management 2 - Manager インストール先フォルダ¥mgr¥db¥CONF に格納されている pdsys ファイルをテキストエディタで開きます。
3. 「set pd_service_port = ポート番号」の記述を追加し、ポート番号部分には固定したいポート番号を記述します。

（例）使用するポート番号に 10000 を指定する場合

```
set pd_service_port = 10000
```

4. startservice コマンドを実行し、管理用サーバのサービスを開始します。

リモートインストールマネージャ(接続先)のポート番号を固定する場合

受信用ポートは、デフォルトでは OS が自動でポート番号を割り当てます。なお、受信用ポートは 10 個以上使用されます。

1. リモートインストールマネージャおよびそのほかの JP1/IT Desktop Management 2 のアプリケーションを停止します。

2. Remote Install Manager インストール先フォルダ¥mgr¥dbclt に格納されている HiRDB.ini をテキストエディタで開きます。

Remote Install Manager を管理用サーバと同じコンピュータにインストールした場合、HiRDB.ini は JP1/IT Desktop Management 2 - Manager インストール先フォルダ¥mgr¥db¥CONF¥emb に格納されています。

3. 「PDCLTRCVPORT=」に使用するポート番号の範囲を「ポート番号-ポート番号」の形式で指定します。なお、PDCLTRCVPORT= のあとに何も指定しないか「0」を指定した場合、使用するポート番号の範囲は設定されません。デフォルトでは、使用するポート番号の範囲は設定されていません。

(例) 使用するポート番号の範囲に 10000~10500 を指定する場合

```
PDCLTRCVPORT=10000-10500
```

4. リモートインストールマネージャおよびそのほかの JP1/IT Desktop Management 2 のアプリケーションを起動します。

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。

管理者のコンピュータで、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 Remote Install Manager 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）。

中継システムのポート番号一覧

中継システムのポート番号	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	リモートインストールマネージャを使用した配布をする場合に、管理用サーバから中継システムへの通信に使用されます。
31002	←	エージェント [ephemeral]	TCP	リモートインストールマネージャを使用した配布をする場合に、エージェントから中継システムへの通信に使用されます。

中継システムのポート番号	接続方向	接続対象 [ポート番号]	プロトコル	用途
31014	←	管理用サーバ [ephemeral]	TCP	マルチキャスト配布をする場合に、管理用サーバから中継システムへの通信に使用されます。
31015	←	エージェント [ephemeral]	TCP	マルチキャスト配布の再送要求をする場合に、エージェントから中継システムへの通信に使用されます。
ephemeral	→	管理用サーバ [31021]	TCP	リモートインストールマネージャを使用した配布をする場合に、中継システムから管理用サーバへ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。

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。
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] ダイアログー [接続] タブで設定する。

JP1/IT Desktop Management 2 - 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	←	管理用サーバまたは中継システム [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。
ephemeral	→	中継システム [31002]	TCP	リモートインストールマネージャを使用した配布をする場合に、エージェントから中継システムへの通信に使用されます。
31014	←	管理用サーバまたは中継システム [ephemeral]	TCP	マルチキャスト配布をする場合に、管理用サーバまたは中継システムからエージェントへの通信に使用されます。
ephemeral	→	管理用サーバまたは中継システム [31015]	TCP	マルチキャスト配布の再送要求をする場合に、エージェントから管理用サーバ、中継システムへの通信に使用されます。
ephemeral	→	管理用サーバ [31021]	TCP	リモートインストールマネージャを使用した配布をする場合に、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。

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、JP1/IT Desktop Management 2 - Manager と JP1/IT Desktop Management 2 - 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 管理用サーバとエージェント間の通信

管理用サーバとエージェントを導入したコンピュータの間では、データの送受信による通信が発生します。通信発生の代表的な契機を次の表に示します。

分類	通信発生の代表的な契機
コンピュータの管理状態の変更通知	- エージェントのインストール時（インストール直後に管理対象機器として登録し、管理種別をエージェント管理に変更するための情報を送信） - エージェントのアンインストール時（管理状態をエージェントレス管理に変更するための情報を送信）
インベントリ情報の自動取得	- エージェントが監視間隔（セキュリティ項目）に従ってセキュリティ情報を取得し、前回取得した情報から変更があった場合 - エージェントが監視間隔（セキュリティ項目以外）に従ってセキュリティ以外の情報を取得し、前回取得した情報から変更があった場合 - 使用を許可した USB デバイスを PC に接続した場合（USB デバイスの切断時、または USB デバイスを切断しないで PC の電源を落とした場合などは、次の PC 起動時にファイルの一覧の情報を送信） - USB デバイスを切断した場合、または USB デバイスを切断しないで PC の電源を落とした場合（次の PC 起動時にファイルの一覧の情報を送信） - PC の電源断など、エージェントが停止した場合（停止情報を送信）
エージェントの設定情報の適用または変更	- セキュリティポリシーや、エージェント設定など、エージェントに適用する設定を割り当てた場合 - セキュリティポリシーや、エージェント設定など、エージェントに適用する設定を変更した場合 - エージェントの起動時（セキュリティポリシー、エージェント設定などを受信）
管理者の操作	- 管理者が「最新の情報を取得する」を実行した場合（エージェントがインベントリ情報を送信） - 管理者が利用者のコンピュータの電源 ON/OFF、または再起動を実行した場合 - 管理者が「利用者にメッセージを通知する」を実行した場合 - 管理者が配布またはアンインストールを実行した場合 - 管理者がリモートコントロールを実行した場合
セキュリティ対策	- セキュリティ判定時（セキュリティ対策の自動実行） - セキュリティ判定時（未適用の更新プログラムの自動配布）
エージェントでの入力	- 利用者情報を入力したとき - USB デバイスを登録したとき - オフライン管理のコンピュータから収集した機器情報を通知したとき
操作ログまたは禁止操作	操作ログまたは禁止操作のアップロード

付録 A.3 セキュリティ状況の判定除外ユーザー設定ファイルの形式

ファイル名は、「jdn_except_users.dat」としてください。

判定除外ユーザー設定ファイルは、次の形式で作成してください。

OS のユーザーアカウント名 1

OS のユーザーアカウント名 2

1 行に 1 つのユーザーアカウント名を指定してください。複数のユーザーアカウントを指定する場合は、複数行で指定できます。

ユーザーアカウント名は 20 文字以内の半角英数字および記号で指定してください。ただし、次の記号は使えません。

「`“`」、`/`、`¥`、`[`、`]`、`:`、`;`、`|`、`=`、`,`、`+`、`*`、`?`、`<`、`>`」

また、`.`（ピリオド）または半角スペースだけを指定することはできません。

ポイント

「HOGE*」のように、末尾に「`*`」を指定した前方一致でユーザーアカウント名を指定できます。
「`*`」は末尾だけに指定できます。ユーザーアカウント名に「`*`」だけを指定した場合は無視されます。

付録 A.4 エクスポートした操作ログの出力形式

`ioutils exporttoplog` コマンドまたは操作ログの定期エクスポートを利用して操作ログをエクスポートしたときの CSV ファイルの出力形式を次の表に示します。

出力される項目	出力形式	出力される文字列の最大 バイト数（バイト）※1
不審操作	「警戒」または「FALSE」が出力されます。	8
操作日時	次の形式で出力されます。 YYYY/MM/DD△hh:mm:ss※2	19
発生元	256 文字以内の文字列が出力されます。	1,024
ユーザー名	1,024 文字以内の文字列が出力されます。	4,096
操作種別	次のどれかが出力されます。 • コンピュータの起動と停止、ログオンとログオフ • プログラムの起動と停止 • ファイル操作 • 印刷操作 • 外部メディア操作 • Web アクセス • ウィンドウ操作 • デバイス操作	88

出力される項目	出力形式	出力される文字列の最大 バイト数 (バイト) ※1
操作種別(詳細)	次のどれかが出力されます。 • コンピュータ起動 • コンピュータ停止 • ログオン • ログオフ • プログラム起動抑止 • プロセス起動 • プロセス停止 • ファイルコピー • ファイル移動 • ファイル名称変更 • ファイル作成 • ファイル削除 • フォルダコピー • フォルダ移動 • フォルダ名称変更 • フォルダ作成 • フォルダ削除 • ファイルアップロード • ファイルダウンロード • ファイル送信 • ファイル受信 • メール送信 (添付ファイル付) • メール受信 (添付ファイル付) • 添付ファイル保存 • 印刷 • 印刷抑止 • 外部メディア接続 • 外部メディア取り外し • 外部メディア接続抑止 • Web アクセス • アクティブウィンドウ変更 • デバイス接続 • デバイス切断 • デバイス接続抑止 • デバイス接続許可	56
ファイル作成日時	次の形式で出力されます。 YYYY/MM/DD△hh:mm:ss※2	19
ファイル更新日時	次の形式で出力されます。 YYYY/MM/DD△hh:mm:ss※2	19

出力される項目	出力形式	出力される文字列の最大 バイト数 (バイト) ※1
ファイルサイズ	小数点を含む数値に、単位「B」、「KB」、「MB」、「GB」、「TB」または「PB」が付いた状態で出力されます。最大値は 8,191PB です。	6
持ち込み元ドライブ種別	次のどれかが出力されます。 - ローカルディスク - ネットワークドライブ - リムーバブルディスク - CD-ROM - RAM ディスク - Web - FTP - メール - その他	40
持ち込み日時	次の形式で出力されます。 YYYY/MM/DD△hh:mm:ss※2	19
持ち出し元ファイル情報 ※3	2,083 文字以内の文字列が出力されます。	8,332
持ち出し元ドライブ種別	次のどれかが出力されます。 - ローカルディスク - ネットワークドライブ - リムーバブルディスク - CD-ROM - RAM ディスク - Web - FTP - メール - その他	40
持ち出し先ファイル情報 ※3	2,083 文字以内の文字列が出力されます。	8,332
持ち出し先ドライブ種別	次のどれかが出力されます。 - ローカルディスク - ネットワークドライブ - リムーバブルディスク - CD-ROM - RAM ディスク - Web - FTP - メール - その他	40

出力される項目	出力形式	出力される文字列の最大 バイト数 (バイト) ※1
ユーザー名(実行アカウント名)	1,024 文字以内の文字列が出力されます。	4,096
ファイル名	520 文字以内の文字列が出力されます。	2,080
ソフトウェア名	512 文字以内の文字列が出力されます。	2,048
ソフトウェアバージョン	128 文字以内の文字列が出力されます。	512
ファイルバージョン	20 文字以内の文字列が出力されます。	80
プロセス名	520 文字以内の文字列が出力されます。	2,080
ドライブ種別	次のどれかが出力されます。 - ローカルディスク - ネットワークドライブ - リムーバブルディスク - CD-ROM - RAM ディスク - その他	40
ドライブ名	[A:¥] から [Z:¥] までのどれかが出力されます。	3
シリアルナンバー	256 文字以内の文字列が出力されます。	1,024
デバイス種別	1,024 文字以内の文字列が出力されます。	4,096
デバイス名	1,024 文字以内の文字列が出力されます。	4,096
デバイスインスタンス ID	1,024 文字以内の文字列が出力されます。	4,096
印刷ドキュメント名	1,024 文字以内の文字列が出力されます。	4,096
プリンター名	1,024 文字以内の文字列が出力されます。	4,096
印刷ページ数	2,147,483,647 以内の整数が出力されます。	10
URL	2,083 文字以内の文字列が出力されます。	8,332
Web ページタイトル	1,024 文字以内の文字列が出力されます。	4,096
ウィンドウタイトル	512 文字以内の文字列が出力されます。	2,048
ホスト識別子	64 文字以内の文字列が出力されます。	64
デバイス区分	次のどれかが出力されます。 - USB デバイス - 内蔵 CD/DVD ドライブ - 内蔵 FD ドライブ - IEEE1394 デバイス - 内蔵 SD カード - Bluetooth デバイス - イメージングデバイス	64

出力される項目	出力形式	出力される文字列の最大 バイト数 (バイト) ※1
デバイス区分	- Windows ポータブルデバイス - 不明	64

注※1 ioutils exportoplog コマンド実行時、文字コードに UTF-8 や UTF-16 を指定した場合の最大バイト数です。半角英数字と記号は 1 文字当たり 1 バイト、それら以外は 1 文字当たり 4 バイトとして算出しています。

