HITACHI
Inspire the Next

JP1 Version 11

# JP1/IT Desktop Management 2 - Smart Device Manager

3021-3-B61-10

# 前書き

## ■ 対象製品

適用 OS のバージョン、JP1/IT Desktop Management 2 - Smart Device Manager が前提とするサービスパックやパッチなどの詳細については、リリースノートで確認してください。

P-2A42-7EBL JP1/IT Desktop Management 2 - Smart Device Manager 11-10

JP1/IT Desktop Management 2 - Smart Device Manager は、次に示すコンポーネントで構成されています。

JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイスマネージャー）（適用 OS：Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、Windows Server 2008 R2）

JP1/IT Desktop Management 2 - Smart Device Manager（通信サーバ）（適用 OS：Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、Windows Server 2008 R2）

JP1/IT Desktop Management 2 - Smart Device Manager（メッセージングサーバ）（適用 OS：Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、Windows Server 2008 R2）

JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイス Android エージェント）（適用 OS：Android 4.1 以降）

JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイス iOS エージェント）（適用 OS：iOS 7.1 以降）

## ■ 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

HITACH、HiRDB、JP1、Job Management Partner 1、uCosminexus は、（株）日立製作所の商標または登録商標です。

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。

iOS は、Apple Inc.の OS 名称です。 IOS は、Cisco Systems, Inc.またはその関連会社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あり、ライセンスに基づき使用されています。

Microsoft 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 Exchange 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。

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。

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

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

Windows 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。

その他記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。

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。

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 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/).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

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

This product includes software developed by Andy Clark.

HITACHI
Inspire the Next
株式会社 日立製作所

Java™ COMPATIBLE ENTERPRISE EDITION

Java™ COMPATIBLE

## ■ マイクロソフト製品のスクリーンショットの使用について

マイクロソフトの許可を得て使用しています。

## ■ マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

| 表記 | | | 製品名 |
|---|---|---|---|
| Exchange | | | Microsoft(R) Exchange Server |
| IE | Internet Explorer | | Windows(R) Internet Explorer(R) |
| Windows | Windows Server 2008 | Windows Server 2008 R2 | Microsoft(R) Windows Server(R) 2008 R2 Datacenter |
| | | | Microsoft(R) Windows Server(R) 2008 R2 Enterprise |
| | | | Microsoft(R) Windows Server(R) 2008 R2 Standard |
| | Windows Server 2012 | Windows Server 2012 | Microsoft(R) Windows Server(R) 2012 Datacenter |
| | | | Microsoft(R) Windows Server(R) 2012 Standard |
| | | Windows Server 2012 R2 | Microsoft(R) Windows Server(R) 2012 R2 Datacenter |
| | | | Microsoft(R) Windows Server(R) 2012 R2 Standard |
| | Windows Server 2016 | Windows Server 2016 | Microsoft(R) Windows Server(R) 2016 Datacenter |
| | | | Microsoft(R) Windows Server(R) 2016 Standard |

■ 発行

2017 年 3 月 3021-3-B61-10

■ 著作権

Copyright (C) 2016, 2017, Hitachi, Ltd.
Copyright (C) 2016, 2017, Hitachi Solutions, Ltd.

# 変更内容

## 変更内容（3021-3-B61-10） JP1/IT Desktop Management 2 - Smart Device Manager 11-10

| 追加・変更内容 | 変更個所 |
|---|---|
| 利用者の操作でアプリケーションをインストールできる Pull 配布機能を追加した。 | 2.6.2、4.2、4.11、9.11、9.12、9.13、9.14、15. sdmioutils exportdeliverypermit、15. sdmioutils importdeliverypermit、15. sdmioutils deletedeliverypermit、付録 E.6 |
| 大容量なアプリケーションを配布できる標準配布機能を追加した。 | 2.6.2、4.9、4.10、4.12、9.1、9.2、9.3、9.5、9.6、9.7、9.9、12.1、12.2、付録 A.2 |
| 次のコマンドを追加した。<br>• sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）<br>• sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）<br>• sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）<br>• sdmdistributeapp（アプリケーションのインストール指示）<br>• sdmapplyprofile（iOS プロファイルの適用または適用解除）<br>• sdmgetinvenroty（インベントリ情報の取得）<br>• sdmexportdistributestatus（アプリケーション配布状況の出力）<br>• sdmexportinstallapp（全端末のインストールソフトウェア情報の出力） | 8.6、9.6、9.7、9.9、9.11、9.12、9.13、12.3、15. コマンド一覧、15. sdmioutils exportdeliverypermit、15. sdmioutils importdeliverypermit、15. sdmioutils deletedeliverypermit、15. sdmdistributeapp、15. sdmapplyprofile、15. sdmgetinvenroty、15. sdmexportdistributestatus、15. sdmexportinstallapp、付録 E.6、付録 E.7、付録 E.8、付録 E.9、付録 E.10、付録 E.11 |
| Windows Server 2016 をサポート対象とした。 | － |

単なる誤字・脱字などはお断りなく訂正しました。

# はじめに

このマニュアルは、JP1/IT Desktop Management 2 - Smart Device Manager（以降、JP1/ITDM2 - SDM と略す）の製品概要、機能、システムの設計方法、構築方法、運用例、操作方法などを説明したものです。

## ■ 対象読者

このマニュアルは、次の方にお読みいただくことを前提に説明しています。

- JP1/ITDM2 - SDM の導入検討またはシステムの設計をしている方
- JP1/ITDM2 - SDM の製品概要や機能詳細について知りたい方
- JP1/ITDM2 - SDM のシステムの構築をしている方
- JP1/ITDM2 - SDM の構築方法について知りたい方
- JP1/ITDM2 - SDM を利用して、組織内のスマートデバイスを管理する方
- JP1/ITDM2 - SDM 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、次に示す章から構成されています。

**第 1 章　製品の概要**

JP1/ITDM2 - SDM の概要とシステムを構成する要素について説明しています。

**第 2 章　機能の紹介**

JP1/ITDM2 - SDM の機能の詳細について説明しています。

**第 3 章　システムの構築**

システムの構築方法について説明しています。

**第 4 章　製品を使った運用方法**

JP1/ITDM2 - SDM を使用した運用方法について説明しています。

**第 5 章　操作を開始・終了する**

JP1/ITDM2 - SDM の操作を開始・終了する方法について説明しています。

**第 6 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 7 章　セキュリティ状況を管理する

組織内のスマートデバイス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 8 章　スマートデバイスを管理する

組織内のスマートデバイス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 9 章　アプリケーションを管理する

組織内のスマートデバイスに配布するアプリケーションを管理する方法について説明しています。

第 10 章　イベントを参照する

JP1/ITDM2 - SDM 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 11 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 12 章　データベースを管理する

JP1/ITDM2 - SDM のコマンドを使用し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 13 章　トラブルシューティング

JP1/ITDM2 - SDM で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 14 章　画面リファレンス

JP1/ITDM2 - SDM の画面や項目名を説明しています。

第 15 章　コマンド

JP1/ITDM2 - SDM のコマンドについて説明しています。

第 16 章　定義ファイル

JP1/ITDM2 - SDM の定義ファイルについて説明しています。

第 17 章　メッセージ

JP1/ITDM2 - SDM のメッセージを一覧で説明しています。

# 目次

前書き　2
変更内容　6
はじめに　7

1　製品の概要　19
1.1　製品概要　20
1.1.1　この製品でできること　20
1.1.2　スマートデバイスの管理の流れ　21
1.2　システムの構成要素の紹介　23
1.3　操作画面の紹介　25
1.3.1　基本的な画面構成　25
1.3.2　ホーム画面でできること　27
1.3.3　セキュリティ画面でできること　27
1.3.4　スマートデバイス画面でできること　29
1.3.5　配布画面でできること　31
1.3.6　イベント画面でできること　32
1.3.7　設定画面でできること　33

2　機能の紹介　36
2.1　機能一覧　37
2.2　システムの概況表示　38
2.3　ユーザーアカウントの管理　40
2.3.1　ユーザーアカウントのロック　40
2.3.2　ユーザーアカウントの権限　40
2.3.3　参照権限で実行できない操作一覧　41
2.4　セキュリティの管理　44
2.4.1　セキュリティのルールの種類　44
2.4.2　セキュリティポリシーの管理　45
2.4.3　セキュリティポリシーに設定できる項目　45
2.4.4　Android ポリシーの管理　46
2.4.5　Android ポリシーに設定できる項目　46
2.4.6　iOS プロファイルの管理　48
2.4.7　iOS プロファイルに設定できる項目について　49
2.5　スマートデバイスの管理　50
2.5.1　管理対象のスマートデバイスの管理　50

2.5.2 管理対象外のスマートデバイスの管理 51
2.6 アプリケーションの管理 53
2.6.1 配布アプリケーションの管理 53
2.6.2 配布するアプリケーションについて 53
2.6.3 Android アプリケーションの管理 54
2.6.4 iOS アプリケーションの管理 55
2.7 イベントの表示 57
2.7.1 出力されるイベント 57
2.7.2 イベントの種類 57
2.7.3 イベントの形式 58

**3 システムの構築 60**
3.1 システムを構築する流れ 61
3.2 前提 OS 63
3.3 前提プログラム 64
3.4 JP1/ITDM2 - SDM を構成するコンポーネント 65
3.5 JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする手順 66
3.6 JP1/ITDM2 - SDM（通信サーバ）をインストールする手順 68
3.7 JP1/ITDM2 - SDM（メッセージングサーバ）をインストールする手順 70
3.8 ルータのポート開放および各サーバのファイアウォールの設定について 72
3.9 SSL 通信用証明書の種類 73
3.10 SSL 通信用証明書の配置 74
3.11 SSL 通信用証明書の取得 75
3.11.1 通信サーバの SSL 通信用証明書を取得する流れ 75
3.11.2 スマートデバイスマネージャーの SSL 通信用証明書を取得する流れ 76
3.11.3 APNs サーバの SSL 通信用ルート証明書を取得する手順（iOS 端末を管理する場合） 77
3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合） 78
3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合） 78
3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合） 80
3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合） 81
3.12 スマートデバイスマネージャーでの SSL 通信用証明書の設定 83
3.12.1 スマートデバイスマネージャーで通信サーバの SSL 通信用ルート証明書を設定する手順 83
3.12.2 スマートデバイスマネージャーで SSL 通信用サーバ証明書を設定する手順 84
3.13 通信サーバでの SSL 通信用証明書の設定 86
3.13.1 通信サーバで APNs サーバの SSL 通信用ルート証明書を設定する手順（iOS 端末を管理する場合）86
3.13.2 通信サーバで SSL 通信用サーバ証明書を設定する手順 87
3.13.3 通信サーバで APNs サーバの SSL 通信用クライアント証明書を設定する手順（iOS 端末を管理する場合） 88
3.13.4 通信サーバで構成プロファイルを作成する手順（iOS 端末を管理する場合） 88

3.14 スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ 92
3.14.1 組織のセキュリティ方針の策定について 93
3.14.2 プロビジョニングの設定について 94
3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順 94
3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順 95
3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順 96
3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合） 96
3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合） 97
3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順 98
3.15 サーバから JP1/ITDM2 - SDM をアンインストールする手順 99
3.16 Android 端末から JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールする手順（Android 端末の設定メニューを使用する場合） 100
3.17 Android 端末から JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールする手順（Google Play ストアアプリを使用する場合） 101
3.18 iOS 端末から JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をアンインストールする手順 102
3.19 バージョンアップインストール時の作業 103
3.19.1 通信サーバをバージョンアップインストールするときの作業 103

**4 製品を使った運用方法 105**
4.1 スマートデバイスに対する遠隔操作について 106
4.1.1 Android 端末の管理について 106
4.1.2 iOS 端末の管理について 106
4.2 運用中にできること 108
4.3 スマートデバイスの準備について 110
4.3.1 新規に購入したスマートデバイスを準備する流れ 110
4.3.2 すでに JP1/ITDM2 - SDM に登録されているスマートデバイスを準備する流れ 111
4.4 スマートデバイスを新規に配布する流れ 112
4.5 スマートデバイスをリプレースする流れ 113
4.6 スマートデバイスの利用者を変更する流れ 114
4.7 スマートデバイスを保管する流れ 116
4.8 スマートデバイスを滅却する流れ 117
4.9 Android 端末にアプリケーションを配布・インストールする流れ 118
4.10 iOS 端末にアプリケーションをインストールする流れ 120
4.11 スマートデバイスから利用者の操作でアプリケーションをインストールする流れ 122
4.12 不要となったアプリケーションを削除する流れ 124
4.13 セキュリティのルールの管理について 125
4.13.1 Android ポリシーを適用する流れ 125
4.13.2 iOS プロファイルを適用する流れ 126

4.14 スマートデバイス紛失時の対処について 128
4.14.1 紛失したスマートデバイスをロックする流れ 128
4.14.2 紛失したスマートデバイスを初期化する流れ 129
4.15 利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合の対処について 130
4.15.1 Android 端末のパスワードを変更する流れ 130
4.15.2 iOS 端末のパスコードをリセットする流れ 131
4.15.3 JP1/ITDM2 - SDM（スマートデバイスエージェント）によって初期化されたスマートデバイスを管理対象にする流れ 131
4.16 発生したイベントをメールで通知する流れ 133