注※2 YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

注※3 操作種別(詳細)が「メール送信 (添付ファイル付)」、「メール受信 (添付ファイル付)」または「添付ファイル保存」の場合、「¥r¥n」(改行コード)は「¥n」に変換してから出力されます。

関連リンク

- 15.3.3 操作ログを定期的にエクスポートする手順
- 17.16 ioutils exportoplog (操作ログのエクスポート)

付録 A.5 共通管理項目と追加管理項目の定義のインポートファイルの設定項目

共通管理項目と追加管理項目の定義のインポートファイルを編集するときに、値を入力する項目を編集内容ごとに次の表に示します。

編集内容	更新区分 ※1	資産管理 項目種類	更新項目言 語キー	更新 項目	他言語の 設定	nn - 設 定値(変 更前)※2	nn - 設定値 (変更後)※2	nn - 説明 ※2
階層型の項目の追加	○	○	○	○	○	×	△※3	×
階層型の項目の変更	○	○	○	○	○	○	○	△
階層型の項目の削除	○	○	○	○	—	○	—	—
選択型の項目の追加	○	○	○	○	○	×	△※3	△※4
選択型の項目の変更	○	○	○	○	○	○	○	△
選択型の項目の削除	○	○	○	○	—	○	—	—

(凡例) ○：必ず値を入力する △：必要に応じて値を入力する ×：値を入力してはいけない –：入力した値は無視される

注※1 更新区分は次のとおり入力してください。

- 追加する場合：A
- 変更する場合：U
- 削除する場合：D

注※2 [他言語の設定] ダイアログで設定している数だけ、この3列が追加された状態でインポートファイルが出力されます。*nn* は設定している言語種別の略記です。(例) ja、en など

注※3 デフォルトの言語の場合は省略できません。デフォルトの言語以外の場合に値を省略したときは、デフォルトの言語と同じ値が設定されます。

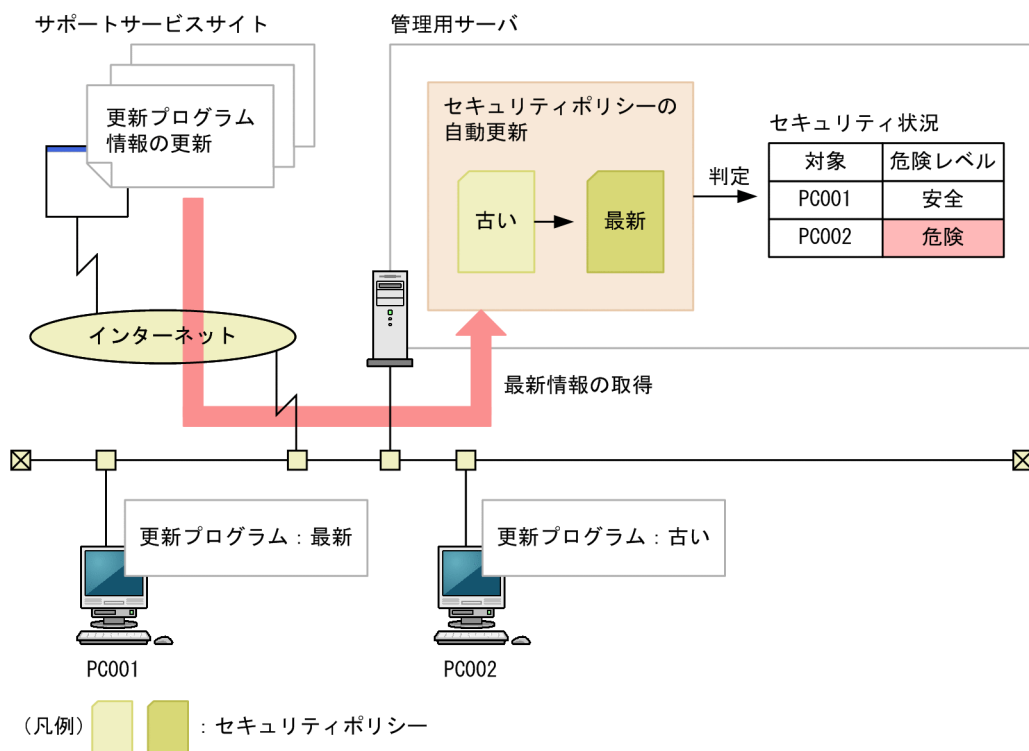
注※4 デフォルトの言語の場合に値を省略したときは、空文字が設定されます。デフォルトの言語以外の場合に値を省略したときは、デフォルトの言語と同じ値が設定されます。

付録 A.6 サポートサービスからの情報の取得

サポートサービス契約をしていると、サポートサービスから更新プログラム情報や SAMAC 辞書の情報を取得して、JP1/IT Desktop Management 2 の情報を更新できます。

(1) サポートサービスからの情報の自動取得

管理用サーバは、更新プログラムの情報が更新されているかどうかを定期的（デフォルトでは1日1回）に確認します。最新の更新プログラム情報が更新されていた場合の、更新プログラム情報の取得からセキュリティポリシーの更新までの流れを次の図に示します。



注意事項

サポートサービスから更新情報を自動取得するためには、次の条件を満たしている必要があります。

- サポートサービス契約をしていること
- 管理用サーバがインターネットに接続できること

(2) サポートサービスからの情報のオフライン更新

管理用サーバがインターネット接続できない環境にある場合や、SAMAC 辞書の情報を更新したい場合は、管理者が外部接続できるコンピュータからサポートサービスサイトに接続し、サポートサービスからの情報をダウンロードします。ダウンロードした情報を管理用サーバに登録することで、管理用サーバの情報を更新できます。定期的にサポートサービスサイトを確認して、最新の情報が公開されている場合は、オフライン更新を実行してください。

サポートサービスからの情報をオフライン更新する方法には、次の 2 種類があります。

操作画面からオフライン更新する

セキュリティ画面の【更新プログラム一覧】画面、資産画面の【管理ソフトウェア一覧】画面、および機器画面の【ソフトウェア一覧】画面の操作メニューから更新できます。

コマンドを実行してオフライン更新する

updatesupportinfo コマンドを実行して更新できます。詳細については、「[17.19 updatesupportinfo \(サポートサービスからの情報の登録\)](#)」を参照してください。

(3) サポートサービスから取得できる情報

サポートサービスから取得できる情報を次の表に示します。

取得できる情報			説明	自動取得の可否
サポート情報ファイル	更新プログラム情報	更新プログラム名	更新プログラムの名称です。	○
		セキュリティ情報番号	更新プログラムのセキュリティ情報番号です。	
		セキュリティ深刻度	更新プログラムの影響度で、「緊急」または「重要」です。	
		クラス	更新プログラムの種類です。	
		詳細情報 URL	更新プログラムの詳細情報が記載された日本マイクロソフト社のサイトの URL です。	
		説明	更新プログラムの説明です。	
		リリース日	更新プログラムがリリースされた日付です。	
		対象製品	更新プログラムの対象製品名です。	
		サービスパック	〔Windows 種別〕 で選択した OS のサービスパックです。	
		対象種別	対象となる製品名、バージョン、サービスパックです。	
		更新プログラムのダウンロード URL	更新プログラムをダウンロードするための URL です。	
SAMAC ソフトウェア辞書のオフライン更新用ファイル		ソフトウェア種別	SAMAC 辞書の情報を基に分類されたソフトウェアの種別です。JP1/IT Desktop Management 2 で管理するソフトウェアの情報の一つです。	×

(凡例) ○：自動取得できる ×：自動取得できない

付録 A.7 再起動によって設定が適用されるケース

JP1/IT Desktop Management 2 では、設定を適用するためにコンピュータの再起動が必要な場合があります。次の場合に、再起動が必要です。

- セキュリティポリシーを編集または割り当てた場合
- 手動でセキュリティ対策を実施した場合

セキュリティポリシーを編集した場合

次の項目のうちどれかを編集したときに、編集したセキュリティポリシーが割り当てられているコンピュータを再起動してください。() 内には、該当するセキュリティ設定項目を示します。再起動すると編集後のセキュリティポリシーがコンピュータに適用されます。

- Windows 自動更新の有効化の自動対策（更新プログラム）

- 管理共有の無効化の自動対策（OS のセキュリティ設定）
- 匿名接続の無効化の自動対策（OS のセキュリティ設定）
- Windows ファイアウォールの有効化の自動対策（OS のセキュリティ設定）
コンピュータの OS が、Windows Server 2003、および Windows XP の場合は、再起動は不要です。
- DCOM の無効化の自動対策（OS のセキュリティ設定）
- リモートデスクトップの無効化の自動対策（OS のセキュリティ設定）
- 機器の使用抑止（禁止操作）※
- 操作ログの取得（不審と見なす操作の取得を含む）の有効化または無効化（操作ログ）※

注※ 機器の使用抑止と操作ログの取得は、セキュリティポリシーが割り当てられたタイミングで適用されます。ただし、機器の使用抑止や操作ログの一部の設定は、再起動後に有効になることがあります。

セキュリティポリシーを割り当てた場合

セキュリティポリシーを割り当てたコンピュータを再起動してください。再起動すると、割り当てたセキュリティポリシーがコンピュータに適用されます。

機器の使用抑止と操作ログの取得は、セキュリティポリシーが割り当てられたタイミングで適用されます。ただし、機器の使用抑止や操作ログの一部の設定は、再起動後に有効になることがあります。

手動でセキュリティ対策を実施した場合

次の設定項目を対策した場合に、対策を実施したコンピュータを再起動してください。() 内には、該当するセキュリティ設定項目を示します。再起動すると、セキュリティ対策が実行されます。

- Windows 自動更新の有効化（更新プログラム）
- 管理共有の無効化（OS のセキュリティ設定）
- 匿名接続の無効化（OS のセキュリティ設定）
- Windows ファイアウォールの有効化（OS のセキュリティ設定）
コンピュータの OS が、Windows Server 2003、および Windows XP の場合は、再起動は不要です。
- DCOM の無効化（OS のセキュリティ設定）
- リモートデスクトップ接続の無効化（OS のセキュリティ設定）

付録 A.8 時間の取り扱い

JP1/IT Desktop Management 2 に表示されている日時は、機能ごとに異なります。表示に利用しているローカルタイムを次の表に示します。

この表に記載していない機能に表示されている日時については、基本的には、管理用サーバから実行・発生するものは管理用サーバのローカルタイムが利用されます。エージェント導入済みのコンピュータから実行・発生するものはエージェント導入済みコンピュータのローカルタイムが利用されます。

機能		表示される日時		説明
		管理用サーバのローカルタイム	エージェント導入済みのコンピュータのローカルタイム	
機器管理	登録日時	○	×	「登録日時」とは、機器情報が管理用サーバに登録された日時です。この日時は更新されません。
	管理開始日時	○	×	「管理開始日時」とは、コンピュータが管理対象となった日時です。
	更新日時	○	○	「更新日時」とは、機器情報が更新された日時です。 管理用サーバの機器情報が更新された日時は、管理用サーバのローカルタイムが表示されます。エージェント導入済みのコンピュータの機器情報が更新された日時は、エージェント導入済みのコンピュータのローカルタイムが表示されます。 最後の更新が外部記憶媒体を使用した情報通知の場合は、情報を収集した日時です。オフライン管理用のエージェント導入済みのコンピュータのローカルタイムが表示されます。
	最終接続確認日時	○	×	「最終接続確認日時」とは、コンピュータの管理用サーバへの接続が、最後に確認できた日時です。ここには、管理用サーバのローカルタイムが表示されます。 最後の接続が外部記憶媒体を使用した情報通知の場合は、日時は更新されません。通知前の日時が維持されます。
集計	操作日時	×	○	エージェント導入済みのコンピュータでのソフトウェアの起動抑止、および操作ログなど、エージェント導入済みのコンピュータのローカルタイムを利用します。
	集計日時	○	×	管理用サーバのローカルタイムで、集計を実行します。
イベント	登録日時	○	×	「登録日時」とは、発生したイベントが管理用サーバに登録された日時で

機能		表示される日時		説明
		管理用サーバのローカルタイム	エージェント導入済みのコンピュータのローカルタイム	
イベント	登録日時	○	×	す。ここには、管理用サーバのローカルタイムが表示されます。
管理用サーバからのスケジュール実行	設定画面の [機器の探索] – [探索条件の設定] で設定できる次に示す探索スケジュール - Active Directory の探索 - ネットワークの探索	○	×	管理用サーバのローカルタイムで、探索を実行します。
	設定画面の [セキュリティ管理] – [セキュリティのスケジュール設定] のスケジュール	○	×	管理用サーバのローカルタイムで、セキュリティ状況を判定します。

(凡例) ○：表示される ×：表示されない

注意事項

JP1/IT Desktop Management 2 の運用中は、JP1/IT Desktop Management 2 のシステムを構成するすべてのコンピュータで、日時を戻さないようにしてください。日時に基づいて順序性を確保している機能で、不具合が発生することがあるためです。

付録 A.9 監査ログの出力

監査ログとは、JP1/IT Desktop Management 2 を「誰が」、「いつ」、「どこで」、「どのような操作を実行したか」を示したログです。内部統制の評価と監査などに利用できます。JP1/IT Desktop Management 2 の運用上必要な情報はこのログに保管されます。なお、リモートインストールマネージャを使用した配布機能の監査ログについては、マニュアル「JP1 Version 10 JP1/IT Desktop Management 2 配布機能 運用ガイド」を参照してください。

ポイント

監査ログは、JP1/IT Desktop Management 2 をはじめ、各 JP1 製品、OS (Windows イベントログ) などからも出力されます。監査ログを JP1/Audit Management - Manager[※]で収集・管理することで、組織の内部統制の評価と監査に利用できます。

注※ JP1/Audit Management - Manager とは、監査ログを収集・管理することで、システム全体の内部統制の評価と監査を支援するプログラムです。なお、Version 9 以前の製品名称は、JP1/NETM/Audit - Manager です。

(1) 監査ログに出力される事象の種別

監査ログを出力する対象となる事象の種別、および JP1/IT Desktop Management 2 が監査ログを出力する契機を次の表に示します。事象の種別とは、監査ログに出力される事象を分類するための識別子です。

事象の種別	説明	JP1/IT Desktop Management 2 が出力する契機
StartStop	ソフトウェアの起動および終了に関する監査ログであることを示しています。	• JP1/IT Desktop Management 2 - Manager のサービスの起動および停止 • JP1/IT Desktop Management 2 - Manager のサービスの起動失敗 • JP1/IT Desktop Management 2 - Manager のサービスの異常終了
Authentication	JP1/IT Desktop Management 2 - Manager の利用者の認証結果に関する監査ログであることを示しています。	• JP1/IT Desktop Management 2 - Manager へのログインの成功および失敗 • JP1/IT Desktop Management 2 - Manager からのログアウト
ConfigurationAccess	ユーザーアカウントの登録や、エージェントのセットアップなど、管理者が実行した操作に関する監査ログであることを示しています。	• ユーザーアカウントの登録、削除 • ユーザーアカウントのロック、ロック解除 • 権限の変更 • JP1/IT Desktop Management 2 - Manager のセットアップの正常終了および異常終了 • エージェント設定の正常終了および異常終了 • ライセンス情報の登録の正常終了および異常終了 • サポートサービスサイトの ID、パスワード設定の成功および失敗 • 探索認証 ID、パスワード設定の成功および削除 • AMT 連携 ID、パスワード設定の成功および失敗

事象の種別	説明	JP1/IT Desktop Management 2 が出力する契機
ConfigurationAccess	ユーザーアカウントの登録や、エージェントのセットアップなど、管理者が実行した操作に関する監査ログであることを示しています。	• Active Directory 接続 ID、パスワードの設定および削除の成功 • メールサーバ接続 ID、パスワードの設定の成功および失敗 • 操作ログの保管先フォルダがネットワーク上にある場合の、保管先フォルダに接続するための ID とパスワードの設定の成功 • MDM 設定の追加の成功および失敗 • MDM 設定のサーバまたはプロキシの ID、パスワードの変更の成功および失敗 • MDM 設定の削除の成功および失敗 • 変更履歴の設定の正常終了および異常終了 • 保存用の変更履歴の出力先フォルダがネットワーク上にある場合の、出力先フォルダに接続するための ID とパスワードの設定の成功 • ネットワーク制御リストの自動更新の設定の変更の成功および失敗 • JP1/NETM/NM - Manager 連携の設定の成功および失敗 • 操作ログの設定変更の成功および失敗
ExternalService	Active Directory との接続、メール送信、サポートサービスサイトとの接続など、外部サービスとの通信結果に関する監査ログであることを示しています。	• Active Directory との接続の成功および失敗 • JP1/NETM/NM との接続の成功および失敗 • メール送信の成功および失敗 • サポートサービスサイトとの接続の成功および失敗 • MDM システムとの接続の成功および失敗
ContentAccess	セキュリティポリシーの変更、機器情報のエクスポート、サポートサービスからの情報取得などの操作に関する監査ログであることを示しています。	• セキュリティポリシーの変更の正常終了および異常終了 • 機器情報のエクスポートの成功および失敗 • 資産情報のインポート、エクスポートの成功

事象の種別	説明	JP1/IT Desktop Management 2 が出力する契機
ContentAccess	セキュリティポリシーの変更、機器情報のエクスポート、サポートサービスからの情報取得などの操作に関する監査ログであることを示しています。	- 資産情報のインポート、エクスポートの失敗 - 更新プログラム追加の成功および失敗 - SAMAC 辞書の情報の更新成功および更新失敗 - ウィルス対策製品情報追加の成功および失敗 - 管理者の動作定義ファイル更新の成功および失敗 - エージェント更新の成功および失敗 - 操作ログ削除の成功および失敗
Maintenance	データベース操作に関する監査ログであることを示しています。	- データベースのバックアップの成功および失敗 - データベースのリストアの成功および失敗 - データベース再編成の成功および失敗
ManagementAction	セキュリティ状況の判定結果とアクション項目の実行結果、スマートデバイスに対するアクション項目の実行結果に関する監査ログであることを示しています。	- セキュリティ状況の判定結果およびアクション項目の実行結果 - スマートデバイスに対するアクション項目の実行結果

(2) 監査ログの出力形式

監査ログの出力形式は、監査ログのフォーマットであることを示す「CALFHM」、監査ログのリビジョン番号、該当する出力項目の順で出力されます。監査ログの出力項目に出力される値および内容を次の表に示します。

出力項目		値	内容
項目名	出力される属性名		
共通仕様識別子	—	「CALFHM」	監査ログのフォーマットであることを示す識別子
共通仕様リビジョン番号	—	1.0	監査ログを管理するためのリビジョン番号
通番	seqnum	通番	監査ログの通し番号
メッセージ ID	msgid	公開メッセージ ID	製品ごとのメッセージ ID
日付、時刻	date	ログ出力日時	YYYY-MM-DDThh:mm:ss.sssTZD • YYYY：年（数字 4 バイト）

出力項目		値	内容
項目名	出力される属性名		
日付、時刻	date	ログ出力日時	• MM：月（数字 2 バイト） • DD：日（数字 2 バイト） • T：区切り文字（固定） • hh：時（数字 2 バイト） • mm：分（数字 2 バイト） • ss：秒（数字 2 バイト） • sss：ミリ秒（数字 3 バイト） • TZD：タイムゾーン
発生プログラム名	progid	JP1/ITDM2	事象が発生したプログラム名
発生コンポーネント名	compid	次のどれかが出力されます。 • Installer（インストーラー） • Setup（セットアップ） • Gui（GUI） • Api（API） • ManagerService（マネージャサービス） • Utility（ユーティリティ） • AgentControl（エージェント制御） • Agent（エージェント）	事象が発生したコンポーネント名
発生プロセス ID	pid	プロセスの ID	事象の発生を検出したプロセス ID
発生場所	ocp:ipv4 または ocp:host	管理用サーバの IP アドレスまたはコンピュータ名	事象が発生したサーバの IP アドレスまたはホストのコンピュータ名
監査事象の種別	ctgry	次のどれかが出力されます。 • StartStop • Authentication • ConfigurationAccess • ExternalService • ContentAccess • Maintenance • ManagementAction	監査ログに出力される事象を分類するための識別子
監査事象の結果	result	次のどれかが出力されます。 • Success（成功） • Failure（失敗） • Occurrence（発生（成功または失敗以外））	発生した事象の結果

出力項目		値	内容
項目名	出力される属性名		
サブジェクト識別子	subj:uid または subj:euid	ユーザーアカウントまたは Administrator	事象を発生させたユーザーの情報
オブジェクト情報	obj	次のどれかが出力されます。 • User (ユーザーアカウント) • Role (権限) • Setup (JP1/IT Desktop Management 2 - Manager のセットアップ) • Config (エージェント設定) • Policy (セキュリティポリシー) • DeviceInfo (機器情報) • DataBase (データベース) • UpdateInfo (更新プログラム情報) • AntivirusInfo (ウィルス対策製品情報) • ActionDefinition (JP1/IT Desktop Management 2 - Manager の動作定義ファイル) • Agent (エージェント) • AssetInfo (資産情報) • SecurityInfo (操作ログ)	事象を発生させたオブジェクト情報
動作情報	op	次のどれかが出力されます。 • Start (起動) • Stop (停止) • Login (ログイン) • Logout (ログアウト) • Add (登録) • Update (変更) • Delete (削除) • Request (接続要求) • Response (応答) • Import (インポート) • Export (エクスポート) • Backup (バックアップ) • Maintain (再編成) • Recovery (リストア)	事象を発生させたユーザーの動作の情報
権限情報	auth	次のどちらかが出力されます。 • JP1/IT Desktop Management 2 のユーザー権限 • Administrator (OS 権限)	権限が取得できない場合は出力されません。

出力項目		値	内容
項目名	出力される属性名		
リクエスト送信元	from:ipv4	操作画面を操作するコンピュータの IP アドレス	事象が発生したサーバの IP アドレス
メッセージテキスト	msg	任意のメッセージ	事象の内容を示すメッセージ

(凡例) - : 該当なし

(3) 監査ログの保存形式

監査ログの保存形式について説明します。監査ログは、JDNAUDTn.LOG (n : 1 ~ 9) に出力されます。

ログファイル (JDNAUDTn.LOG) が一定の容量に達すると、監査ログの出力先ファイルが変わります。例えば、JDNAUDT1.LOG が一定の容量に達すると、JDNAUDT2.LOG に監査ログを出力します。このように監査ログの出力先ファイルが順次変わります。JDNAUDT9.LOG が一定の容量に達した場合、JDNAUDT1.LOG に格納されている監査ログを削除してから、JDNAUDT1.LOG に監査ログを出力します。

付録 A.10 各バージョンの変更内容

10-50 の変更内容

- resetnid.vbs (ホスト識別子のリセット) コマンドでリターンコードを表示させる方法を追記し、使用例を修正した。
- サイトサーバ構成システムの機能を削除し、リモートインストールマネージャを使用した配布を利用する場合に必要なシステムとして、中継システムを追加した。
- リモートインストールマネージャを使用した配布機能によって、管理対象のコンピュータの条件や、コンピュータでの動作を詳細に指定して配布できるようにした。
- ネットワーク装置を含めたハードウェア情報、ソフトウェア情報、契約情報などをデータベースで一元管理できるようにした。
- 管理対象のコンピュータに格納されているファイルを一括で収集できるようにした。
- 次のデバイスの使用を抑止できるようにした。
 - Bluetooth デバイス
 - イメージングデバイス
 - Windows ポータブルデバイス

また、Windows 8、Windows Server 2012、Windows 7、Windows Server 2008、および Windows Vista でリムーバブルディスクとして使用を抑止していた次のデバイスをデバイスの種類ごとに抑止できるようにした。