**5 操作を開始・終了する 134**
5.1 ログインする手順 135
5.2 ユーザーアカウント情報を設定する手順 137
5.3 デフォルトパスワードを変更する手順 138
5.4 ログアウトする手順 139

**6 ユーザーアカウントを管理する 140**
6.1 ユーザーアカウントを追加する手順 141
6.2 自分のユーザーアカウントを編集する手順 142
6.3 ほかの管理者のユーザーアカウントを編集する手順 143
6.4 ユーザーアカウントを削除する手順 144
6.5 自分のパスワードを変更する手順 145
6.6 ほかの管理者のパスワードを初期化する手順 146
6.7 ユーザーアカウントのロックを解除する手順 147

**7 セキュリティ状況を管理する 148**
7.1 セキュリティポリシーを利用する 149
7.1.1 セキュリティポリシーを追加する手順 149
7.1.2 セキュリティポリシーを編集する手順 150
7.1.3 セキュリティポリシーを削除する手順 151
7.1.4 セキュリティポリシーを適用する手順 152
7.2 Android ポリシーを利用する 154
7.2.1 Android ポリシーを追加する手順 154
7.2.2 Android ポリシーを編集する手順 154
7.2.3 Android ポリシーを削除する手順 155
7.2.4 Android ポリシーを適用する手順 156
7.3 iOS プロファイルを利用する 158
7.3.1 iOS プロファイルを追加する手順 158
7.3.2 iOS プロファイルをエクスポートする手順 159
7.3.3 iOS プロファイルを削除する手順 159

7.3.4 iOS プロファイルを適用する手順 160
7.3.5 iOS プロファイルを適用解除する手順 161
7.3.6 iOS プロファイル情報を編集する手順 162

8 スマートデバイスを管理する 164
8.1 スマートデバイスの JP1/ITDM2 - SDM への登録 165
8.1.1 手動でスマートデバイスを登録する手順 165
8.1.2 CSV ファイルでスマートデバイスを登録する手順 167
8.2 スマートデバイス一覧をエクスポートする手順 169
8.3 管理対象外のスマートデバイスを管理対象にする 170
8.3.1 スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にする手順 170
8.3.2 Android 端末で再度管理対象とするための手順 171
8.3.3 iOS 端末で再度管理対象とするための手順 172
8.4 管理対象のスマートデバイスを管理対象外にする手順 173
8.5 スマートデバイスを JP1/ITDM2 - SDM から削除する手順 174
8.6 スマートデバイスから最新のインベントリ情報を取得する手順 175
8.7 スマートデバイスを初期化する手順 176
8.8 スマートデバイスをロックする手順 177
8.9 Android 端末のパスワードを変更する手順 178
8.10 iOS 端末のパスコードをリセットする手順 179
8.11 Android 端末にメッセージを通知する手順 180
8.12 スマートデバイスのログを取得する手順 181

9 アプリケーションを管理する 182
9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順 183
9.2 配布するアプリケーションを通信サーバに配置する手順 185
9.3 登録したアプリケーションの情報を編集する手順 186
9.4 アプリケーションを JP1/ITDM2 - SDM から削除する手順 188
9.5 不要となったアプリケーションを通信サーバから削除する手順 189
9.6 Android 端末にアプリケーションを配布する手順 190
9.7 Android 端末にアプリケーションのインストールを指示する手順 192
9.8 Android 端末に配布したアプリケーションをアンインストールする手順 194
9.9 iOS 端末にアプリケーションのインストールを指示する手順 195
9.10 iOS 端末に配布したアプリケーションをアンインストールする手順 196
9.11 利用者の操作でインストールできるアプリケーションを管理する 197
9.12 Android 端末から利用者の操作でアプリケーションをインストールする手順 199
9.13 iOS 端末から利用者の操作でアプリケーションをインストールする手順 200
9.14 配布アプリケーションの最大同時ダウンロード数を制限する手順 201

10 イベントを参照する 202
10.1 イベントの詳細を確認する手順 203
10.2 イベント情報をエクスポートする手順 204

11 設定をカスタマイズする 205
11.1 イベント通知の設定をする手順 206
11.2 メールサーバを設定する手順 207

12 データベースを管理する 208
12.1 データベースをバックアップする手順 209
12.2 データベースをリストアする手順 211
12.3 データベースの接続先ポート番号を変更する手順 213

13 トラブルシューティング 215
13.1 スマートデバイスマネージャーでのトラブルシューティングの手順 216
13.2 スマートデバイスでのトラブルシューティングの手順 217
13.3 ディスクの空き容量が少ないときの対処方法 218
13.4 サーバ間での通信エラー発生時のトラブルシューティング 219
13.4.1 スマートデバイスマネージャーと通信サーバ間で通信エラーが発生する場合の対処方法 219
13.4.2 通信サーバとメッセージングサーバ間で通信エラーが発生する場合の対処方法 219
13.5 画面操作時のトラブルシューティング 221
13.6 データベース障害のトラブルシューティング 222
13.6.1 データベース接続エラーが発生する場合の対処方法 222
13.6.2 データベースのアクセスエラーが発生する場合の対処方法 222
13.6.3 データベースのバックアップ、リストアが失敗する場合の対処方法 222
13.7 iOS アプリケーションのインストールでのトラブルシューティング 224
13.7.1 iOS アプリケーションのインストールに失敗する場合の対処方法 224
13.7.2 アプリーションのインストール結果が［iOS アプリケーション］画面に反映されない場合の対処方法 224

14 画面リファレンス 225
14.1 画面遷移図 226
14.1.1 ログイン画面からログイン直後までの画面遷移 226
14.1.2 セキュリティ画面の画面遷移 227
14.1.3 スマートデバイス画面の画面遷移 227
14.1.4 配布画面の画面遷移 228
14.1.5 イベント画面の画面遷移 229
14.1.6 設定画面の画面遷移 229
14.2 ログイン画面 231
14.2.1 ［パスワードの変更］ダイアログ 231

14.3 ホーム画面 233
14.3.1 [システムサマリ] パネル 233
14.3.2 [イベントの状況] パネル 234
14.3.3 [データベースとディスクの状況] パネル 235
14.3.4 [MDM 用証明書の状況] パネル 236
14.4 セキュリティ画面 238
14.4.1 [セキュリティポリシー一覧] 画面 238
14.4.2 [セキュリティポリシーの追加] ダイアログ 240
14.4.3 [セキュリティポリシーの編集] ダイアログ 241
14.4.4 [セキュリティポリシーの参照] ダイアログ 242
14.4.5 [電話番号の追加] ダイアログ 243
14.4.6 [電話番号の編集] ダイアログ 244
14.4.7 [Web サイトの追加] ダイアログ 245
14.4.8 [Web サイトの編集] ダイアログ 245
14.4.9 [アプリケーションの追加] ダイアログ 246
14.4.10 [アプリケーションの編集] ダイアログ 247
14.4.11 [Android ポリシー一覧] 画面 248
14.4.12 [Android ポリシーの追加] ダイアログ 249
14.4.13 [Android ポリシーの編集] ダイアログ 250
14.4.14 [Android ポリシーの参照] ダイアログ 251
14.4.15 [iOS プロファイル一覧] 画面 252
14.4.16 [iOS プロファイルの追加] ダイアログ 254
14.4.17 [iOS プロファイル情報の編集] ダイアログ 254
14.5 スマートデバイス画面 256
14.5.1 [管理対象のスマートデバイス一覧] 画面 256
14.5.2 [管理対象のスマートデバイス一覧] 画面で表示されるタブ 259
14.5.3 [管理対象外のスマートデバイス一覧] 画面 264
14.5.4 [管理対象外のスマートデバイス一覧] 画面で表示されるタブ 265
14.5.5 [スマートデバイスの初期化] ダイアログ 266
14.5.6 [スマートデバイスのロック] ダイアログ 267
14.5.7 [スマートデバイスのパスコードのリセット] ダイアログ 268
14.5.8 [管理対象外にする] ダイアログ 268
14.5.9 [セキュリティポリシーを適用する] ダイアログ 269
14.5.10 [Android ポリシーを適用する] ダイアログ 269
14.5.11 [iOS プロファイルの適用] ダイアログ 270
14.5.12 [iOS プロファイルの適用解除] ダイアログ 270
14.5.13 [スマートデバイスの追加] ダイアログ 271
14.5.14 [スマートデバイス一覧のインポート] ダイアログ 272
14.5.15 [スマートデバイスへのメッセージ通知] ダイアログ 273

14.6 配布画面 274
14.6.1 [配布アプリケーション一覧]画面 274
14.6.2 [Android アプリケーション]画面 276
14.6.3 [Android アプリケーション]画面で表示されるタブ 277
14.6.4 [iOS アプリケーション]画面 279
14.6.5 [iOS アプリケーション]画面で表示されるタブ 280
14.6.6 [Android アプリケーションの追加]ダイアログ 281
14.6.7 [Android アプリケーションの編集]ダイアログ 282
14.6.8 [Android アプリケーションの参照]ダイアログ 282
14.6.9 [iOS アプリケーションの追加]ダイアログ 283
14.6.10 [iOS アプリケーションの編集]ダイアログ 284
14.6.11 [iOS アプリケーションの参照]ダイアログ 285
14.7 イベント画面 286
14.7.1 [イベント一覧]画面 286
14.7.2 [イベント詳細]ダイアログ 288
14.8 設定画面 289
14.8.1 [ユーザーアカウントの管理]画面 289
14.8.2 [ユーザーアカウントの追加]ダイアログ 290
14.8.3 [ユーザーアカウントの編集]ダイアログ 291
14.8.4 [イベント通知の設定]画面 293
14.8.5 [メールサーバ設定]画面 294

15 コマンド 296
コマンドの説明形式 297
コマンドを実行する流れ 298
コマンド一覧 299
sdmexportdb（バックアップの取得） 302
sdmimportdb（バックアップデータのリストア） 305
sdmioutils exportdevice（スマートデバイス情報のエクスポート） 308
sdmioutils importdevice（スマートデバイス情報のインポート） 310
sdmioutils exportpolicy（セキュリティポリシー設定情報のエクスポート） 312
sdmioutils importpolicy（セキュリティポリシー設定情報のインポート） 314
sdmioutils exportsdpolicy（Android ポリシーまたは iOS プロファイルの情報のエクスポート） 316
sdmioutils importsdpolicy（Android ポリシーまたは iOS プロファイルの情報のインポート） 319
sdmioutils exportdeliveryapp（アプリケーション配布情報のエクスポート） 321
sdmioutils importdeliveryapp（アプリケーション配布情報のインポート） 324
sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート） 326
sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定） 330

sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除） 334
sdmdistributeapp（アプリケーションのインストール指示） 337
sdmapplyprofile（iOS プロファイルの適用または適用解除） 339
sdmgetinventory（インベントリ情報の取得） 341
sdmexportdistributestatus（アプリケーション配布状況の出力） 343
sdmexportinstallapp（インストールソフトウェア情報の出力） 346
sdmnetchange（スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更） 347
sdmcreatemdmcertreq（MDM 用署名済み証明書要求ファイルの作成） 350
sdmgetlogs（ログ情報の取得） 352

16 定義ファイル 355
16.1 定義ファイル一覧 356
16.2 スマートデバイスマネージャー環境設定ファイル（manager.properties） 357
16.3 Provisioning 情報設定ファイル（provisioning.properties） 361
16.4 イベントメールフォーマット情報ファイル（eventmail.properties） 363
16.5 テストメール送信フォーマット情報ファイル（testmail.properties） 366
16.6 通信サーバ環境設定ファイル（CommunicationServerEngine.properties） 367
16.7 メッセージングサーバ設定ファイル（SdMessagingServer.ini） 371

17 メッセージ 373
17.1 メッセージの形式 374
17.2 イベントとして出力される JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ 375
17.3 JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ一覧 384
17.4 JP1/ITDM2 - SDM（メッセージングサーバ）のメッセージ一覧 426
17.5 コマンドのメッセージ一覧 430

付録 431
付録 A フォルダ一覧 432
付録 A.1 スマートデバイスマネージャーに作成されるフォルダ 432
付録 A.2 通信サーバに作成されるフォルダ 433
付録 A.3 メッセージングサーバに作成されるフォルダ 434
付録 B サービス、プロセス一覧 435
付録 B.1 サービス一覧 435
付録 B.2 プロセス一覧 436
付録 C ポート番号一覧 438
付録 D パラメーター一覧 440
付録 D.1 ユーザーアカウントの設定のパラメーター 440
付録 D.2 イベント通知の設定のパラメーター 441
付録 D.3 メールサーバ設定のパラメーター 442
付録 E インポート・エクスポートファイルの出力形式 444