- USB デバイス
- IEEE1394 デバイス
- 内蔵 SD カード
- 使用を許可した USB デバイスに格納されているファイル一覧の取得を選択できるようにした。
- 機器の使用を抑止したことを示すメッセージを、利用者のコンピュータに表示するかどうかを設定できるようにした。
- [機器の管理を始めましょう] ウィザードでは、エージェントをインストールする方法で機器を管理できるようにした。
- マルチサーバ構成システムの機能を削除し、1 台の管理用サーバで 30,000 台の機器を管理できるようにした。
- 次の操作に関わる操作ログを取得する条件を設定できるようにした。
 - ファイル操作
 - プログラムの起動と停止
 - ウィンドウ操作
- デバイス接続許可の操作ログを取得できるようにした。
- 禁止操作の抑止イベントと操作ログを上位システムに通知する間隔、および利用者のコンピュータ側で保持する期間の最大値を設定できるようにした。
- 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。
- 製品構成の変更に伴い、インストール、セットアップ、およびエージェント設定の設定内容を変更した。
- Windows 8.1 および Windows Server 2012 R2 を次の製品の適用 OS に追加した。
 - JP1/IT Desktop Management 2 - Manager
 - JP1/IT Desktop Management 2 - Agent
 - JP1/IT Desktop Management 2 - Network Monitor
- Windows 8、Windows 7 を次の製品の適用 OS 外とした。
 - JP1/IT Desktop Management 2 - Manager
- Windows 2000 を次の製品の適用 OS 外とした。
 - JP1/IT Desktop Management 2 - Agent
- サポートする Internet Explorer のバージョンを変更した。
- 一部のポート番号を変更した。
- 次のイベントを追加した。
 - 1011、1138、1139、1140
- 次のイベントを変更した。

1032、1033、1034、1076

- 次のイベントを削除した。

1010、1121

- ネットワーク共有プリンタに対して、印刷の操作ログの取得、および印刷の抑止ができなくなった。
- リモートコントロールのエージェント設定の接続モードについて制御モードと監視モードの表記を入れ替えた。これに伴い、接続モードの決定方式の説明を変更した。
- 監査ログの出力内容を変更した。
- コマンド実行中のフェールオーバー後の対処方法に次の項目を追記した。
 - ioutils exportdevice (機器情報のエクスポート)
 - ioutils exportdevicedetail (詳細な機器情報のエクスポート)
 - ioassetsfieldutil export (共通管理項目と追加管理項目の定義のエクスポート)
- ioutils importasset コマンドで CSV ファイルをインポートするときの値の扱いを追記した。

10-10 の変更内容

- ネットワークに接続されている機器の探索で、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する必要があることを追記した。
- セキュリティ画面および機器画面で、任意の条件に従って管理対象のコンピュータを自動で振り分けられるグループを作成できるようにした。
- タスクトレイの JP1/IT Desktop Management のアイコンに表示されるバルーンヒントと、利用者情報の入力画面を、利用者のコンピュータに表示させるかどうかを選択できるようにした。
- ネットワーク制御リストの自動更新について、すべての自動更新を有効にするか、自動更新のうち追加だけを有効にするかを設定できるようにした。
- JP1/NETM/NM - Manager と連携することで、JP1/NETM/NM を導入したアプライアンス製品で監視しているネットワーク接続を JP1/IT Desktop Management から制御できるようにした。
- 管理用サーバにサーバ証明書をインポートしたあとに、MDM システムのサーバ証明書を変更する場合の説明を追加した。また、MDM システムと連携するための情報を設定する手順の Internet Explorer のバージョンの記述を削除した。また、JP1 スマートデバイス管理サービスと連携する場合の設定について追記した。
- コマンドの実行権限に関する記載を「[17.1 コマンドを実行する手順](#)」に集約した。また、getinv.vbs コマンド以外のコマンドを実行する場合で、OS のユーザーアカウント制御 (UAC) が有効なときの説明を追記した。
- コマンド実行中の注意事項を記載した。
- ioutils importfield コマンドに戻り値「1」を追加した。
- ioutils exportoplog コマンドを利用して操作ログをエクスポートしたときの CSV ファイルの出力形式を記載した。

- resetnid.vbs コマンドに /i オプションを追加して、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が表示されるようにした。
- 障害発生時に対処が必要なイベントとして、次のイベントを追加した。
1059
- 次のメッセージを追加した。
KDEX1598-E、KDEX3319-I、KDEX3320-E、KDEX3321-I、KDEX3322-E、KDEX4126-W、
KDEX5305-I、KDEX5306-E、KDEX5464-I、KDEX5465-I、KDEX5466-E、KDEX5467-E、
KDEX5468-E、KDEX5469-E、KDEX5470-E、KDEX5471-E
- 次のメッセージを変更した。
KDEX1534-W、KDEX1557-W、KDEX1576-W、KDEX1583-W、KDEX4010-E、KDEX4387-E、
KDEX4388-E、KDEX4389-E、KDEX4390-E、KDEX4391-E、KDEX4392-E、KDEX4394-E、
KDEX4395-E、KDEX4396-E、KDEX4397-E、KDEX4398-W
- 次のメッセージを削除した。
KDEX6321-E
- 次のイベントを追加した。
1134、1135、1136、1137
- 次のイベントを変更した。
19
- 次のイベントの、JP1 イベントの属性を追加した。
1135、1136、1137
- 次のイベントの、JP1 イベントの属性を変更した。
1118
- ポートの設定についての説明を修正した。また、JP1/IT Desktop Management - Remote Site Server
とエージェントレスのコンピュータ間のネットワークの説明を追記した。
- 機器一覧に表示される、登録日時および管理開始日時について説明を追記した。

10-02 の変更内容

- セキュリティポリシーにコンピュータのセキュリティ設定に関する任意のポリシーを追加し、任意の判定条件でセキュリティ判定できるようにした。
- 機器情報の変更履歴を取得できるようにした。
- [ソフトウェアライセンス状況] 画面で、管理ソフトウェアごとにソフトウェアライセンスの利用状況を管理できるようにした。
- 職制変更に伴い部署の定義を変更する流れを記載した。
- メニューエリアに表示されるグループのうち、定義から削除した部署および設置場所を一括で削除できるようにした。
- 利用者が利用者情報の入力を開始できる日時を、システム管理者が設定画面で設定できるようにした。

- ユーザーアカウントに設定した管轄範囲に合わせて、ソフトウェアライセンスおよび契約の表示範囲を限定できるようにした。
- 次のプログラムの適用 OS に、Windows 8 および Windows Server 2012 を追加した。
 - JP1/IT Desktop Management - Manager
 - JP1/IT Desktop Management - Remote Site Server
 - JP1/IT Desktop Management - Network Monitor
- エージェント導入済みのコンピュータでコマンドを実行する手順を追記した。
- 資産管理項目の定義を、CSV 形式でエクスポートおよびインポートできるようにした。
- `ioutils exportoplog` コマンドの `-filter` オプションを指定する際の注意事項を追記した。
- 次のコマンドで指定するフォルダ名に使用できる文字についての説明を追記した。
 - `exportdb` コマンド
 - `importdb` コマンド
 - `reorgdb` コマンド
 - `getlogs` コマンド
 - `getinstlogs` コマンド
- サイトサーバをインストールしたコンピュータでホスト識別子をリセットする場合の手順を記載した。
- 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よう、注意事項を記載した。
- 次のメッセージを追加した。
KDEX1597-E、KDEX4387-E、KDEX4388-E、KDEX4389-E、KDEX4390-E、KDEX4391-E、KDEX4392-E、KDEX4393-E、KDEX4394-E、KDEX4395-E、KDEX4396-E、KDEX4397-E、KDEX4398-W、KDEX4399-I、KDEX4400-E、KDEX4401-E、KDEX4402-E、KDEX4403-E、KDEX5460-I、KDEX5461-I、KDEX5462-E、KDEX5463-E
- 次のメッセージを削除した。
KDEX1543-E、KDEX4065-E
- 次のイベントを追加した。
1127、1128、1129、1130、1131、1132、1133
- 次のイベントを削除した。
50、51、52
- 次のイベントを変更した。
1079、1082

10-01 の変更内容

- JP1/IT Desktop Management - Agent の適用 OS に、Windows 8 および Windows Server 2012 を追加した。

- CD-R をエージェントインストール用の媒体にする場合に、Autorun.inf を使用してエージェントのインストールを自動で開始できることを記載した。
- 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。
- ファイル持ち出しによる不審と見なす操作と、印刷による不審と見なす操作で、画面表示や調査方法などが異なることを明記した。
- `recreatelogdb` コマンドについての注意事項を訂正した。
- Internet Explorer 9 で JP1/IT Desktop Management の操作画面を操作する場合の注意事項を記載した。
- 操作画面を開いたときやログインしたときに「異常なリクエスト」または「予期せぬエラー」のダイアログが表示される場合の対処方法を記載した。
- サイトサーバおよびネットワークモニタを有効化するコンピュータのエージェント設定を編集する手順を記載した。
- ウィルス対策製品情報を含むサポートサービスの情報を取得して、JP1/IT Desktop Management の情報を更新できるようにした。
- MDM システムと連携するための情報を設定する方法を訂正した。
- Windows のタスクに JP1/IT Desktop Management のコマンドを登録する場合の参考情報を訂正した。
- `ioutils exportoplog` コマンドを実行できるサーバの説明を訂正した。
- 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、JP1/IT Desktop Management の情報を更新できるようにした。
- `getlogs` コマンドでメッセージ (KDEX4041-E) が出力される場合の注意事項を記載した。
- `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の参考情報の説明を改善した。
- 次のメッセージを追加した。
KDEX1005-W、KDEX1036-W、KDEX1076-E、KDEX1543-E、KDEX1594-E、KDEX3029-E、KDEX3030-I、KDEX4203-E、KDEX4270-I、KDEX4287-E、KDEX5401-E、KDEX5437-I、KDEX5438-E、KDEX5440-E、KDEX5450-E、KDEX5451-E、KDEX5452-E、KDEX5453-E、KDEX5454-E、KDEX5455-E、KDEX5456-E
- 次のメッセージを変更した。
KDEX4023-E、KDEX4073-I、KDEX4204-E、KDEX4220-E、KDEX4295-E、KDEX4378-Q、KDEX5336-I、KDEX5337-E、KDEX5338-E、KDEX5339-E、KDEX5340-I、KDEX5341-E、KDEX5342-E、KDEX5346-E、KDEX5385-I、KDEX5386-E、KDEX5387-E、KDEX5388-E、KDEX5389-I、KDEX5390-E、KDEX5391-E、KDEX5392-E、KDEX5393-E、KDEX5394-E、KDEX5396-I、KDEX5397-E、KDEX5407-E、KDEX5414-E、KDEX5415-E、KDEX5423-E、

KDEX5426-E、KDEX5427-E、KDEX5428-E、KDEX5430-E、KDEX5431-I、KDEX5432-I、KDEX5435-E、KDEX6112-E、KDEX6113-E、KDEX6115-E、KDEX6132-E、KDEX6151-E、KDEX6152-E、KDEX8006-E、KDEX8019-E、KDEX8022-W、KDEX8024-W、KDEX8028-E

- 次のイベントを追加した。
1117、1118、1123、1124
- 次のイベントを削除した。
1107、1108
- JP1/IM と連携する場合に、JP1/IM に表示される JP1 イベント ID を記載した。
- JP1/IM と連携する場合に、イベント「1118」を JP1 イベントとして JP1/IM に出力できるようにした。
- JP1 イベントの属性を記載した。
- JP1/IT Desktop Management - Manager で使用するポート番号を、シングルサーバ構成の場合とマルチサーバ構成の場合に分けて記載した。
- 操作ログまたは禁止操作のアップロード時にエージェント導入済みのコンピュータの電源が OFF である場合は、そのコンピュータの電源が ON になったあとにアップロードされることを記載した。
- 監査ログを収集・管理することで、システム全体の内部統制の評価と監査を支援するプログラムの名称を、JP1/Audit Management - Manager に変更した。
- ContentAccess の監査ログが出力される契機に、「SAMAC 辞書の情報の更新成功および更新失敗」を追加した。