付録 E.1　スマートデバイス一覧エクスポート・インポート CSV ファイルの形式　444
付録 E.2　イベント一覧エクスポート CSV ファイルの形式　448
付録 E.3　セキュリティポリシー一覧エクスポート XML ファイルの形式　449
付録 E.4　スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式　451
付録 E.5　配布アプリケーションエクスポート XML ファイルの形式　452
付録 E.6　配布許可定義ファイルの形式　454
付録 E.7　アプリケーション配布情報ファイルの形式　455
付録 E.8　iOS プロファイル情報ファイルの形式　456
付録 E.9　デバイス情報ファイルの形式　457
付録 E.10　配布状況出力ファイルの形式　457
付録 E.11　インストールソフトウェア情報出力ファイルの形式　460
付録 F　サポートに必要な情報の格納先または入手方法　461
付録 G　SSL 通信用証明書の取得に使用するコマンド　463
付録 G.1　Web サーバの秘密鍵の作成（keygen）　463
付録 G.2　証明書発行要求（CSR）の作成（certutil reqgen）　464
付録 G.3　証明書発行要求（CSR）の内容表示（certutil req）　465
付録 G.4　証明書の内容表示（certutil cert）　465
付録 G.5　証明書の形式変換（certutil cert）　466
付録 G.6　パスワードファイルの作成（sslpasswd）　467
付録 H　インベントリ情報一覧　469
付録 I　各バージョンの変更内容　474
付録 I.1　11-10 の変更内容　474
付録 I.2　11-00 の変更内容　474
付録 J　このマニュアルの参考情報　476
付録 J.1　関連マニュアル　476
付録 J.2　このマニュアルで使用する書式　476
付録 J.3　コマンドの文法に使用する書式　476
付録 J.4　製品名の表記　477
付録 J.5　英略語　478
付録 J.6　KB（キロバイト）などの単位表記　479
付録 J.7　オンラインマニュアルについて　479
付録 K　用語解説　480

索引　484

# 1 製品の概要

ここでは、JP1/ITDM2 - SDM でできること、システムを構成する要素、各操作画面でできることなどについて説明します。

## 1.1 製品概要

JP1/ITDM2 - SDM は、スマートデバイスの運用管理およびセキュリティ対策を実現する製品です。

近年、スマートデバイス（スマートフォンやタブレット PC など）を IT 機器として業務目的で導入する企業が増えてきています。この動向に伴い、スマートデバイスをほかの IT 機器と同様に管理したいというニーズが高まっています。

JP1/ITDM2 - SDM は、組織内のスマートデバイスの運用管理やセキュリティ管理を支援します。JP1/ITDM2 - SDM を使用すると、JP1/IT Desktop Management 2 から PC やサーバ機器とスマートデバイスを一元管理できます。

### 1.1.1 この製品でできること

JP1/ITDM2 - SDM では、スマートデバイスの現状の把握、利用ルールの徹底、盗難・紛失時の情報漏えい対策、およびアプリケーションの配布ができます。また、統合的な IT 資産の管理ができます。

組織の業務でスマートデバイスを利用する場合、スマートデバイスの管理者は、組織で利用されているすべてのスマートデバイスを管理しなければなりません。また、利用者が業務以外の目的でスマートデバイスを使用することも防ぐ必要があります。さらに、スマートデバイス内の業務情報が外部に漏えいしないように対策する必要もあります。

JP1/ITDM2 - SDM は、スマートデバイスの一元管理を次の点から支援します。

- スマートデバイスの現状の把握
- スマートデバイスに対する利用ルールの徹底
- スマートデバイスの盗難・紛失時の情報漏えい対策
- スマートデバイスへのアプリケーションの配布
- 統合的な IT 資産の管理

スマートデバイスの現状を把握できます

組織で利用されているスマートデバイスが多くなると、スマートデバイスをどこで誰が使用しているのか把握することが困難になります。JP1/ITDM2 - SDM では、組織で所有するスマートデバイスを一覧で表示できます。これによって、管理者は組織内のスマートデバイスの情報を容易に把握できます。例えば、スマートデバイスの利用申請を受けた場合、管理者は利用されていないスマートデバイスを容易に特定でき、申請者に素早く配布できます。

スマートデバイスの利用ルールを徹底できます

スマートデバイスの管理者は、利用者が業務以外の目的でスマートデバイスを使用することを防ぐ必要があります。JP1/ITDM2 - SDM では、スマートデバイスにセキュリティのルールを適用することで、ルールに反した使用があった場合は管理者に通知したり、スマートデバイスの特定の機能を制限したりできます。例えば、通話できる電話番号や閲覧できる Web サイト、使用を許可するアプリケーション

をセキュリティポリシーとして定義し、スマートデバイスに適用すると、許可していない電話番号やWeb サイト、アプリケーションが使用された場合に管理者に通知されます。また、業務でカメラ機能を使う必要がない場合は、カメラ機能の使用を禁止するなどの制限もできます。

スマートデバイスの盗難や紛失時の情報漏えいを対策できます

利用者がスマートデバイスを紛失したり、盗難にあったりした場合に、第三者による悪用や情報漏えいを防ぐ必要があります。JP1/ITDM2 - SDM では、スマートデバイスを遠隔からロックし、第三者によるスマートデバイスの使用を防止できます。さらに、スマートデバイスを遠隔から初期化することで、紛失や盗難にあったスマートデバイスから情報が漏えいするのを防ぎます。

スマートデバイスにアプリケーションを配布できます

社内業務で利用するアプリケーションを一元管理したり、業務で使用するアプリケーションをスマートデバイスに一括配布したりできます。これによって、組織で利用するアプリケーションを統一し、スマートデバイスにアプリケーションを配布する作業を簡略化できます。

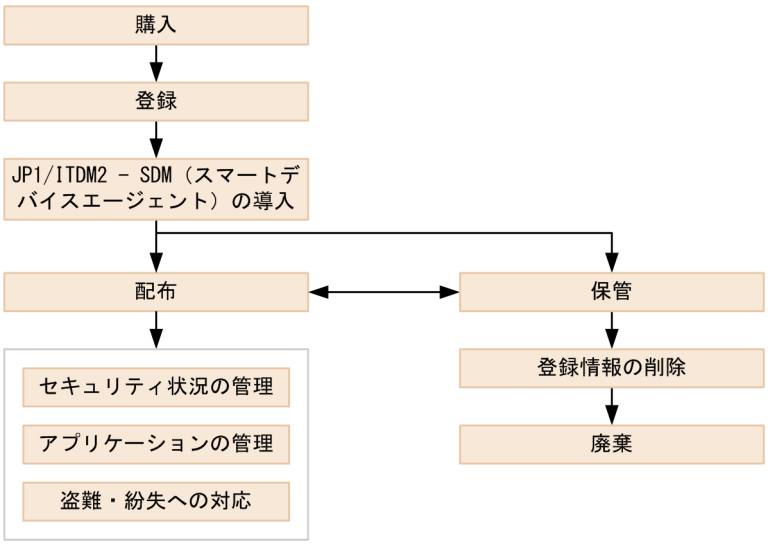
統合的に IT 資産を管理できます

JP1/ITDM2 - SDM のスマートデバイスの情報は、JP1/IT Desktop Management 2 から参照したり操作したりできます。これによって、PC やサーバ機器などのほかの IT 資産と同列にスマートデバイスを管理できます。例えば、管理者がスマートデバイスだけでなくほかの IT 資産も管理している場合、JP1/IT Desktop Management 2 を使用するだけで、スマートデバイスを含めた IT 資産全般を管理できます。

## 1.1.2 スマートデバイスの管理の流れ

JP1/IT Desktop Management 2 および JP1/ITDM2 - SDM では、組織内のスマートデバイスの購入から廃棄までを管理できます。

スマートデバイスの購入から廃棄までの流れを次に示します。



スマートデバイスを購入したら、JP1/ITDM2 - SDM にスマートデバイスの情報を登録します。スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入し、利用者に配布します。なお、スマートデバイスの情報は PC 等と同様に JP1/IT Desktop Management 2 で資産管理を実施します。

配布したスマートデバイスに対して、セキュリティ状況やアプリケーションを管理します。利用者がスマートデバイスを紛失したり、盗難にあったりした場合は、遠隔操作でロックや初期化などの対処をします。

利用しなくなったスマートデバイスは、設定を管理対象外に変更して保管します。以後利用しない場合は、JP1/ITDM2 - SDM から登録情報を削除し、スマートデバイスを廃棄します。

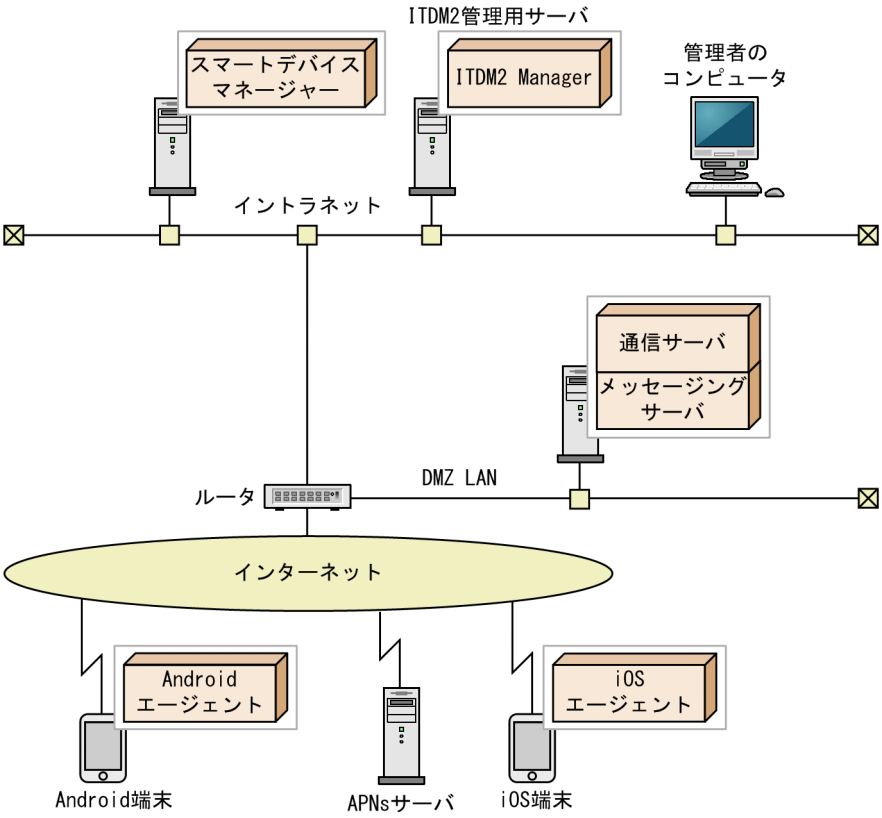
## 1.2 システムの構成要素の紹介

このマニュアルでは、JP1/ITDM2 - SDM で管理するシステムを説明するに当たり、JP1/ITDM2 - SDM がインストールされたサーバやスマートデバイスなどの、システムを構成する各要素の呼び方を定義しています。

JP1/ITDM2 - SDM の基本的なシステム構成要素の定義を次の表に示します。

| 項番 | 構成要素名 | 定義 |
|---|---|---|
| 1 | スマートデバイスマネージャー | JP1/ITDM2 - SDM（スマートデバイスマネージャー）がインストールされたサーバです。スマートデバイスマネージャーにはデータベースが生成され、JP1/ITDM2 - SDM で管理するさまざまな情報が格納されます。<br>1 台のスマートデバイスマネージャーで管理できるスマートデバイスは、最大 2,000 台です。 |
| 2 | ITDM2 管理用サーバ | PC やサーバ機器などの IT 資産とスマートデバイスを一元管理する構成要素です。 |
| 3 | 管理者のコンピュータ | 管理者が JP1/ITDM2 - SDM を画面で操作するためのコンピュータです。JP1/ITDM2 - SDM は Web ブラウザから操作画面を表示して操作します。そのため、スマートデバイスマネージャーにアクセスできるコンピュータであれば、どこからでも操作できます。スマートデバイスマネージャー自身も、管理者のコンピュータとして使用できます。 |
| 4 | 通信サーバ | スマートデバイスとデータ通信をするための、JP1/ITDM2 - SDM（通信サーバ）がインストールされたサーバです。<br>スマートデバイスからインベントリ情報を取得してデータベースに保存します。また、管理者からインベントリ取得要求やロック・初期化要求やポリシー適用要求があったときに、スマートデバイスに対して処理を要求します。 |
| 5 | メッセージングサーバ | Android 端末と JP1/ITDM2 - SDM の同期を取るための、JP1/ITDM2 - SDM（メッセージングサーバ）がインストールされたサーバです。<br>管理者からインベントリ取得要求やロック・初期化要求などがあったときに、Android 端末に対して、通信サーバに接続するよう要求します。 |
| 6 | Android 端末 | Android 端末を監視および制御するための、JP1/ITDM2 - SDM（スマートデバイス Android エージェント）がインストールされた Android 端末です。<br>インベントリや位置情報などのスマートデバイスの情報を JP1/ITDM2 - SDM に送信し、管理者からロックや初期化要求があった場合に処理をします。 |
| 7 | iOS 端末 | iOS 端末を監視および制御するための、JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）がインストールされた iOS 端末です。<br>インベントリなどのスマートデバイスの情報を JP1/ITDM2 - SDM に送信します。 |
| 8 | APNs サーバ | iOS 端末を制御するための Apple 社のサーバです。JP1/ITDM2 - SDM から iOS 端末に対するインベントリの取得要求や、ロック・初期化の要求などは APNs サーバ経由で要求をします。 |