10-00 の変更内容

- マルチサーバ構成システムでの運用によって、最大で 50,000 台の機器を管理できるようにした。
- ユーザーアカウントに設定した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。
- 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。
- MDM サービスと連携してスマートデバイスを管理できるようにした。
- JP1/IM と連携して、JP1 イベントを通知できるようにした。
- 操作画面の一覧をページごとに表示できるようにした。
- 簡易フィルタを適用および解除する方法を変更した。
- セキュリティポリシーの適用やセキュリティの自動対策で変更した、管理対象のコンピュータのセキュリティ設定項目を、変更前の状態に戻す手順を記載した。
- ディスクコピーでエージェントを導入する際に、複数の機器が 1 つの機器として識別されてしまった場合の対処方法を記載した。
- ネットワーク制御リストに自動で追加された機器を、ネットワーク制御リストから削除する方法を記載した。
- ネットワークモニタ機能によって発見された機器を削除した場合、ネットワークをいったん切断して再接続しないと、その機器は再発見できないことを記載した。

- ネットワーク監視機能の監視対象を明記した。
- 設定画面の [エージェント] – [エージェント設定] 画面では、OS が Windows 2000、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、[エージェントをインストールする際の、管理者権限を持つアカウントを設定する] の設定が有効になることを記載した。
- ネットワークモニタの設定で未登録機器のネットワーク接続を禁止している場合の、機器の発見とエージェントの配信についての注意事項を訂正した。
- JP1/IT Desktop Management のログイン画面の URL を記載した。
- JP1/IT Desktop Management のダイアログを表示したまま [OK] ボタンをクリックしない状態で 60 分以上続けると、タイムアウトが発生することを記載した。
- ハードウェア資産情報に関連づけている機器情報の [ホスト名] を変更しても、ハードウェア資産情報の [機器名称] は自動で変更されないことを記載した。
- システム管理者が追加した資産状態または契約状態のうち、フィルタ条件として保存している資産状態または契約状態は、削除できないことを記載した。
- インポート時にマッピングキーにできるシリアルナンバーは、BIOS 情報であることを記載した。
- [部署] または [設置場所] のデータ型は変更できるが、それ以外の追加した資産管理項目は、一度設定したデータ型をほかのデータ型に変更できないことを記載した。
- `resetnid.vbs` コマンドを実行してから新規のホスト名が生成されるまでに掛かる時間を記載した。
- `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。
- ネットワーク制御リストに登録する IP アドレスおよび MAC アドレスに関する注意事項を記載した。
- メッセージを追加した。
KDEX1077-E、KDEX1078-W、KDEX1581-E、KDEX1582-W、KDEX1583-W、KDEX1584-E、KDEX1587-Q、KDEX1588-Q、KDEX1589-Q、KDEX1590-E、KDEX1591-W、KDEX1592-E、KDEX1593-E、KDEX4074-E、KDEX4075-E、KDEX4076-E、KDEX4202-E、KDEX4215-Q、KDEX4216-Q、KDEX4233-E、KDEX5399-E、KDEX5400-E、KDEX5435-E、KDEX5436-E、KDEX6119-E、KDEX6151-E、KDEX6152-E、KDEX6511-E
- メッセージの内容を変更した。
KDEX1505-E、KDEX1506-E、KDEX4020-E、KDEX4023-E、KDEX4085-I、KDEX4100-E、KDEX4221-E、KDEX5071-W、KDEX5407-E、KDEX5415-E、KDEX5423-E、KDEX5426-E、KDEX5427-E、KDEX5428-E、KDEX5430-E、KDEX5431-I、KDEX5432-I、KDEX8003-I、KDEX8022-W、KDEX8030-E
- イベント（イベント番号 1120、1121、1122）を追加した。
- イベント（イベント番号 1107、1108）の内容を変更した。
- 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を修正した。
- 管理用サーバとエージェント間の通信発生の契機を訂正した。

- 管理用サーバが更新プログラムの情報が更新されているかどうかを確認するタイミングについての説明を訂正した。
- サポートサービスから更新情報を自動取得するための条件を訂正した。
- セキュリティポリシーの「禁止操作」で「機器の操作抑止」を編集した場合に、そのセキュリティポリシーが割り当てられているコンピュータを再起動する必要があることを記載した。
- 監査ログに出力される事象の種別に対応する、説明および JP1/IT Desktop Management が出力する契機を訂正した。
- 監査ログのオブジェクト情報として出力される値に、次の項目を記載した。
 - UpdateInfo（更新プログラム情報）
 - AntivirusInfo（ウィルス対策製品情報）
 - ActionDefinition（JP1/ITDesktop Management -Manager の動作定義ファイル）
 - Agent（エージェント）
 - AssetInfo（資産情報）
- 監査ログのリクエスト送信元として出力される値を訂正した。
- 監査ログの保存形式についての説明を訂正した。
- 次の情報をマニュアル「JP1 Version 10 JP1/IT Desktop Management 導入・設計ガイド」に集約した。
 - マイクロソフト製品の表記について
 - マニュアルで使用しているアイコンと書式について
 - オンラインヘルプについて
 - 関連マニュアル
 - 関連ドキュメント
 - このマニュアルでの表記
 - このマニュアルで使用する英略語
 - KB（キロバイト）などの単位表記について
 - 用語解説

09-51 の変更内容

- MDM 製品と連携してスマートデバイスを管理できるようにした。
- 管理ソフトウェア情報に、インストールされている機器の総数（ライセンス消費数）を表示するようにした。
- ログイン時にパスワードの変更が要求されるタイミングを記載した。また、パスワードを設定してから 180 日が経過すると、ログイン時にパスワードの変更が必要になることを記載した。
- ログアウトする手順を記載した。

- ユーザーアカウントのロックを解除する手順を記載した。
- メニューエリアから部署および設置場所の定義を編集するアイコンを変更した。また、部署および設置場所の定義を追加、編集および削除する手順を記載した。
- 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。また、部署および設置場所の名称を変更する手順を記載した。
- 部署および設置場所を削除する手順を記載した。
- ネットワークモニタを有効にしていないネットワークセグメントでは、[ネットワークへの接続] が「許可しない」と表示されていても、コンピュータのネットワーク接続は遮断されないことを、注意事項として記載した。
- ネットワーク制御のアクション項目を設定している場合、エージェント導入済みのコンピュータは、再接続後にセキュリティの判定に従ってネットワーク接続が制御されることを記載した。
- 製品単位で認識される USB デバイスを登録する場合と、個別に認識される USB デバイスを登録する場合の説明を記載した。
- `deletelog` コマンドを使って、サイトサーバに保管されている不要な操作ログを削除できるようにした。
- ハードウェア資産情報の CSV ファイルに空の値が含まれる場合、インポートしても更新されないことを記載した。
- 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。
- 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)」または「ドメイン名¥ユーザー ID」の形式で指定することを記載した。
- 言語ごとの部署・設置場所の表示名を設定する手順を記載した。
- `ioutils importfield` コマンドは、インポートによる項目の追加だけができることを記載した。対処が必要なイベントに、イベント番号が 1085～1116 のイベントを追加した。
- メッセージを追加した。
KDEX3299-I、KDEX3300-E、KDEX3301-I、KDEX3302-E、KDEX3303-I、KDEX3304-E、
KDEX5104-I、KDEX5396-I、KDEX5397-E、KDEX5402-I、KDEX5403-E、KDEX5404-E、
KDEX5405-E、KDEX5406-E、KDEX5407-E、KDEX5409-E、KDEX5410-I、KDEX5411-E、
KDEX5412-E、KDEX5413-E、KDEX5414-E、KDEX5415-E、KDEX5417-E、KDEX5418-I、
KDEX5419-E、KDEX5420-E、KDEX5421-E、KDEX5422-E、KDEX5423-E、KDEX5425-E、
KDEX5426-E、KDEX5427-E、KDEX5428-E、KDEX5430-E、KDEX5431-I、KDEX5432-I、
KDEX5434-E、KDEX8031-I、KDEX8032-W、KDEX8033-E、KDEX8034-E、KDEX8035-W、
KDEX8036-E、KDEX8037-E、KDEX8038-E、KDEX8039-E
- メッセージの内容を変更した。
KDEX5000-I、KDEX5010-W
- イベント（イベント番号：1105～1116）を追加した。

索引

A

Active Directory に登録されている機器の探索手順 25, 248

Active Directory の接続設定手順 527

Active Directory の探索条件の設定手順 499

Active Directory 連携時のトラブルシューティング手順 670

addfwlist.bat コマンド 619

AMT の認証情報の設定手順 520

AVI 形式への録画ファイルの変換手順 332

C

CSV ファイルが正しく表示されない場合の対処 640

E

exportdb コマンド 600

G

getinstlogs コマンド 617

getinv.vbs コマンド 624

getlogs コマンド 615

I

importdb コマンド 604

ioassetsfieldutil export (共通管理項目と追加管理項目の定義のエクスポート) 626

ioassetsfieldutil import (共通管理項目と追加管理項目の定義のインポート) 629

ioutils exportasset コマンド 549

ioutils exportdevicedetail コマンド 571

ioutils exportdevice コマンド 568

ioutils exportfield コマンド 556

ioutils exportfilter コマンド 590

ioutils exporttoplog コマンド 586

ioutils exportpolicy コマンド 574

ioutils exporttemplate コマンド 562

ioutils exportupdategroup コマンド 580

ioutils importasset コマンド 552

ioutils importfield コマンド 559

ioutils importfilter コマンド 594

ioutils importpolicy コマンド 577

ioutils importtemplate コマンド 565

ioutils importupdategroup コマンド 583

IP アドレスを直接指定したリモートコントロールの開始手順 292

J

JP1/NETM/NM - Manager 連携の設定を有効にする手順 364

M

MDM システムと連携するための情報を設定する手順 529

MDM システムを導入する流れ 63

MDM 連携時のトラブルシューティング 671

R

reorgdb コマンド 608

resetnid.vbs コマンド 621

S

SNMP の認証情報 500

startservice コマンド 613

stopservice コマンド 611

U

updatesupportinfo コマンド 597

USB デバイスの使用許可 383

USB デバイスの使用の制限 121

USB デバイスの使用履歴の確認 124

USB デバイスの登録手順 383

USB デバイスの紛失への対応 126

USB デバイスの利用者への貸し出し 123

W

Windows の管理共有の認証情報 500

あ

- 新しい機器を配布する流れ 147
- 新しいスマートデバイスを利用者に配布する流れ 68
- アンインストールするソフトウェアの調査 196
- アンインストール手順 [コントローラ] 288
- アンインストール手順 [ソフトウェア] - [機器画面] 270
- アンインストール [ソフトウェア] - [配布 (ITDM 互換) 画面] 195

い

- 一時的に機器のネットワーク接続を許可する流れ 100
- 一覧の表示項目の変更手順 228
- イベント一覧 675
- イベント詳細の確認手順 484
- イベント情報のエクスポート手順 485
- イベント情報のコピー 484
- イベント通知の設定手順 524
- イベントの参照 483
- イベントの設定 524
- 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] 617
- インストール状況を管理するための設定 167
- インストールセットの作成手順 32, 246
- インストール手順 [コントローラ] 286
- インストールの延期 [配布機能] 481
- インストール [ソフトウェア] - [配布 (ITDM 互換) 画面] 186
- インポート 455
- インポート手順 [管理ソフトウェア情報] 458
- インポート手順 [契約会社リスト] 461
- インポート手順 [契約情報] 459
- インポート手順 [ソフトウェア検索条件] 519
- インポート手順 [ソフトウェアライセンス情報] 456
- インポート手順 [ハードウェア資産情報] 455

う

- ウィザード [[機器の管理を始めましょう] ウィザード] 244
- ウィザード [[ソフトウェアをアンインストールしましょう] ウィザード] 198, 469
- ウィザード [[ソフトウェアをインストールしましょう] ウィザード] 189, 465
- ウィザード [[ファイルを配布しましょう] ウィザード] 193, 467
- ウィルスが発見された機器のネットワーク接続を遮断する流れ 96
- ウィルスが発見されたコンピュータの確認 116
- ウィルス感染時に機器のネットワーク接続を遮断する流れ 95
- ウィルス感染時の確認 116
- ウィルス対策状況の確認 117
- 運用時のトラブルシューティングの流れ 634