各システム構成要素を配置した、JP1/ITDM2 - SDM で管理する基本的なシステムの構成例を次の図に示します。




## 関連項目

- 3.4 JP1/ITDM2 - SDM を構成するコンポーネント

## 1.3　操作画面の紹介

JP1/ITDM2 - SDM では、上部のボタンで画面を切り替えて各機能を使用します。

各画面でできることを次に示します。

ホーム画面

ホーム画面では、JP1/ITDM2 - SDM で管理している情報の概況を各パネルで確認できます。また、各パネルからほかの画面に移動して、管理作業を始められます。

セキュリティ画面

セキュリティ画面では、組織で策定したセキュリティのルールを一覧で把握できます。また、セキュリティのルールのスマートデバイスへの適用状況を把握できます。

スマートデバイス画面

スマートデバイス画面では、組織で管理しているスマートデバイスを一覧で把握できます。また、管理対象のスマートデバイスのハードウェア情報やインストールされているアプリケーションの情報などを確認したり、スマートデバイスに対する遠隔操作を実行したりできます。これによって、セキュリティ状況に問題があるスマートデバイスに対する対策を実行できます。

配布画面

配布画面では、スマートデバイスに配布するアプリケーションを一覧で把握できます。また、管理対象のスマートデバイスに対し、アプリケーションを配布してインストールを指示したり、アンインストールを指示したりできます。

イベント画面

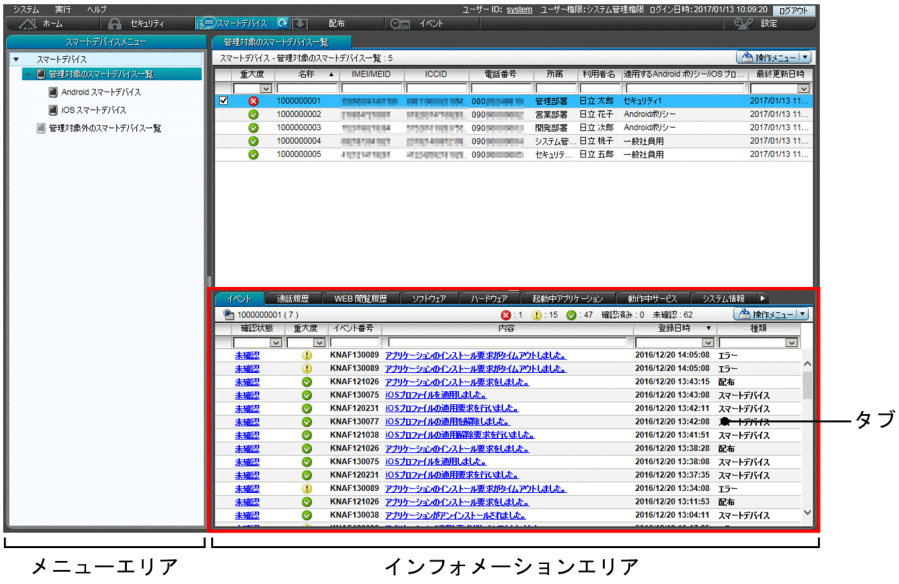
イベント画面では、JP1/ITDM2 - SDM の運用中に発生したイベントを確認できます。

設定画面

設定画面では、ユーザーアカウントやイベントのメール通知など JP1/ITDM2 - SDM の各種設定をカスタマイズできます。

### 1.3.1　基本的な画面構成

JP1/ITDM2 - SDM の基本的な画面構成と、画面内の呼び方について説明します。




メニューエリア

選択した画面に応じてメニューが表示されます。各メニューの項目を選択すると、対応する情報がインフォメーションエリアに表示されます。

インフォメーションエリア

メニューエリアで選択した項目に応じて、情報が表示されます。

タブ

インフォメーションエリアの下部にはインフォメーションエリアの上部で選択した情報の詳細情報が表示されます。

### 画面上部のメニュー

画面上部のメニューでは、各画面で共通の項目が表示されます。

システム

JP1/ITDM2 - SDM からログアウトできます。

実行

現在ログインしているユーザーアカウントの編集ができます。

ヘルプ

JP1/ITDM2 - SDM のヘルプおよび製品のバージョン情報を確認できます。

［ログアウト］ボタン

JP1/ITDM2 - SDM からログアウトできます。［ログアウト］ボタンの左には、現在ログインしているユーザーアカウントのユーザー ID、ユーザー権限、およびログイン日時が表示されます。ユーザー ID をクリックすると、ユーザーアカウントの情報を編集したり、パスワードを変更したりできます。

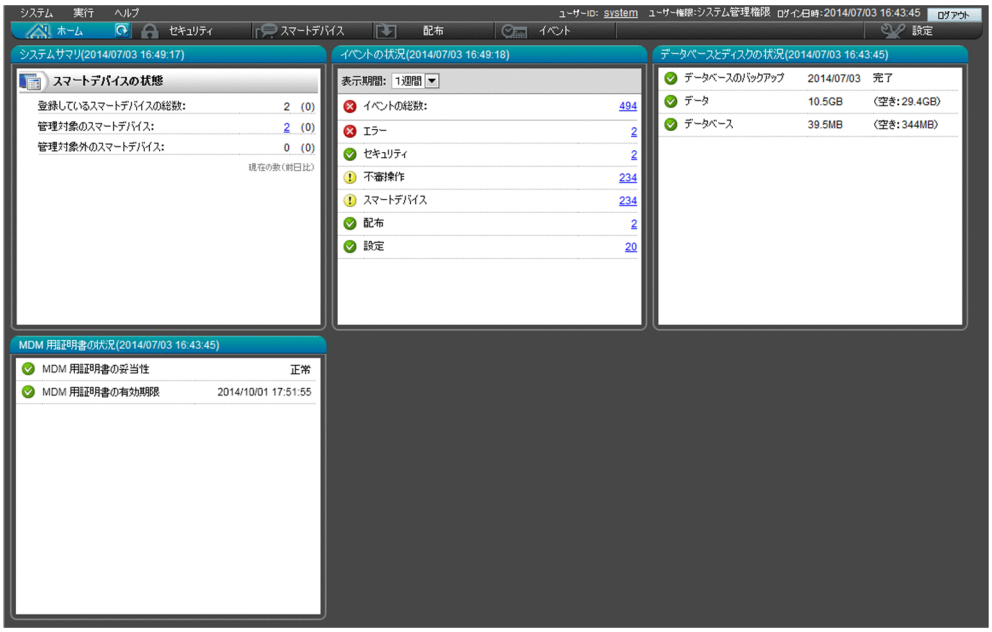
**画面上部のボタン**

画面上部のボタンで、画面を切り替えて各機能を使用できます。

## 1.3.2　ホーム画面でできること

ホーム画面は、ログイン後に最初に表示され、JP1/ITDM2 - SDM の運用の基点となる画面です。

ホーム画面では、JP1/ITDM2 - SDM で管理している情報の概況を各パネルで確認できます。各パネルには、それぞれの画面で管理している情報が表示され、状況を素早く確認できます。




状況を確認したら、各画面のボタン、または各パネルのリンクからほかの画面に移動し、管理作業を始めてください。

## 1.3.3　セキュリティ画面でできること

セキュリティ画面では、セキュリティのルールを作成できます。セキュリティのルールをスマートデバイスに適用することで、セキュリティ状況を管理したり、セキュリティ状況に問題があるスマートデバイスに対策を実行したりできます。

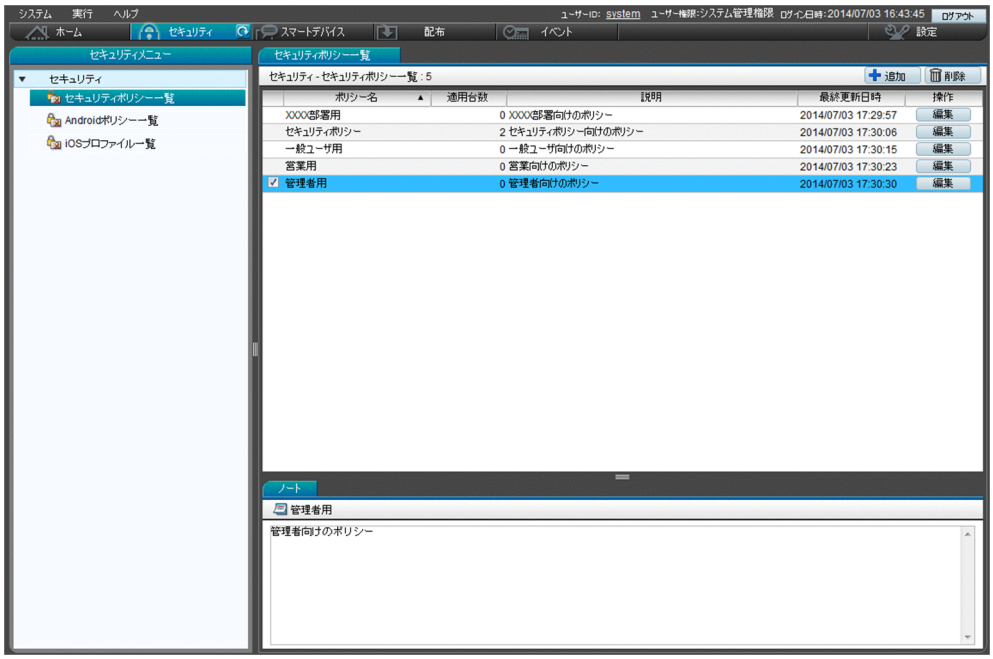
セキュリティ画面には次に示す画面があります。

- [セキュリティポリシー一覧] 画面
- [Android ポリシー一覧] 画面
- [iOS プロファイル一覧] 画面

各画面について以降で説明します。

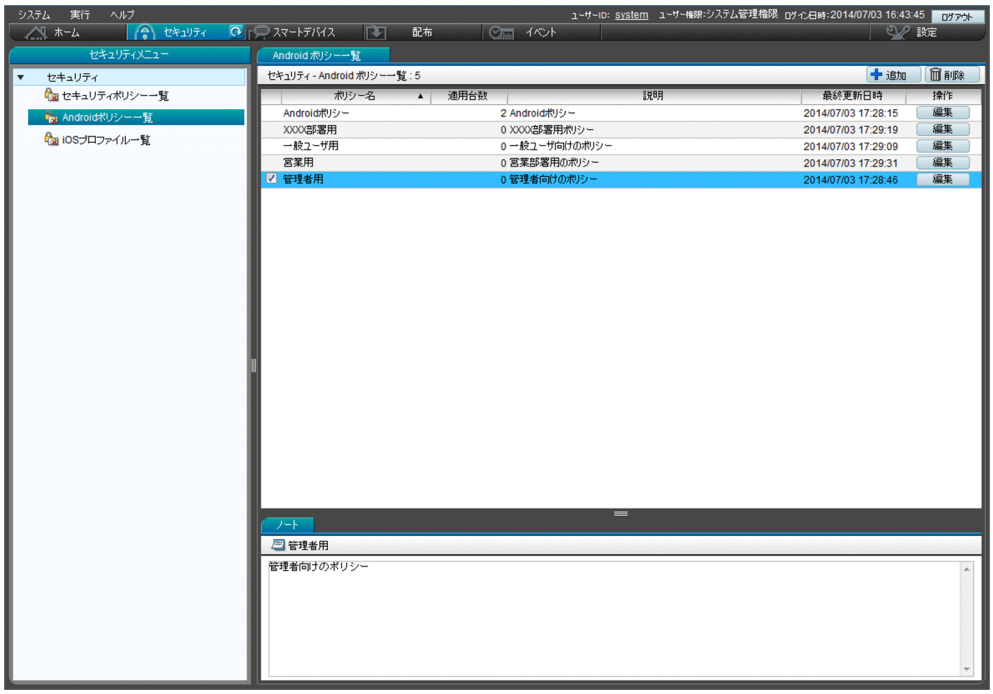
[セキュリティポリシー一覧] 画面

スマートデバイスに適用するセキュリティポリシーを作成できます。



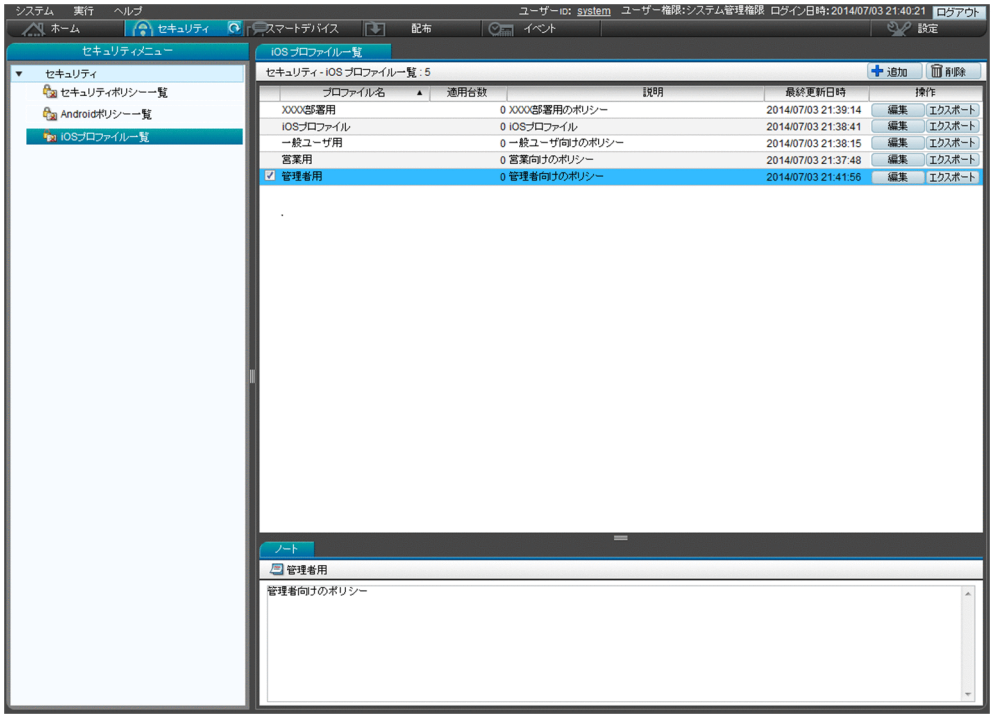

[Android ポリシー一覧] 画面

Android 端末に適用する Android ポリシーを作成できます。




[iOS プロファイル一覧] 画面

iOS 端末に適用する iOS プロファイルを登録できます。




## 1.3.4　スマートデバイス画面でできること

スマートデバイス画面では、スマートデバイスの情報を確認・登録したり、セキュリティ画面で作成したセキュリティのルールをスマートデバイスに適用したりできます。また、ロックや初期化など、スマートデバイスに対して遠隔操作をすることもできます。