え

- エージェント設定の解除手順 495
- エージェント設定の管理 492
- エージェント設定の削除手順 494
- エージェント設定の追加手順 493
- エージェント設定の編集手順 493
- エージェント設定の割り当て手順 495
- エージェントと管理用サーバ間の通信 715
- エージェントのインストール状況を確認する流れ 48
- エージェントのインストール [自動] 42
- エージェントのインストール [手動] 31
- エージェントの設定 492
- エージェントの導入 23
- エージェントの導入計画 30
- エージェントの導入方法 34
- エージェントの導入 [Web サーバで公開] 35
- エージェントの導入 [ディスクコピー] 40
- エージェントの導入 [媒体で配布] 37
- エージェントの導入 [ファイルサーバで公開] 36
- エージェントの導入 [メールで配布] 38
- エージェントの導入 [ログオンスクリプト] 39
- エージェントのトラブルシューティング手順 665

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〕 47

エージェントを導入する流れ〔オフライン管理したい
コンピュータ〕 51

エクスポートした操作ログの出力形式 716

エクスポート手順〔イベント情報〕 485

エクスポート手順〔機器情報〕 266

エクスポート手順〔契約会社リスト〕 515

エクスポート手順〔ソフトウェア検索条件〕 519

エクスポート手順〔ソフトウェア情報〕 267

エクスポート手順〔タスク情報〕 480

エクスポート手順〔パッケージ情報〕 472

遠隔地にあるサーバに接続する流れ 85

遠隔地にあるサーバの環境設定を変更する流れ 86

遠隔地にあるサーバを運用する流れ 85

遠隔地にいる利用者に作業を指示する流れ 87

お

オートスクロールでリモートコントロールする手順
303

オプションの設定 345

オフライン管理 50

オフライン管理からオンライン管理への切り替え手順
253

オフライン管理したいコンピュータにエージェントを
導入する流れ 51

オフライン管理の情報収集〔getinv.vbs コマンド〕
624

オフライン更新〔サポートサービスからの情報〕 722

オンライン管理からオフライン管理への切り替え手順
254

か

開始日の設定手順〔レポート〕 522

外部記憶媒体を利用した機器情報の取得の流れ〔オフ
ライン管理のコンピュータ〕 52

過去の操作ログの取り込み手順 405

過去の操作ログを取り込む 405

カスタムグループからの情報の削除手順 238

カスタムグループの管理 235

カスタムグループの削除手順 236

カスタムグループの追加手順 235

カスタムグループへの情報の追加手順 237

カスタムグループ名の変更手順 236

画面の共通操作 230

画面の更新手順 227

画面の整列 303

画面の保存 305

管轄範囲の削除手順 223

管轄範囲の追加手順 222

環境設定の変更手順〔コントローラ〕 289

監査ログに出力される事象の種別 727

監査ログの出力形式 729

監査ログの保存形式 732

制御モードの強制解除 334

管理ソフトウェア情報のインポート手順 458

管理ソフトウェア情報の削除手順 437

管理ソフトウェア情報の追加手順 436

管理ソフトウェア情報の編集手順 437

管理対象の機器の確認手順 46, 503

管理対象のコンピューター一覧の出力 129

管理対象の設定手順 251

管理台帳の登録 138

管理用サーバとエージェント間の通信 715

管理用サーバのトラブルシューティング 645

管理〔エージェント設定〕 492

管理〔カスタムグループ〕 235

管理〔機器〕 243

管理〔契約会社情報〕 513

管理〔更新プログラム〕 385

管理〔資産〕 413

管理〔スマートデバイス〕 61, 64

管理〔セキュリティ状況〕 102, 365

管理〔セキュリティポリシー〕 105

管理〔操作ログ〕 397

管理〔タスク〕 474

管理〔特例接続〕 362

管理〔ネットワーク制御リスト〕 359

管理〔ネットワーク接続〕 346

管理 [ネットワークモニタ設定] 356
管理 [パッケージ] 471
管理 [フィルタ] 239
管理 [ユーザーアカウント] 215
関連づけ手順 [契約対象のソフトウェアライセンス] 453
関連づけ手順 [契約対象のハードウェア資産] 453
関連づけ手順 [ソフトウェアライセンスの契約情報] 448
関連づけ手順 [ハードウェア資産の契約情報] 426
関連づけ手順 [複数のハードウェア資産情報] 427

き

キーボードの入力バーの表示 300
キーボードの入力バーの表示の切り替え 303
期間を指定して機器のネットワーク接続を許可する流れ 100
機器が発見されない場合の対処 636
機器管理の設定 517
機器情報 (最新) の取得手順 257
機器情報のエクスポート手順 266
機器情報のエクスポート [ioutils exportdevice コマンド] 568
機器情報の代表の設定手順 [ハードウェア資産情報] 429
機器情報の通知手順 260
機器情報の編集手順 256
機器の管理 243
[機器の管理を始めましょう] ウィザード 244
機器の管理を始める方法 244
機器の検知 27
機器の購入 142
機器の削除手順 255
機器の資産情報を登録する流れ 143
機器の障害に対応する流れ 157
機器の探索の設定 498
機器のネットワーク接続状況のリアルタイム監視 94
機器のネットワーク接続の管理 89
機器の把握 24
機器のリモートコントロール 81, 285

機器の利用状況を調査する流れ 153
機器を購入する流れ 141
機器を棚卸する流れ 149
機器を廃棄する流れ 80, 156
機器を減却する流れ 155
機器をリプレイスする流れ 145
機器を利用者に配布する流れ 145
旧体制だけで使われていた情報を削除する流れ 205
旧体制で使われていた階層の削除手順 282, 432, 512
共通管理項目と追加管理項目の定義のインポートに失敗した場合のトラブルシューティング 641
共通管理項目と追加管理項目の定義のインポートファイルの設定項目 720
共通管理項目と追加管理項目の定義のインポート [ioassetsfieldutil import コマンド] 629
共通管理項目と追加管理項目の定義のエクスポート [ioassetsfieldutil export コマンド] 626
共通操作 230
許可した USB デバイス以外の使用の抑止 123
許可したソフトウェアだけ利用できるようにする流れ 118
許可なく利用されているソフトウェアライセンスを対処する流れ 170
禁止操作の抑止イベントと操作ログを上位システムに通知する間隔を設定する手順 395
禁止操作の抑止イベントと操作ログを保持する期間を設定する手順 396
禁止操作の抑止状況を出力する流れ 129

け

契約会社情報の管理 513
契約会社情報の削除手順 514
契約会社情報の追加手順 513
契約会社情報の編集手順 514
契約会社リストのインポート手順 461
契約会社リストのエクスポート手順 515
契約状態の追加手順 451
契約状態の変更手順 452
契約情報 (満了) の把握 178
契約情報のインポート手順 459

契約情報の関連づけ手順〔ソフトウェアライセンス〕
448

契約情報の関連づけ手順〔ハードウェア資産〕 426

契約情報の削除手順 450

契約情報の追加手順 449

契約情報の編集手順 449

契約情報の利用 449

契約の更改 179

契約の終了 180

検知された不審操作を調査する流れ 131

現品確認できなかった機器を調査する流れ 151

現品確認できなかったソフトウェアライセンスを調査する流れ 175

現品確認の結果を反映する流れ〔機器の棚卸〕 150

現品確認の結果を反映する流れ〔ソフトウェアライセンスの棚卸〕 174

現品確認を実施する流れ〔機器の棚卸〕 150

現品確認を実施する流れ〔ソフトウェアライセンスの棚卸〕 173

こ

更新手順〔画面〕 227

更新手順〔機器情報〕 257

更新頻度の設定手順〔エージェントレス〕 496

更新プログラム一覧への更新プログラムの手動追加手順 387

更新プログラムグループからの更新プログラムの削除手順 394

更新プログラムグループの削除手順 392

更新プログラムグループの作成手順 390

更新プログラムグループの設定のインポート〔ioutils importupdategroup コマンド〕 583

更新プログラムグループの設定のエクスポート〔ioutils exportupdategroup コマンド〕 580

更新プログラムグループへの更新プログラムの追加手順 393

更新プログラムグループ名の変更手順 391

更新プログラムの管理 385

更新プログラムの最新情報を取得する方法 109

更新プログラムの手動登録手順 387

更新プログラムの適用状況を確認する流れ 112, 115

更新プログラムの配布手順〔自動〕 385

更新プログラムの配布手順〔手動〕 386

更新プログラムファイルの登録手順 389

更新プログラムを手動で登録して配布する方法 113

個人所有 PC のネットワーク接続を禁止する流れ 91

コマンド 543

コマンド一覧 547

コマンドの実行手順 544

コマンドの説明形式 546

コントローラとの接続の切断 335

コントローラのアンインストール手順 288

コントローラのインストール手順 286

コントローラの環境設定の変更手順 289

コントローラの終了手順 297

コントローラの直接起動手順 291

コントローラのバーの表示切り替え手順 303

コントローラへの接続要求 336

コントローラへの特殊キーの登録手順 300

コンピュータごとの接続環境の設定手順 317

コンピュータに自動で更新プログラムを配布する方法 110

コンピュータの画面の拡大と縮小手順 301

コンピュータを検索したりリモートコントロールの開始手順 294

コンピュータを選択したりリモートコントロールの開始手順 291

コンピュータを選択して操作ログを取り込む手順 406

コンピュータをリモートコントロールして問い合わせに対処する流れ 82

さ

サービス開始〔startservice コマンド〕 613

サービス停止〔stopservice コマンド〕 611

再起動によって設定が適用されるケース 723

最近インストールされたソフトウェアを確認する流れ 119

最新の探索状況の確認手順 45, 502

再生画面の拡大 329

再生画面の縮小 329

再生画面の表示手順 329

再生画面表示 329
再生時にできる操作手順 328
再生の一時停止 328
再生の再開 328
再生のスキップ 328
再生の停止 328
再登録〔初期化されたスマートデバイス〕 78
再配布の準備〔スマートデバイス〕 72
削除手順〔エージェント設定〕 494
削除手順〔カスタムグループの情報〕 238
削除手順〔カスタムグループ〕 236
削除手順〔管轄範囲〕 223
削除手順〔管理ソフトウェア情報〕 437
削除手順〔機器情報〕 255
削除手順〔契約会社情報〕 514
削除手順〔契約情報〕 450
削除手順〔セキュリティポリシー〕 375
削除手順〔ソフトウェア検索条件〕 518
削除手順〔ソフトウェア情報〕 268
削除手順〔ソフトウェアライセンス情報〕 440
削除手順〔タスク〕 476
削除手順〔特例接続の設定〕 363
削除手順〔ネットワーク制御リスト〕 360
削除手順〔ネットワークモニタ設定〕 356
削除手順〔ハードウェア資産情報〕 416
削除手順〔パッケージ〕 472
削除手順〔フィルタ〕 239
削除手順〔ユーザーアカウント〕 218
削除〔ファイル〕 315
削除〔フォルダ〕 315
サポートサービスから取得できる情報 723
サポートサービスからの情報のオフライン更新 722
サポートサービスからの情報の自動取得 721
サポートサービスからの情報の取得 721
サポートサービスからの情報の登録 597
サポートサービスの接続設定手順 528
参考情報 710

し

時間の取り扱い 724
資産管理項目の設定手順 507
資産管理項目の追加手順 507
資産管理項目のデータ型の変更手順 507
資産管理項目の入力方法の変更手順 507
資産管理の設定 507
資産状態の追加手順 418
資産状態の変更手順 419
資産情報のインポート 455
資産情報を新体制に合わせて更新する 204
資産に掛かるコストの確認 181
資産に関する契約を管理する流れ 178
資産の管理 413
資産のコスト削減を検討する流れ 181
自動的にネットワーク接続が遮断された機器の再接続
手順 354
自動で更新プログラムを配布する流れ 109
修理後の機器を利用者に返却する流れ 159
障害対応〔機器〕 157
障害内容の確認 158
障害履歴の記録 160
使用禁止ソフトウェアの設定手順〔機器画面〕 269
詳細な機器情報のエクスポート〔ioutils
exportdevicedetail コマンド〕 571
情報が持ち出された形跡を調査する流れ 133
情報収集用ツールで収集した機器情報の通知手順 260
情報収集用ツールで収集した機器情報の通知に失敗し
た場合のトラブルシューティング 639
情報収集用ツールの生成手順 259
情報の更新 227
情報漏えいの確認 131
使用を許可する USB デバイスの登録 122
除外対象の機器の確認手順 47, 504
除外対象の設定手順 252
初期化されたスマートデバイスを再登録する流れ 78
初期化手順〔スマートデバイス〕 276
初期化〔紛失したスマートデバイス〕 74
職制変更に伴い部署の定義を変更する流れ 201

新規に接続された機器の確認 135
新体制の部署の規定を検討する 201

す

スケジュールの変更手順〔セキュリティ判定〕 505
ステータスウィンドウの非表示 333
ステータスウィンドウの表示 333
ステータスバーの表示の切り替え 303
すべてのコントローラとの接続の一括切断 335
スマートデバイスの管理 61
スマートデバイスの管理を始める流れ 63
スマートデバイスの情報の取得手順 273
スマートデバイスの初期化手順 276
スマートデバイスのパスコードのリセット手順 275
スマートデバイスのパスコードをリセットする流れ 77
スマートデバイスの紛失の対応 74
スマートデバイスのリプレースの計画を立てる流れ 67, 146
スマートデバイスの利用者を変更する流れ 70
スマートデバイスのロック手順 274
スマートデバイスを管理対象にする流れ 64
スマートデバイスを再配布する準備をする流れ 72
スマートデバイスを滅却する流れ 78
スマートデバイスをリプレースする流れ 67
スマートデバイスを利用者に配布する流れ 65, 73

せ

生成手順〔情報収集用ツール〕 259
製品ライセンスの情報を確認する方法 208
製品ライセンスの追加手順 209
製品ライセンスの登録 206
製品ライセンスの登録手順 207
製品を使った運用方法 22
セキュリティ監査に対応する流れ 127
セキュリティ管理に関するイベントの一覧を出力する流れ 128
セキュリティ管理の設定 505
セキュリティ状況の確認 366
セキュリティ状況の管理 102, 365

セキュリティ状況の判定除外ユーザー設定ファイルの形式 715
セキュリティ設定の確認 135
セキュリティの判定結果に応じた機器のネットワーク接続の制御手順 378
セキュリティ方針の策定 104
セキュリティポリシー違反の強制対策手順 379
セキュリティポリシー違反の自動対策 108
セキュリティポリシー違反の手動対策 108
セキュリティポリシー違反の対策 106
セキュリティポリシー違反の対策〔オフライン管理のコンピュータ〕 109
セキュリティポリシーに違反した機器の対策 99
セキュリティポリシーに違反した機器のネットワーク接続を自動制御する流れ 97
セキュリティポリシーの解除手順 376
セキュリティポリシーの管理 105
セキュリティポリシーのコピー手順 374
セキュリティポリシーの削除手順 375
セキュリティポリシーの設定 104
セキュリティポリシーの設定のインポート〔ioutils importpolicy コマンド〕 577
セキュリティポリシーの設定のエクスポート〔ioutils exportpolicy コマンド〕 574
セキュリティポリシーの追加手順 373
セキュリティポリシーの判定結果を出力する流れ 128
セキュリティポリシーの編集手順 373
セキュリティポリシーの利用 373
セキュリティポリシーの割り当て手順 375
接続中のユーザーの確認 345
接続モードの変更手順 297
接続要求のキャンセル手順 337
接続要求の許可 334
接続要求の拒否 334
接続リストからコンピュータへの接続 319
接続リストからのリモートコントロールできるコンピュータの検索手順 306
接続リストの項目の移動 323
接続リストの項目の検索手順 325
接続リストの項目のコピー 323

接続リストの項目の削除手順 323
接続リストの項目の属性確認手順 325
接続リストの項目の属性変更手順 324
接続リストの項目名の変更手順 324
接続リストの作成手順 319
接続リストの終了手順 318
接続リストの表示手順 318
接続リストの利用 317
接続履歴を利用したリモートコントロールの開始手順 293
設定のカスタマイズ 491
選択ファイルの情報の確認 311

そ

操作画面からのリモートコントロールの開始手順 295
操作画面の利用 225
操作画面へのログイン 210
操作画面利用時の注意事項 241
操作ログのエクスポート [ioutils exportoplog コマンド] 586
操作ログの確認 134
操作ログの確認手順 399
操作ログの管理 397
操作ログの収集の設定手順 [管理用サーバ] 398
操作ログの追跡手順 404
操作ログのディスクの空き容量のしきい値を変更する手順 411
操作ログの取り込み手順 405
操作ログのトレース手順 404
操作ログのバックアップファイルを管理する 409
操作ログの保管先フォルダからバックアップファイルを削除する手順 409
操作ログの保管先フォルダの変更手順 410
操作ログを自動的に取り込む手順 505
操作ログを定期的にエクスポートする手順 506
操作ログをバックアップする手順 409
送受信データの暗号化手順 [リモートコントロール] 301
送付先の設定手順 [ダイジェストレポート] 522
属性の変更 [ファイル] 315

属性の変更 [フォルダ] 315
組織内の機器の把握 24
ソフトウェア検索条件のインポート手順 519
ソフトウェア検索条件のエクスポート手順 519
ソフトウェア検索条件の削除手順 518
ソフトウェア検索条件の追加手順 517
ソフトウェア検索条件の編集手順 517
ソフトウェア情報のエクスポート手順 267
ソフトウェア情報の削除手順 268
ソフトウェアのアンインストール計画を立てる流れ 197
ソフトウェアのアンインストール手順 [機器画面] 270
ソフトウェアのアンインストール [配布 (ITDM 互換) 画面] 195
ソフトウェアのインストール状況の確認 187
ソフトウェアのインストール [配布 (ITDM 互換) 画面] 186
ソフトウェアの検収 167
ソフトウェアの情報を登録する流れ 166
ソフトウェアの媒体の利用者への貸し出し 167
ソフトウェアの配布 185, 464
ソフトウェアの配布計画 188
ソフトウェアの利用を制限する流れ 120
ソフトウェアライセンスが必要かどうかを判断する流れ 176
ソフトウェアライセンス情報のインポート手順 456
ソフトウェアライセンス情報の関連づけ手順 [契約情報] 453
ソフトウェアライセンス情報の削除手順 440
ソフトウェアライセンス情報の追加手順 438
ソフトウェアライセンス情報の編集手順 439
ソフトウェアライセンス情報の利用 436
ソフトウェアライセンスの移管手順 447
ソフトウェアライセンスの管理 162
ソフトウェアライセンスの利用違反に対処する流れ 172
ソフトウェアライセンスの割り当て 170
ソフトウェアライセンスの割り当て手順 446
ソフトウェアライセンスを棚卸する流れ 173

ソフトウェアライセンスを減却して反映する流れ 177
ソフトウェアライセンスを減却する流れ 175
[ソフトウェアをアンインストールしましょう] ウィザード 198, 469
ソフトウェアをアンインストールする流れ 195
[ソフトウェアをインストールしましょう] ウィザード 189, 465
ソフトウェアをインストールする流れ 186
ソフトウェアを購入する流れ 164, 165

た

対策が完了した機器のネットワーク接続を許可する流れ 96
ダイジェストレポートの送付先の設定手順 522
対処 [CSV ファイルが正しく表示されない場合] 640
対処 [機器が発見されない場合] 636
対処 [ディスクの空き容量が少ない場合] 642
対処 [認証エラーが発生した場合] 637
代替機の利用者への貸し出し 159
ダウンロードの延期 [配布機能] 481
他システムとの接続情報の設定 526
タスク情報のエクスポート手順 480
タスクの管理 474
タスクのコピー手順 476
タスクの再実行手順 478
タスクの削除手順 476
タスクの実行結果を確認する流れ 190, 194, 199
タスクの中止手順 477
タスクの追加手順 474
タスクの編集手順 475
棚卸日の一括更新手順 422, 445
棚卸日の自動更新手順 423
棚卸日の手動更新手順 420, 444
棚卸 [機器] 149
棚卸 [ソフトウェアライセンス] 173
棚卸 [バーコードリーダー使用] 425
探索状況の確認 44, 501
探索条件の設定手順 [Active Directory の探索] 499
探索条件の設定手順 [ネットワークの探索] 498

探索手順 [Active Directory に登録されている機器] 25, 248
探索手順 [ネットワークに接続されている機器] 25, 249
探索と同時にエージェントを配信する手順 (Active Directory の探索) [自動配信] 42
探索と同時にエージェントを配信する手順 (機器のネットワーク接続の監視) [自動配信] 43
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] 43

ち

[チャット] ウィンドウからのリモートコントロールの開始手順 344
[チャット] ウィンドウの動作環境の設定手順 338
[チャットサーバ] アイコンからの操作手順 345
チャットサーバの起動手順 339
チャットサーバの動作環境の設定手順 338
チャットでのメッセージの送信手順 342
チャットの開始手順 341
チャットの終了手順 342
チャットの内容の印刷手順 344
チャットの内容の保存手順 343
チャットの利用 338
チャットユーザーとの切断 345
注意事項 [操作画面利用時] 241

つ

追加管理項目の設定手順 507
追加管理項目の設定手順 [Active Directory から取得する情報] 265
追加管理項目の設定のインポート [ioutils importfield コマンド] 559
追加管理項目の設定のエクスポート [ioutils exportfield コマンド] 556
追加手順 [エージェント設定] 493
追加手順 [カスタムグループの情報] 237
追加手順 [カスタムグループ] 235
追加手順 [管轄範囲] 222
追加手順 [管理ソフトウェア情報] 436
追加手順 [契約会社情報] 513

追加手順 [契約情報] 449
追加手順 [資産管理項目] 507
追加手順 [製品ライセンス] 209
追加手順 [セキュリティポリシー] 373
追加手順 [ソフトウェア検索条件] 517
追加手順 [ソフトウェアライセンス情報] 438
追加手順 [タスク] 474
追加手順 [特例接続の設定] 362
追加手順 [ネットワーク制御リスト] 359
追加手順 [ネットワークモニタ設定] 356
追加手順 [ハードウェア資産情報] 414
追加手順 [パッケージ] 471
追加手順 [ファイル転送先のコンピュータ] 310
追加手順 [フィルタ] 239
追加手順 [ユーザーアカウント] 216
追跡手順 [操作ログ] 404
ツールバーの表示の切り替え 303

て

ディスクの空き容量が少ない場合の対処 642
データ型の変更手順 [資産管理項目] 507
データベース障害のトラブルシューティング 673
データベースの管理 532
データベースの再編成 540
データベースの再編成 [reorgdb コマンド] 608
データベースのバックアップ 535
データベースのリストア 537
データベースマネージャの起動手順 533
データ持ち出しの許可 125
デバイスの使用を抑止する手順 381
デフォルトパスワードの変更手順 213
電源 OFF のコンピュータのリモートコントロール
手順 298
電源の制御手順 272
転送データの暗号化 311
テンプレートのインポート [ioutils importtemplate
コマンド] 565
テンプレートのエクスポート [ioutils
exporttemplate コマンド] 562

と

動作環境の設定手順 [リモコンエージェント] 290
特例接続の管理 362
特例接続の設定の削除手順 363
特例接続の設定の追加手順 362
特例接続の設定の編集手順 362
ドラッグ&ドロップでの転送 312
トラブルシューティング 633
トラブルシューティング [Active Directory 連携時]
670
トラブルシューティング [MDM 連携時] 671
トラブルシューティング [エージェント] 665
トラブルシューティング [管理用サーバ] 645
トラブルシューティング [情報収集用ツールで収集し
た機器情報の通知の失敗時] 639
トラブルシューティング [データベース障害] 673
トラブルシューティング [ネットワーク制御時] 669
トラブルシューティング [リモートコントロール時]
668
トラブルシュート用情報の採取 [エージェント] 665
トラブルシュート用情報の取得 [getlogs コマンド]
615