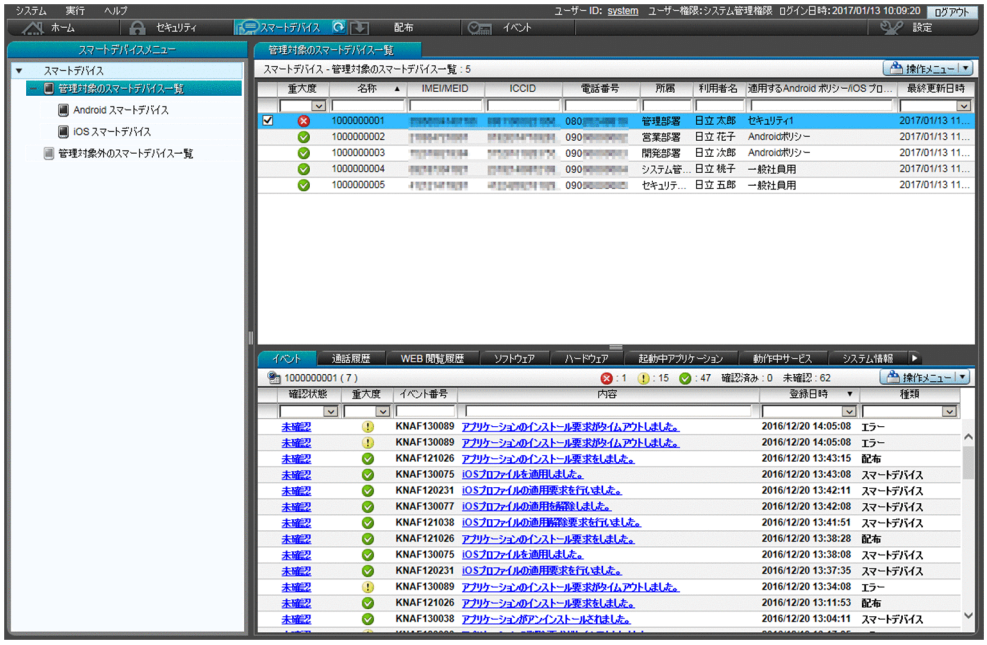
スマートデバイス画面には次に示す画面があります。

- ［管理対象のスマートデバイス一覧］画面
- ［管理対象外のスマートデバイス一覧］画面

各画面について以降で説明します。

［管理対象のスマートデバイス一覧］画面

　管理対象のスマートデバイスの情報を確認できます。

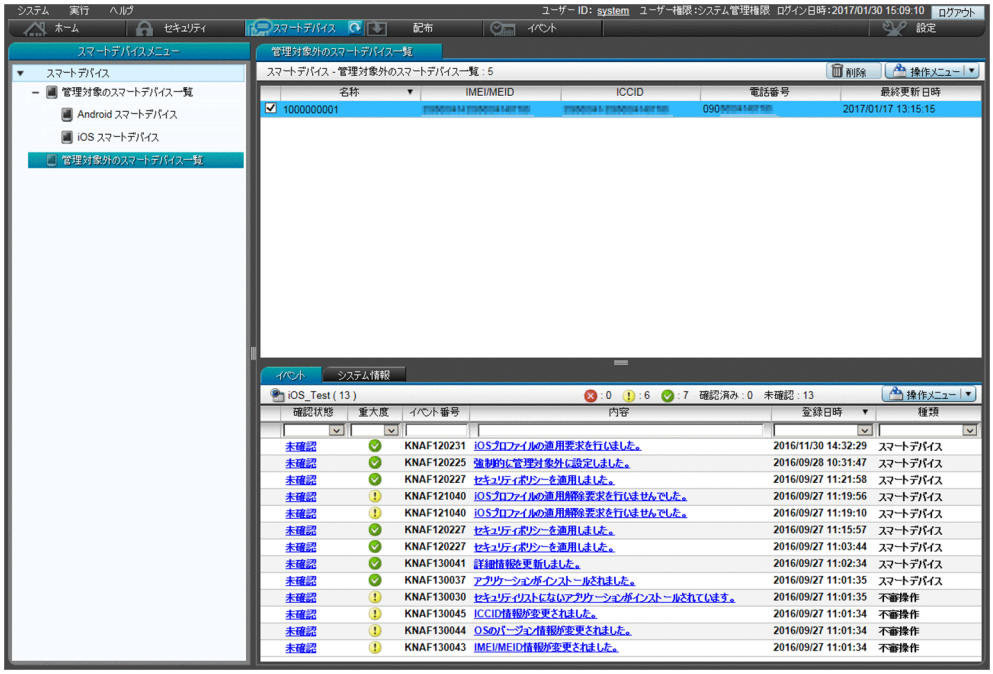


メニューエリアの［Android スマートデバイス］を選択すると Android 端末の一覧を、［iOS スマートデバイス］を選択すると iOS 端末の一覧を表示できます。

インフォメーションエリアの上部で選択したスマートデバイスの詳細情報が、下部のタブに表示されます。発生したイベント、通話履歴、Web 閲覧履歴、ソフトウェア（アプリケーション）、ハードウェア、起動中アプリケーション、動作中サービス、システム情報、セキュリティ、および Bluetooth 接続情報が確認できます。

［管理対象外のスマートデバイス一覧］画面

管理対象外のスマートデバイスの情報を確認できます。



インフォメーションエリアの上部で選択したスマートデバイスの詳細情報が、下部のタブに表示されます。イベントおよびシステム情報が確認できます。

なお、管理対象外のスマートデバイスに、セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを適用すると、そのスマートデバイスを管理対象にできます。

## 1.3.5 配布画面でできること

配布画面では、スマートデバイスに配布するアプリケーションを管理できます。また、スマートデバイスにアプリケーションを配布したり、インストールの指示をしたりできます。配布したアプリケーションについて、アンインストールの指示をしたり、削除したりすることもできます。

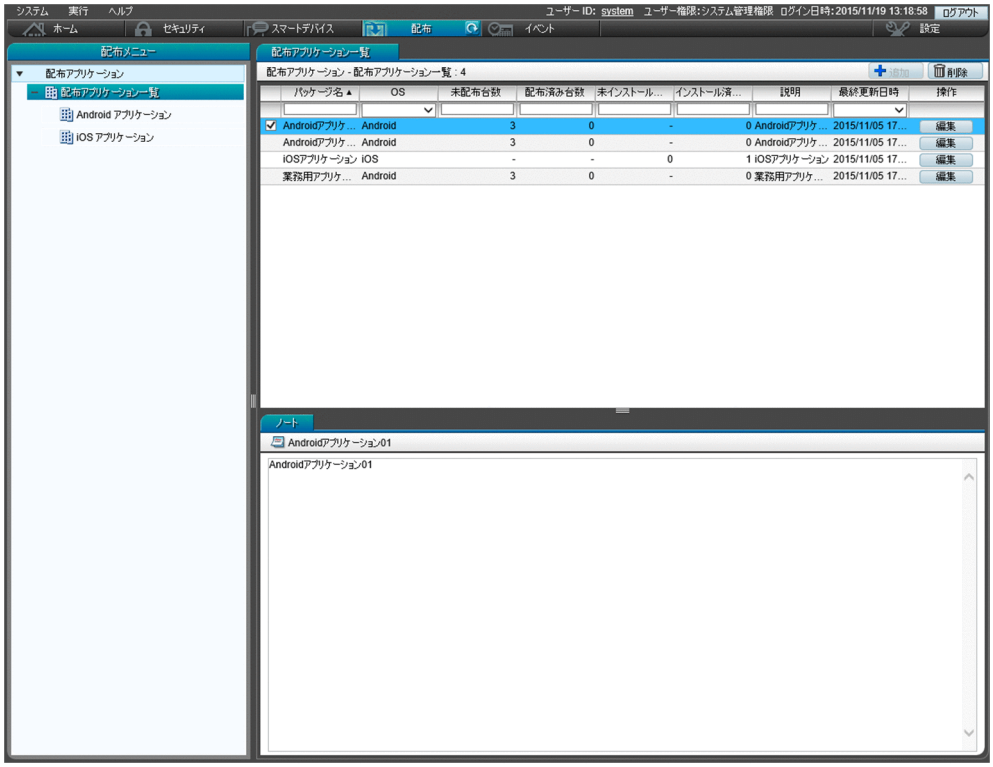
配布画面には次に示す画面があります。

- [配布アプリケーション一覧] 画面
- [Android アプリケーション] 画面
- [iOS アプリケーション] 画面

各画面について以降で説明します。

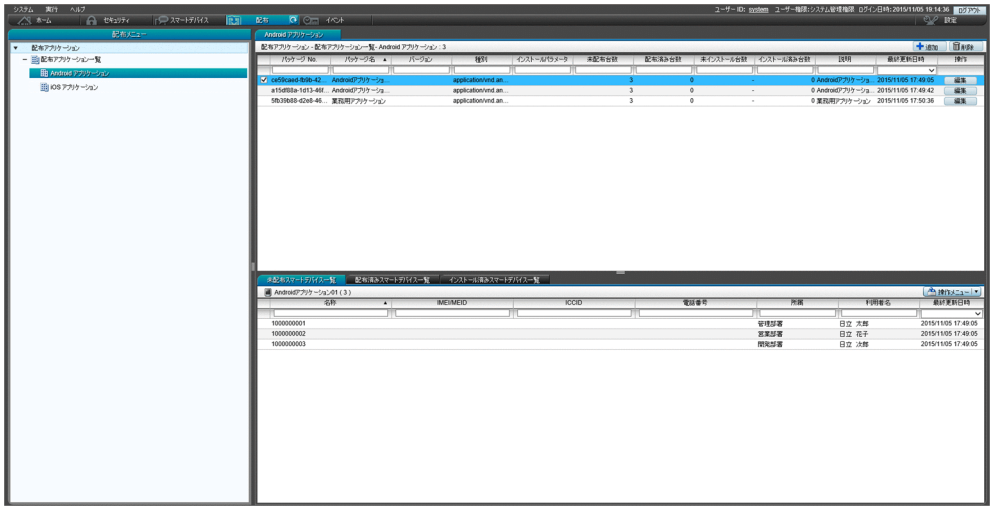
[配布アプリケーション一覧] 画面

スマートデバイスに配布するアプリケーションの一覧およびアプリケーションの配布状況のサマリを確認できます。




[Android アプリケーション] 画面

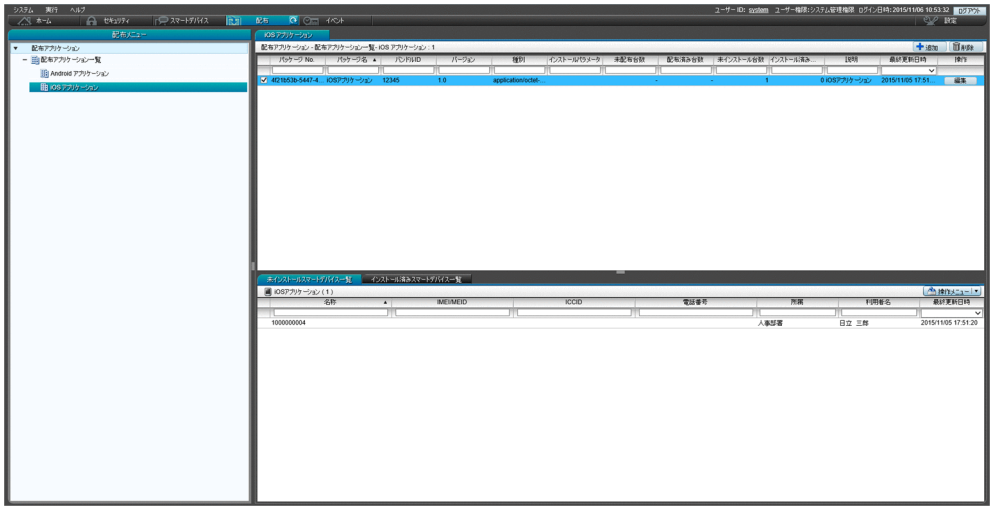
JP1/ITDM2 - SDM に登録した Android アプリケーションの一覧を確認できます。



インフォメーションエリアの上部で Android アプリケーションを選択すると、下部のタブに配布状態ごとにスマートデバイスの一覧が表示されます。配布状態は未配布、配布済み、インストール済みの 3 種類です。また、各スマートデバイスに対してアプリケーションの配布と削除、インストールの指示、およびアンインストールの指示を実行できます。

[iOS アプリケーション] 画面

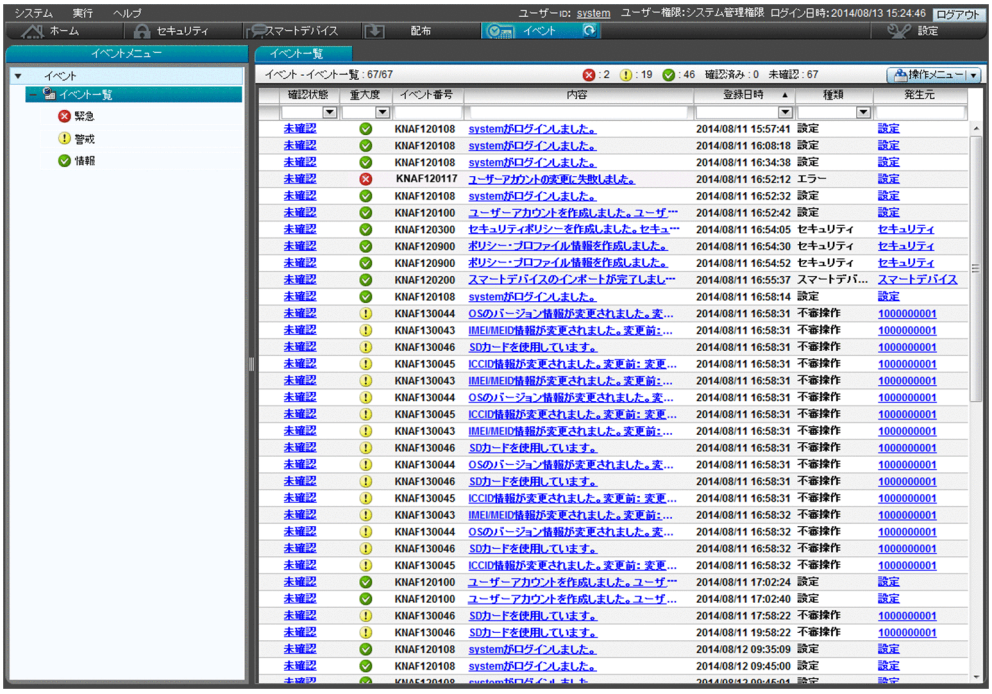
JP1/ITDM2 - SDM に登録した iOS アプリケーションの一覧を確認できます。



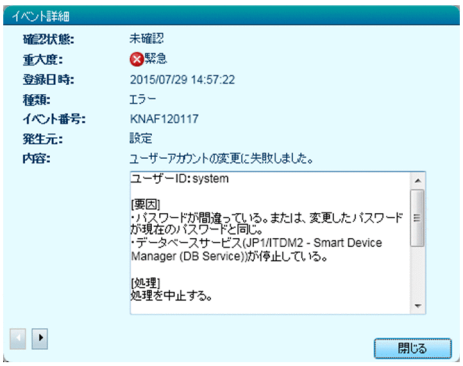
インフォメーションエリアの上部で iOS アプリケーションを選択すると、下部のタブに配布状態ごとにスマートデバイスの一覧が表示されます。配布状態は未インストール、インストール済みの 2 種類です。また、各スマートデバイスに対してアプリケーションのインストールの指示、およびアンインストールの指示を実行できます。

## 1.3.6 イベント画面でできること

イベント画面では、JP1/ITDM2 - SDM の運用中に発生したイベントを確認できます。セキュリティ判定の操作が正常に終了したかどうかなどがイベントとして表示されます。




[内容] のリンクをクリックすると、イベントの詳細を確認できます。




イベントの内容によっては早急に対処が必要な場合があります。重大度が [緊急] のイベントを最優先に確認し、次に [警戒] のイベントを確認してください。イベントの内容から原因を特定して対処します。

イベントを確認して対処が完了したら、イベントの [確認状態] を [確認済み] にします。[確認状態] を変更することで、対処が完了したイベントかどうかを区別できます。

## 1.3.7 設定画面でできること

設定画面では、ユーザーアカウントの管理や、イベントが発生した際のメール通知など、JP1/ITDM2 - SDM を運用するために必要な設定ができます。

設定画面には次に示す画面があります。

ユーザー管理

［ユーザーアカウントの管理］画面

イベント

［イベント通知の設定］画面

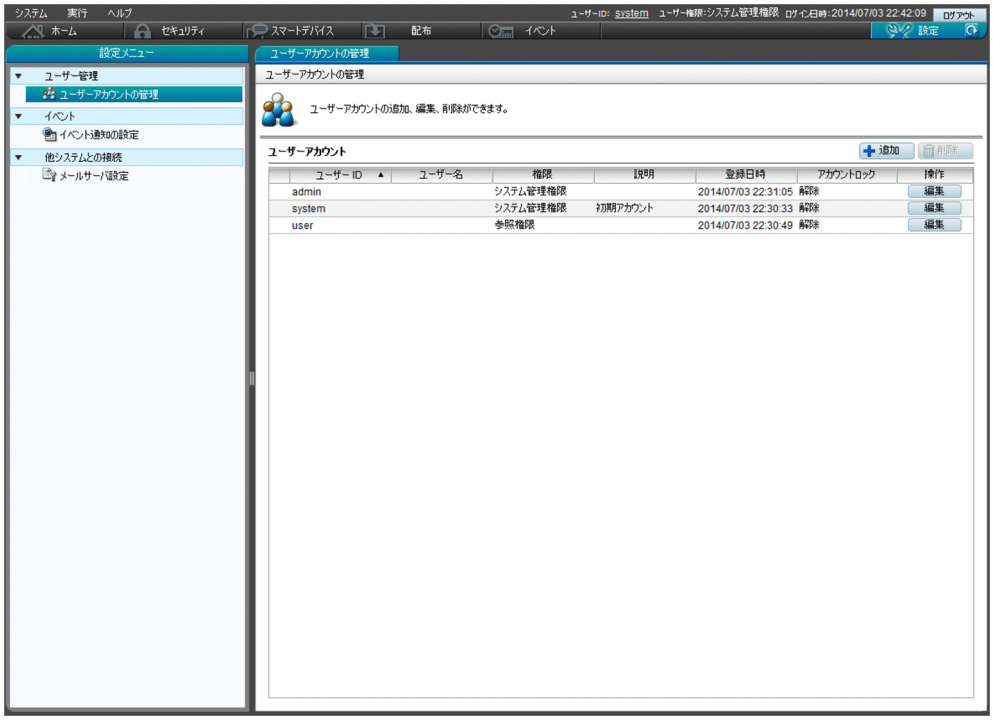
他システムとの接続

［メールサーバ設定］画面

各画面について以降で説明します。

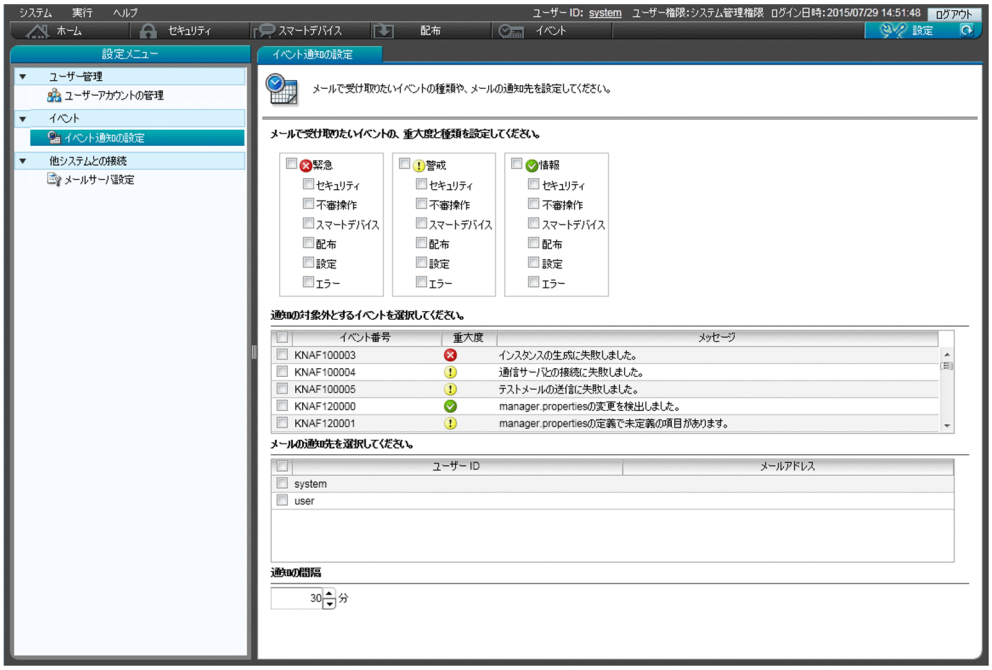
［ユーザーアカウントの管理］画面

JP1/ITDM2 - SDM のユーザーアカウントを追加、編集、および削除できます。



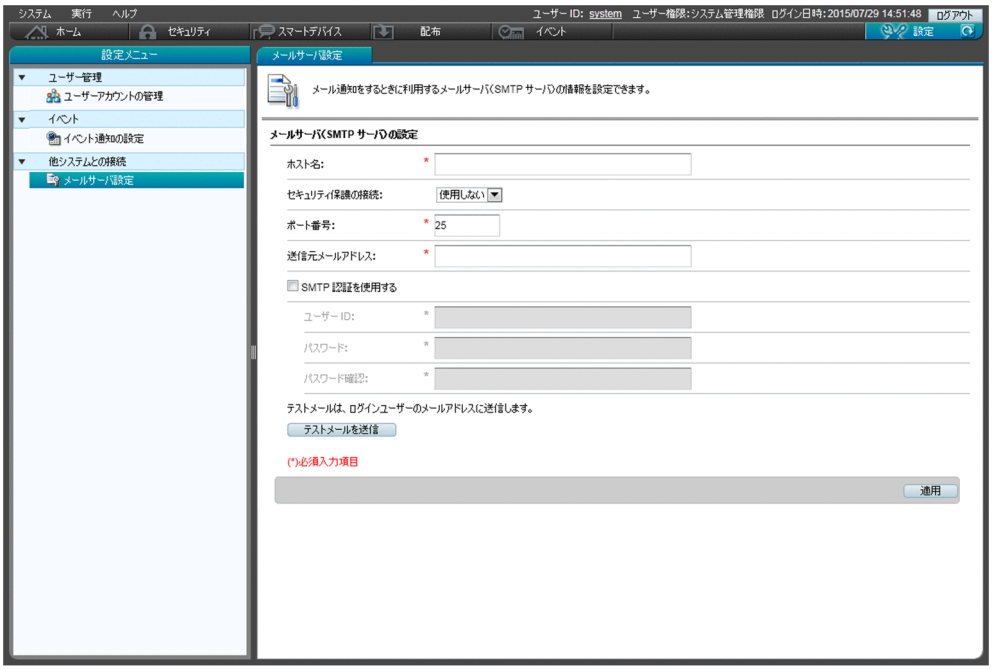

［イベント通知の設定］画面

メールで通知するイベントの重大度および種類、通知の対象外にするイベント、イベント発生時にメールで通知するユーザーを設定できます。




［メールサーバ設定］画面

イベントをメールで通知する場合に、メールサーバとの接続情報を設定できます。



# 2 機能の紹介

ここでは、セキュリティの管理や、スマートデバイスの管理、アプリケーションの管理やイベントの表示などの、JP1/ITDM2 - SDM の機能の詳細について説明します。

# 2.1 機能一覧

JP1/ITDM2 - SDM の機能を一覧で説明します。

### 機能一覧

| 項番 | 機能 | 概要 |
|---|---|---|
| 1 | システムの概況表示 | システムの概況として次の確認ができます。<br>• スマートデバイスの状態<br>• イベントの状況<br>• データベースとハードディスクの状況<br>• MDM 用証明書の状況 |
| 2 | ユーザーアカウントの管理 | JP1/ITDM2 - SDM の使用者の役割に応じたユーザーアカウントを作成できます。 |
| 3 | セキュリティの管理 | スマートデバイスのセキュリティポリシーを作成できます。また、スマートデバイスに応じて Android ポリシーを作成したり、iOS プロファイルを登録したりできます。これらをスマートデバイスに適用することでセキュリティ状況を判定できます。 |
| 4 | スマートデバイスの管理 | JP1/ITDM2 - SDM に登録されているスマートデバイスを一覧で確認できます。また、スマートデバイスごとにハードウェア情報やソフトウェア情報などの機器の詳細情報を確認できます。さらに、セキュリティ上問題が発生したスマートデバイスに対して、ロックや初期化などの遠隔操作ができます。 |
| 5 | アプリケーションの管理 | スマートデバイスに配布するアプリケーションを一元管理できます。スマートデバイスへのアプリケーションの配布と削除、インストールの指示、およびアンインストールの指示ができます。 |
| 6 | イベントの表示 | JP1/ITDM2 - SDM の各機能の実行結果や発生した事象などをイベントとして確認できます。 |