に

入力方法の変更手順 [資産管理項目] 507
認証エラーが発生した場合の対処 [機器の探索] 637
認証情報の設定手順 [AMT] 520
認証情報 [SNMP] 500
認証情報 [Windows の管理共有] 500
認証情報 [ネットワークの探索] 500

ね

ネットワーク監視機能による機器の検知 27
ネットワーク制御時のトラブルシューティング 669
ネットワーク制御の設定 97
ネットワーク制御リストからの機器の削除手順 360
ネットワーク制御リストの管理 359
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 360
ネットワーク制御リストの編集手順 359

ネットワーク制御リストへの機器の追加手順 359
ネットワーク制御リストへの登録 92
ネットワーク接続が自動遮断された機器の再接続手順 354
ネットワーク接続が遮断された機器の確認 99
ネットワーク接続許可の期間の延長 101
ネットワーク接続した機器の確認 94
ネットワーク接続の管理 346
ネットワーク接続の許可手順 351
ネットワーク接続の遮断手順 352
ネットワークに接続されている機器の探索手順 25, 249
ネットワークの探索時に使用する認証情報 500
ネットワークの探索条件の設定手順 498
ネットワークモニタ設定の管理 356
ネットワークモニタ設定の削除手順 356
ネットワークモニタ設定の追加手順 356
ネットワークモニタ設定の編集手順 356
ネットワークモニタ設定の割り当て手順 357
ネットワークモニタ設定の割り当ての変更手順 358
ネットワークモニタの無効化手順 349
ネットワークモニタの有効化手順 347
ネットワークモニタを有効化するコンピュータのエージェント設定の編集手順 494

は

バーコードリーダーを使用した棚卸 425
ハードウェア資産情報に対応する機器情報の変更手順 427
ハードウェア資産情報のインポート手順 455
ハードウェア資産情報のインポート [ioutils importasset コマンド] 552
ハードウェア資産情報のエクスポート [ioutils exportasset コマンド] 549
ハードウェア資産情報の関連づけ手順 [契約情報] 453
ハードウェア資産情報の関連づけ手順 [ハードウェア資産] 427
ハードウェア資産情報の削除手順 416
ハードウェア資産情報の追加手順 414
ハードウェア資産情報の編集手順 415

ハードウェア資産情報の利用 414
ハードウェア資産情報をメンテナンスする方法 140
ハードウェア資産の管理 137
配布機能 185
配布する更新プログラムを準備する流れ 114
配布 [ソフトウェア] 185, 464
配布 [ファイル] 185, 191, 464
パスコードのリセット手順 [スマートデバイス] 275
パスコードのリセット [スマートデバイス] 77
パスコードを忘れた場合の対処 [スマートデバイス] 76
パスワードの初期化手順 221
パスワードの変更手順 [自分] 219
パスワードの変更手順 [ほかの管理者] 220
バックアップデータのリストア [importdb コマンド] 604
バックアップの取得 [exportdb コマンド] 600
パッケージ情報のエクスポート手順 472
パッケージの管理 471
パッケージの削除手順 472
パッケージの追加手順 471
パッケージの編集手順 471
発見した機器の確認手順 45, 502
パネルの設定手順 226
判定対象から除外するユーザーの設定手順 [セキュリティ] 372

ひ

表示項目の変更手順 228

ふ

ファイル情報の確認手順 [ファイル転送] 310
[ファイル転送] ウィンドウの起動手順 309
[ファイル転送] ウィンドウの終了手順 310
ファイル転送先のコンピュータの追加手順 310
ファイル転送時のセキュリティ設定手順 311
ファイル転送のオプションの設定手順 315
ファイル転送の接続の切断手順 309
ファイル転送の利用 309
ファイル登録での転送 312

ファイルの削除 315
ファイルの手動での削除 314
ファイルの手動での転送 314
ファイルの属性の変更 315
ファイルの転送手順 312
ファイルの配布 185, 464
ファイルの配布計画 192
ファイルの編集手順〔ファイル転送〕 314
ファイルの名称の変更 315
ファイルへのアクセス権の設定 312
〔ファイルを配布しましょう〕ウィザード 193, 467
ファイルを配布する流れ 191
フィルタの管理 239
フィルタの削除手順 239
フィルタの設定のインポート〔ioutils importfilter コマンド〕 594
フィルタの設定のエクスポート〔ioutils exportfilter コマンド〕 590
フィルタの追加手順 239
フィルタの保存手順 239
フェールオーバー発生後の対処方法 643
フォルダの削除 315
フォルダの作成 314
フォルダの属性の変更 315
フォルダの名称の変更 315
複数の管理者で業務を分担する流れ 57
複数の管理者と連携して業務を進める流れ 60
複数のコントローラの画面の整列表示手順 303
複数のユーザーアカウントを登録する流れ 59
部署の定義を新体制に合わせて変更する流れ 202
不審操作のイベントの確認手順 403
不審操作の検知手順 402
不審操作の自動通知の設定手順 132
不審操作を調査する流れ 133
不審と見なす操作を検知するための設定手順 401
ブラックリスト方式 89
フルスクリーン表示での機器のリモートコントロール手順 301
紛失したスマートデバイスを初期化する流れ 74

紛失したスマートデバイスをロックする流れ 76
紛失への対応〔スマートデバイス〕 74

へ

編集手順〔エージェント設定〕 493
編集手順〔管理ソフトウェア情報〕 437
編集手順〔機器情報〕 256
編集手順〔契約会社情報〕 514
編集手順〔契約情報〕 449
編集手順〔セキュリティポリシー〕 373
編集手順〔ソフトウェア検索条件〕 517
編集手順〔ソフトウェアライセンス情報〕 439
編集手順〔タスク〕 475
編集手順〔特例接続の設定〕 362
編集手順〔ネットワーク制御リスト〕 359
編集手順〔ネットワークモニタ設定〕 356
編集手順〔ネットワークモニタを有効化するコンピュータのエージェント設定〕 494
編集手順〔ハードウェア資産情報〕 415
編集手順〔パッケージ〕 471
編集手順〔ユーザーアカウント〕 217
編集〔コンピュータのファイル〕 313

ほ

ポート番号一覧 710
保管先ディスク変更手順 411
保守サービスを利用する流れ 158
ホスト識別子のリセット〔resrtnid.vbs コマンド〕 621
ホスト名を直接指定したりリモートコントロールの開始手順 292
保存期間の設定手順〔レポート〕 522
ホワイトリスト方式 89

ま

マルチ転送 312

み

未登録の機器のネットワーク接続を禁止する流れ 93

め

- 名称の変更〔ファイル〕 315
- 名称の変更〔フォルダ〕 315
- メールサーバの設定手順 526
- メール通知〔Active Directory の探索〕 499
- メール通知〔イベント〕 524
- メール通知〔セキュリティ違反〕 106
- メール通知〔ネットワークの探索〕 498
- メール通知〔不審操作〕 132
- メール通知〔レポート〕 522
- メールでのセキュリティポリシー違反の把握 106
- 滅却対象の機器を決定する流れ 79, 155
- 滅却〔機器〕 155
- 滅却〔スマートデバイス〕 78
- 滅却〔ソフトウェアライセンス〕 175
- メッセージの出力形式 634
- メッセージの通知手順〔機器画面〕 271
- メッセージの通知〔自動〕 380

ゆ

- ユーザーアカウントの管理 215
- ユーザーアカウントの削除手順 218
- ユーザーアカウントの情報の設定手順 212
- ユーザーアカウントの設定内容を検討する流れ 57
- ユーザーアカウントの追加手順 216
- ユーザーアカウントの編集手順 217
- ユーザーアカウントのロックの解除手順 224
- ユーザー定義のグループ条件の変更手順 234
- ユーザー定義のグループの管理 232
- ユーザー定義のグループの削除手順 233
- ユーザー定義のグループの追加手順 232
- ユーザー定義のグループ名の変更手順 232

よ

- 余剰ライセンスの確認 183
- 余剰ライセンスを有効利用する流れ 168
- 余剰ライセンスを割り当てる流れ 169
- 予定資産状態の変更手順 419
- 予定ライセンス状態の変更手順 443

予約ファイルの情報の確認 311

ら

- ライセンス状態の追加手順 441
- ライセンス状態の変更手順 442
- ライセンス登録手順 207

り

- リクエストサーバの開始手順 326
- リクエストサーバの作成手順 326
- リクエストサーバの停止手順 326
- リプレイス〔機器〕 145
- リプレイス〔スマートデバイス〕 67
- リモート CD-ROM の利用手順 305
- [リモートコントロール] ウィンドウからのコンピュータの検索手順 306
- リモートコントロール時のトラブルシューティング 668
- リモートコントロール接続できるコンピュータの検索方法のカスタマイズ手順 308
- リモートコントロール対象のコンピュータからの接続の切断手順 335
- リモートコントロール中の [Ctrl] + [Alt] + [Delete] キーの入力手順 299
- リモートコントロール中の画面の画像としての保存手順 304
- リモートコントロール中のコンピュータとの接続の切断手順 296
- リモートコントロール中のコンピュータとの接続を自動切断する設定手順 296
- リモートコントロール中のコンピュータの再起動手順 299
- リモートコントロール中のコンピュータの電源 OFF 手順 298
- リモートコントロール中のコンピュータのファイルの操作手順〔ファイル転送〕 313
- リモートコントロール中の送受信データの暗号化手順 301
- リモートコントロール中の特殊キーの入力手順 300
- リモートコントロール中のマウスホイールでのスクロールの制御手順 304

リモートコントロールによるコンピュータの問題
点対処 84

リモートコントロールによるコンピュータの問題
点調査 84

リモートコントロールの開始手順〔IP アドレスの
指定〕 292

リモートコントロールの開始手順〔コンピュータの検
索〕 294

リモートコントロールの開始手順〔コンピュータの選
択〕 291

リモートコントロールの開始手順〔接続履歴の利用〕
293

リモートコントロールの開始手順〔ホスト名の指定〕
292

リモートコントロールの対象のコンピュータに接続す
る流れ 83

リモートコントロールの対象のコンピュータを特定す
る流れ 82

リモートコントロールの利用 291

リモートコントロールの録画手順 330

リモコンエージェントの終了手順 333

リモコンエージェントのステータスウィンドウの表示
手順 333

リモコンエージェントの動作環境の設定手順 290

リモコンエージェントの利用 333

利用されていない機器を確認する流れ 152

利用されていない資産の確認 182

利用しなくなった機器を回収する流れ 148, 154

利用しなくなったスマートデバイスを回収する流れ
69, 71

利用者がスマートデバイスのパスコードを忘れた場合
の対処 76

利用者情報の取得手順 262

〔利用者情報の入力〕画面の表示間隔の設定手順〔機
器画面〕 264

〔利用者情報の入力〕画面の表示間隔の設定手順〔資
産画面〕 417

利用者の変更〔スマートデバイス〕 70

利用者への作業の指示 87

利用者へのメッセージ通知手順〔セキュリティ〕 380

利用状況の確認〔ソフトウェアライセンス〕 168, 169

利用状況の確認〔割り当てたソフトウェアライセ
ンス〕 171

れ

レイアウトの初期化〔パネル〕 226

レイアウトの設定手順〔パネル〕 226

レポートの印刷手順 489

レポートの開始日の設定手順 522

レポートの参照 486

レポートの設定 522

レポートの表示手順 487

レポートの表示手順〔最新のデータ〕 488

レポートの保存期間の設定手順 522

レポートの保存手順 490

ろ

ログアウト手順 214

ログイン 210

ログイン手順 211

ログオンスクリプトを利用した機器情報の取得の流れ
〔オフライン管理のコンピュータ〕 54

録画機能の利用 328

録画データの再生手順 331

録画手順〔リモートコントロール〕 330

録画の一時停止手順 330

録画の再開手順 330

録画ファイルの AVI 形式への変換手順 332

録画ファイルの情報の確認 331

ロック手順〔スマートデバイス〕 274

ロックの解除〔ユーザーアカウント〕 224

ロック〔紛失したスマートデバイス〕 76

わ

割り当て手順〔エージェント設定〕 495

割り当て手順〔ネットワークモニタ設定〕 357