### 関連項目

- 2.2 システムの概況表示
- 2.3 ユーザーアカウントの管理
- 2.4 セキュリティの管理
- 2.5 スマートデバイスの管理
- 2.6 アプリケーションの管理
- 2.7 イベントの表示

## 2.2　システムの概況表示

JP1/ITDM2 - SDM に登録されているスマートデバイスの状態やイベントの状況を確認できます。また、スマートデバイスマネージャーでの、データベースのバックアップの実施有無、ハードディスクの使用状況や空き容量、MDM 用証明書の状況などを確認できます。

［システムサマリ］パネル

JP1/ITDM2 - SDM に登録されているスマートデバイスの概況が表示されます。

［スマートデバイスの状態］では、次のことが確認できます。

- 登録しているスマートデバイスの総数および前日との差分台数
- 管理対象のスマートデバイスの台数および前日との差分台数
- 管理対象外のスマートデバイスの台数および前日との差分台数

管理対象または管理対象外のスマートデバイスの台数のリンクをクリックすると、スマートデバイス画面が表示され、スマートデバイスの詳細な情報を確認できます。

［イベントの状況］パネル

1 週間以内に発生したイベントの総件数およびイベントの種類別の発生件数が表示されます。

重大度が「緊急」のイベントが発生している場合は、イベントの種類の左側のアイコンが で表示されます。このとき、発生件数のリンクをクリックするとイベント画面が表示され、イベントの内容を確認できます。

なお、表示期間を変更して、3 日以内または 1 日以内のイベント件数を確認することもできます。

［データベースとディスクの状況］パネル

次のことが確認できます。

- データベースのバックアップの実施状況
- データのハードディスクの使用量および空き容量
- データベースのハードディスクの使用量および空き容量

> **ヒント**
>
> ハードディスクの空き容量が少なくなったら、データベースのバックアップ先を十分に空き容量があるディスク上のフォルダに変更したり、不要なデータを退避したりして空き容量を増やす必要があります。

［MDM 用証明書の状況］パネル

次のことが確認できます。

- MDM 用証明書の妥当性
- MDM 用証明書の有効期限

**関連項目**

- 2.5 スマートデバイスの管理
- 2.7 イベントの表示
- 14.3 ホーム画面
- 14.5 スマートデバイス画面
- 14.7 イベント画面

## 2.3　ユーザーアカウントの管理

複数の管理者が JP1/ITDM2 - SDM を使用する場合、管理者ごとにユーザーアカウントを作成できます。

ユーザーアカウントには、ユーザーの操作範囲に応じて次の設定ができます。

権限

情報を参照するだけの経営者、スマートデバイスを管理するシステム管理者など、ユーザーの操作範囲に応じて権限を設定できます。

### 2.3.1　ユーザーアカウントのロック

JP1/ITDM2 - SDM のログインに 3 回続けて失敗すると、ユーザーアカウントがロックされます。そのユーザーアカウントはロックが解除されるまでログインできなくなります。

ロックされているユーザーアカウントがあるかどうかの確認およびロックの解除は、システム管理権限を持つユーザーアカウントでログインしたあと、設定画面の［ユーザーアカウントの管理］画面から実施します。

ロックされているユーザーアカウントは、［ユーザーアカウントの管理］画面で［アカウントロック］に［ロック中］と表示されます。

**関連項目**

- 2.3.2 ユーザーアカウントの権限
- 6.7 ユーザーアカウントのロックを解除する手順
- 14.8.1 ［ユーザーアカウントの管理］画面

### 2.3.2　ユーザーアカウントの権限

JP1/ITDM2 - SDM のユーザーアカウントに設定できる権限は 2 種類あります。

- システム管理権限
  JP1/ITDM2 - SDM のすべての機能が利用できる権限です。
- 参照権限
  JP1/ITDM2 - SDM で管理する情報を参照できる権限です。参照権限はデフォルトで設定されます。

**関連項目**

- 2.3.1 ユーザーアカウントのロック
- 2.3.3 参照権限で実行できない操作一覧

## 2.3.3　参照権限で実行できない操作一覧

ユーザーアカウントに参照権限を設定している場合に実行できない操作について説明します。

### 参照権限で実行できない操作一覧

| 画面 | | 操作 |
|---|---|---|
| セキュリティ画面 | [セキュリティポリシー一覧] 画面 | セキュリティポリシーの操作（追加・編集・削除） |
| | | セキュリティポリシーのノート更新 |
| | [Android ポリシー一覧] 画面 | Android ポリシーの操作（追加・編集・削除） |
| | | Android ポリシーのノート更新 |
| | [iOS プロファイル一覧] 画面 | iOS プロファイルの操作（追加・削除） |
| | | iOS プロファイル情報の編集 |
| | | iOS プロファイルのノート更新 |
| スマートデバイス画面 | [管理対象のスマートデバイス一覧] 画面 | 次の操作メニュー<br>• 最新の情報を取得する<br>• 初期化する<br>• ロックする<br>• パスコードをリセットする<br>• メッセージを通知する<br>• 管理対象外にする<br>• セキュリティポリシーを適用する<br>• Android ポリシーを適用する<br>• iOS プロファイルを適用する<br>• iOS プロファイルの適用を解除する<br>• スマートデバイスを追加する<br>• スマートデバイス一覧をインポートする |
| | [管理対象のスマートデバイス一覧] 画面の［イベント］タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する |
| | [管理対象のスマートデバイス一覧] 画面の［通話履歴］タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する<br>• 許可する |
| | [管理対象のスマートデバイス一覧] 画面の［WEB 閲覧履歴］タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する<br>• 許可する<br>• 禁止する |

| 画面 | | 操作 |
|---|---|---|
| スマートデバイス画面 | [管理対象のスマートデバイス一覧] 画面の [ソフトウェア] タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する<br>• 許可する<br>• 禁止する |
| | [管理対象のスマートデバイス一覧] 画面の [Bluetooth 接続情報] タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する |
| | [管理対象外のスマートデバイス一覧] 画面 | 次の操作メニュー<br>• セキュリティポリシーを適用する<br>• Android ポリシーを適用する<br>• iOS プロファイルを適用する |
| | | スマートデバイスの削除 |
| | [管理対象外のスマートデバイス一覧] 画面の [イベント] タブ | 次の操作メニュー<br>• 確認済みに設定する<br>• 未確認に設定する |
| 配布画面 | [配布アプリケーション一覧] 画面 | 配布アプリケーションの操作（編集・削除） |
| | | 配布アプリケーションのノート更新 |
| | [Android アプリケーション] 画面 | Android アプリケーションの操作（追加・編集・削除） |
| | [Android アプリケーション] 画面の [未配布スマートデバイス一覧] タブ | 次の操作メニュー<br>• アプリケーション配布<br>• アプリケーションインストール |
| | [Android アプリケーション] 画面の [配布済みスマートデバイス一覧] タブ | 次の操作メニュー<br>• アプリケーションインストール<br>• アプリケーション削除 |
| | [Android アプリケーション] 画面の [インストール済みスマートデバイス一覧] タブ | 次の操作メニュー<br>• アプリケーション削除 |
| | [iOS アプリケーション] 画面 | iOS アプリケーションの操作（追加・編集・削除） |
| | [iOS アプリケーション] 画面の [未インストールスマートデバイス一覧] タブ | 次の操作メニュー<br>• アプリケーションインストール |
| | [iOS アプリケーション] 画面の [インストール済みスマートデバイス一覧] タブ | 次の操作メニュー<br>• アプリケーション削除 |
| イベント画面 | [イベント一覧] 画面 | 次の操作メニュー<br>• 確認済みに設定する |

| 画面 | | 操作 |
|---|---|---|
| イベント画面 | ［イベント一覧］画面 | • 未確認に設定する |
| 設定画面 | ［ユーザーアカウントの管理］画面 | ユーザーアカウントの管理 |
| | ［イベント通知の設定］画面 | イベント通知の設定 |
| | ［メールサーバ設定］画面 | メールサーバの設定 |

### 関連項目

- 2.3.2 ユーザーアカウントの権限

## 2.4　セキュリティの管理

セキュリティのルールを作成し、スマートデバイスに適用することで、スマートデバイスを管理できます。

### 2.4.1　セキュリティのルールの種類

セキュリティのルールには、セキュリティポリシー、Android ポリシー、および iOS プロファイルの 3 種類があります。

セキュリティポリシー

スマートデバイスの利用状況を監視するためのポリシーです。セキュリティポリシーには、電話番号、Web サイト、およびアプリケーションを設定できます。このポリシーとスマートデバイスの利用履歴を確認し、ポリシーに反した利用があった場合にイベントを発行します。管理者は、発行されたイベントを確認することでスマートデバイスの不正利用を検知できます。

Android ポリシー

Android 端末に対して設定する動作ポリシーです。パスワードのルールを設定したり、カメラ機能の利用を制限したりできます。

iOS プロファイル

iOS 端末に対して設定する動作ポリシーです。Apple 社が提供する iPhone 構成ユーティリティで構成プロファイルを作成し、iOS プロファイルとして登録できます。パスコードのルールを設定したり、カメラ機能の利用を制限したりできます。

セキュリティのルールによって、スマートデバイスに対して利用を抑止または監視できる代表的な機能を次に示します。

| 機能 | Android 端末 | iOS 端末 |
|---|---|---|
| カメラ | 抑止可 | 抑止可 |
| アプリケーションのインストール（AppStore の利用） | 抑止不可 | 抑止可 |
| 通話履歴 | 監視可 | 監視不可 |
| Web 閲覧履歴 | 監視可 | 監視不可 |
| アプリケーション利用履歴 | 監視可 | 監視不可 |

（凡例）

抑止：Android ポリシーまたは iOS プロファイルで設定します。

監視：セキュリティポリシーで設定します。

**関連項目**

- 2.4.2 セキュリティポリシーの管理
- 2.4.3 セキュリティポリシーに設定できる項目

- 2.4.4 Android ポリシーの管理
- 2.4.5 Android ポリシーに設定できる項目
- 2.4.6 iOS プロファイルの管理
- 2.4.7 iOS プロファイルに設定できる項目について

## 2.4.2 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一覧］画面で、セキュリティポリシーを作成して管理できます。

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。

セキュリティポリシーを編集する

セキュリティ対策の傾向が変化したり、組織のセキュリティ方針が変更になったりした場合は、セキュリティポリシーを編集します。

セキュリティ対策の傾向は、スマートデバイスやネットワークの環境とともに変化しています。最新のセキュリティ対策を組織内に取り込み続けることで、強固なセキュリティ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などに伴って、不要になったセキュリティポリシーを削除します。

**関連項目**

- 2.4.3 セキュリティポリシーに設定できる項目
- 7.1 セキュリティポリシーを利用する

## 2.4.3 セキュリティポリシーに設定できる項目

セキュリティポリシーには、利用を監視する電話番号、Web サイト、およびアプリケーションを設定できます。

**セキュリティポリシーに設定できる項目**

| 項番 | 設定できる項目 | 説明 |
|---|---|---|
| 1 | 電話番号 | 利用を監視する電話番号を設定できます。このリストに登録されていない電話番号が利用された場合、イベントが発行され管理者に通知されます。 |
| 2 | Web サイト | 閲覧を監視する Web サイトを設定できます。<br>ホワイトリストで設定した Web サイト以外、またはブラックリストで設定した Web サイトが閲覧された場合、イベントが発行され管理者に通知されます。 |

| 項番 | 設定できる項目 | 説明 |
|---|---|---|
| 3 | アプリケーション | インストールを監視するアプリケーションを設定できます。ホワイトリストで設定したアプリケーション以外、またはブラックリストで設定したアプリケーションがインストールされた場合、イベントが発行され管理者に通知されます。<br>ホワイトリストで設定したアプリケーションの場合、インストールが必須か任意かを設定できます。インストール必須のアプリケーションがインストールされていない場合、イベントが発行され管理者に通知されます。 |

**関連項目**

- 2.4.2 セキュリティポリシーの管理
- 14.4.1 ［セキュリティポリシー一覧］画面

## 2.4.4 Android ポリシーの管理

セキュリティ画面の［Android ポリシー一覧］画面で、Android ポリシーを作成して管理できます。

Android ポリシーを作成する

組織のセキュリティ方針を基に Android ポリシーを作成します。Android ポリシーは複数作成できます。

Android ポリシーを編集する

組織のセキュリティ方針が変更になった場合は、Android ポリシーを編集します。

Android ポリシーを削除する

管理体制の変更や Android ポリシーの統合などに伴って、不要になった Android ポリシーを削除します。

**関連項目**

- 2.4.5 Android ポリシーに設定できる項目
- 7.2 Android ポリシーを利用する

## 2.4.5 Android ポリシーに設定できる項目

Android ポリシーには、パスワードのルールや、Android 端末が自動的にロックされるまでの時間、カメラの利用可否などを設定できます。

### Android ポリシーに設定できる項目

| 項番 | 設定できる項目 | 説明 |
|---|---|---|
| 1 | パスワードの複雑さ | パスワードの複雑さを次の 5 種類から設定できます。<br>• 1（アルファベットが必要なパスワード） |

| 項番 | 設定できる項目 | 説明 |
|---|---|---|
| 1 | パスワードの複雑さ | • 2（アルファベット、数字が必要なパスワード）<br>• 3（アルファベット、数字および特殊記号が必要なパスワード）<br>• 4（任意の文字列のパスワード）<br>• 5（生体認証）<br>初期値は「1」（アルファベットが必要なパスワード）です。 |
| 2 | パスワード長の下限値 | パスワードに必要な文字数を設定できます。<br>「パスワードの複雑さ」が「5」（生体認証）以外の場合に有効です。<br>初期値は「4」です。設定できる値は 4～16 です。 |
| 3 | パスワード内のアルファベットが必要な最小の文字数 | パスワードに要求されるアルファベットの最小の文字数を設定します。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |
| 4 | パスワード内の小文字が必要な最小の文字数 | パスワードに必要な小文字の最小の文字数を設定できます。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |
| 5 | パスワード内の大文字が必要な最小の文字数 | パスワードに必要な大文字の最小の文字数を設定できます。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |
| 6 | パスワード内のアルファベット以外の最小の文字数 | パスワードに必要なアルファベット以外の最小の文字数を設定できます。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |
| 7 | パスワード内の数字が必要な最小の文字数 | パスワードに必要な数字の最小の文字数を設定できます。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |
| 8 | パスワード内の特殊記号が必要な最小の文字数 | パスワードに必要な特殊記号の最小の文字数を設定できます。<br>「パスワードの複雑さ」が「3」（アルファベット、数字および特殊記号が必要なパスワード）の場合に有効です。<br>初期値は「-」（制限なし）です。設定できる値は「-」（制限なし）と 1～4 です。 |

| 項番 | 設定できる項目 | 説明 |
|---|---|---|
| 9 | パスワード有効期限切れまでのタイムアウト値 | パスワードの変更が必要となる経過日数を設定できます。「0」を指定した場合、機能が無効となります。<br>初期値は「0」（無効）です。設定できる値は 0～730（日）です。 |
| 10 | パスワード履歴制限 | 指定回数前までのパスワードの再利用を禁止できます。「0」を指定した場合、機能が無効となります。<br>初期値は「0」（無効）です。設定できる値は 0～50 です。 |
| 11 | パスワード失敗時の最大試行回数 | パスワードの入力失敗時の最大試行回数を設定できます。「0」を指定した場合、機能が無効となります。<br>初期値は「0」（無効）です。設定できる値は 0、4～10 です。 |
| 12 | 非アクティブ時間ロックの最大値 | Android 端末が自動的にロックされるまでのアイドル時間を設定できます。「0」を指定した場合、機能が無効となります。<br>初期値は「0」（無効）です。設定できる値は 0、1～5、10、15（分）です。 |
| 13 | ストレージ暗号化の要求 | 内部ストレージに対して暗号化するかどうかを設定できます。<br>この機能は、Android 端末がストレージ暗号化をサポートしている場合にチェックすることで利用できるようになります。<br>初期値は「チェックなし」（無効）です。設定できる値は、「チェックあり」（有効）または「チェックなし」（無効）です。 |
| 14 | サーバ接続失敗時のタイムアウト値 | JP1/ITDM2 - SDM と接続できない状態が続いた場合に、Android 端末を初期化するまでの最大時間を設定できます。「OFF」を指定した場合、この機能は無効となります。<br>初期値は「OFF」です。設定できる値は OFF または ON、1～60（分）です。 |
| 15 | カメラの利用禁止 | カメラの利用を禁止できます。<br>初期値は「チェックなし」（カメラの利用可）です。設定できる値は「チェックあり」（カメラの利用禁止）または「チェックなし」（カメラの利用可）です。 |

**重要**

パスワードのルールについては、ルール適用後、次回パスワード変更時に有効となります。

**関連項目**

- 2.4.4 Android ポリシーの管理
- 14.4.11 ［Android ポリシー一覧］画面

## 2.4.6 iOS プロファイルの管理

セキュリティ画面の［iOS プロファイル一覧］画面で、iOS プロファイルを管理できます。

iOS プロファイルを登録する

組織のセキュリティ方針を基に、Apple 社が提供する iPhone 構成ユーティリティで構成プロファイルを作成し、iOS プロファイルとして登録します。iOS プロファイルは複数登録できます。

iOS プロファイル情報を編集する

iOS プロファイル名や説明を編集します。

iOS プロファイルをエクスポートする

組織のセキュリティ方針が変更となった場合や、新たに別の環境を構築する必要が生じた場合に、iOS プロファイルを XML 形式でエクスポートします。エクスポートしたファイルは、拡張子を.mobileconfig に変更すると、Apple 社が提供する iPhone 構成ユーティリティにインポートできます。必要に応じて構成プロファイルを編集してから、iOS プロファイルに再度登録します。

iOS プロファイルを削除する

管理体制の変更や iOS プロファイルの統合に伴って、不要になった iOS プロファイルを削除します。

**関連項目**

- 2.4.7 iOS プロファイルに設定できる項目について
- 7.3 iOS プロファイルを利用する

## 2.4.7 iOS プロファイルに設定できる項目について

iOS プロファイルに設定できる項目は、iPhone 構成ユーティリティで作成できる構成プロファイルの項目です。

iPhone 構成ユーティリティで作成できる構成プロファイルの項目は、Apple 社のホームページなどで確認してください。

**関連項目**

- 2.4.6 iOS プロファイルの管理

## 2.5　スマートデバイスの管理

スマートデバイスの情報を登録して、最新の情報を一覧で確認できます。また、スマートデバイスにセキュリティのルールを適用したり、ロックや初期化などの遠隔操作をしたりできます。

### 2.5.1　管理対象のスマートデバイスの管理

スマートデバイス画面の［管理対象のスマートデバイス一覧］画面では、管理対象のスマートデバイスの一覧が表示されます。この画面から、スマートデバイスの登録やセキュリティのルールの適用、またロックや初期化などの遠隔操作ができます。

#### スマートデバイスの情報の確認

メニューエリアで［Android スマートデバイス］や［iOS スマートデバイス］を選択すると、OS ごとのスマートデバイスの一覧を確認できます。

一覧でスマートデバイスを選択すると、インフォメーションエリア下部に詳細情報がタブごとに表示されます。各タブで確認できる情報を次に示します。

| タブ名 | 説明 |
|---|---|
| ［イベント］タブ | スマートデバイスで発生したイベントを一覧で確認できます。イベントを確認済みにしたり、未確認にしたりできます。 |
| ［通話履歴］タブ | スマートデバイスの通話履歴を一覧で確認できます。履歴を確認済みにしたり、未確認にしたりできます。また、履歴にある電話番号を、利用を許可する電話番号としてセキュリティポリシーに追加できます。 |
| ［WEB 閲覧履歴］タブ | スマートデバイスの Web 閲覧履歴を一覧で確認できます。履歴を確認済みにしたり、未確認にしたりできます。また、履歴にある Web サイトを、許可または禁止する Web サイトとしてセキュリティポリシーに追加できます。 |
| ［ソフトウェア］タブ | スマートデバイスに配布またはインストールされているソフトウェア（アプリケーション）を一覧で確認できます。一覧にあるソフトウェアを確認済みにしたり、未確認にしたりできます。また、一覧にあるソフトウェアを、許可または禁止するアプリケーションとしてセキュリティポリシーに追加できます。 |
| ［ハードウェア］タブ | スマートデバイスのシリアル番号や内部ストレージ容量などのハードウェア情報を確認できます。 |
| ［起動中アプリケーション］タブ | スマートデバイスで起動中のアプリケーションを一覧で確認できます。 |
| ［動作中サービス］タブ | スマートデバイスで動作中のサービスを一覧で確認できます。 |
| ［システム情報］タブ | スマートデバイスの OS 情報や電話番号などのシステム情報を確認できます。 |

| タブ名 | 説明 |
| --- | --- |
| ［セキュリティ］タブ | スマートデバイスに適用されているセキュリティポリシーや、Android ポリシーまたは iOS プロファイル、GPS 電源状態、最後にスマートデバイスをロックした日時などの情報を確認できます。 |
| ［Bluetooth 接続情報］タブ | スマートデバイスの Bluetooth 通信を用いた接続履歴を確認できます。履歴を確認済みにしたり、未確認にしたりできます。 |

### スマートデバイスの情報の登録

名称や OS 種別、セキュリティのルールなどのスマートデバイスの情報を登録できます。登録したいスマートデバイスの情報を CSV ファイルで作成しておくと、ファイルをインポートすることでスマートデバイスの情報を一括で登録できます。登録したスマートデバイスの情報を CSV ファイルでエクスポートすることもできます。

### スマートデバイスに対する操作

スマートデバイスに対して次の操作が実行できます。

- 最新の情報を取得する（スマートデバイスから最新のインベントリ情報を取得する）
- 初期化する（工場出荷状態にする）
- スマートデバイスをロックする
- Android 端末のパスワードを変更する
- iOS 端末のパスコードをリセットする
- Android 端末にメッセージを通知する
- 管理対象外にする
- セキュリティポリシーを適用する
- Android ポリシーを適用する
- iOS プロファイルを適用する
- iOS プロファイルの適用を解除する

### 関連項目

- 2.5.2 管理対象外のスマートデバイスの管理
- 8. スマートデバイスを管理する
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 2.5.2 管理対象外のスマートデバイスの管理

スマートデバイス画面の［管理対象外のスマートデバイス一覧］画面では、管理対象外のスマートデバイスの一覧が表示されます。この画面から、セキュリティのルールを適用できます。

### スマートデバイスの情報の確認

一覧でスマートデバイスを選択すると、インフォメーションエリア下部に詳細情報がタブごとに表示されます。各タブで確認できる情報を次に示します。

| タブ名 | 説明 |
|---|---|
| ［イベント］タブ | スマートデバイスで発生したイベントを一覧で表示できます。イベントを確認済みにしたり、未確認にしたりできます。 |
| ［システム情報］タブ | スマートデバイスの OS 情報や電話番号などのシステム情報を確認できます。 |

### スマートデバイスに対する操作

スマートデバイスに対して、次の操作が実行できます。

- セキュリティポリシーを適用する
- Android ポリシーを適用する
- iOS プロファイルを適用する

### 関連項目

- 2.5.1 管理対象のスマートデバイスの管理
- 8. スマートデバイスを管理する
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 2.6　アプリケーションの管理

スマートデバイスに配布するアプリケーションを管理できます。

### 2.6.1　配布アプリケーションの管理

登録されているアプリケーションを一覧で確認し、アプリケーションの編集や削除ができます。

配布画面の［配布アプリケーション一覧］画面では、管理者が登録したアプリケーションの情報およびスマートデバイスへの配布状態のサマリが一覧で確認できます。また、アプリケーションの編集および削除ができます。

一覧でアプリケーションを選択すると、インフォメーションエリア下部のノートにアプリケーションの説明を入力できます。

**関連項目**

- 2.6.2 配布するアプリケーションについて
- 2.6.3 Android アプリケーションの管理
- 2.6.4 iOS アプリケーションの管理
- 9. アプリケーションを管理する
- 14.6.1 ［配布アプリケーション一覧］画面

### 2.6.2　配布するアプリケーションについて

配布するアプリケーションは、運用に応じて 2 種類の方法で配布できます。

- 管理者がインストールの指示を出して、スマートデバイスにアプリケーションをインストールする（Push 配布）
- 管理者が、利用者の操作でインストールできるアプリケーションを用意しておき、利用者が必要なアプリケーションだけをダウンロードしてインストールする（Pull 配布）

配布できるアプリケーションの最大サイズは、次のとおりです。

| OS | アプリケーションの最大サイズ |
|---|---|
| Android | 100MB |
| iOS | 2GB |

**メモ**

アプリケーションを配布する場合、配布するアプリケーションを通信サーバに手動で配置します（標準配布）。ただし、通信サーバに手動でアプリケーションを配置しない方式（簡易配布）も利用できます。簡易配布の場合、配布できるアプリケーションの最大サイズは、Android の場合 5MB、iOS の場合 50MB です。また、簡易配布では、Pull 配布はできません。

なお、簡易配布をするには、スマートデバイスマネージャーの環境設定ファイルを変更する必要があります。

**関連項目**

- 16.2 スマートデバイスマネージャー環境設定ファイル（manager.properties）

## 2.6.3 Android アプリケーションの管理

登録されている Android アプリケーションを一覧で確認し、Android アプリケーションの登録、編集、および削除ができます。また、配布、インストールの指示およびアンインストールの指示ができます。

配布画面の［Android アプリケーション］画面では、Android アプリケーションの一覧および Android 端末への配布状態のサマリが表示されます。この画面から、Android アプリケーションの登録、登録した情報の編集、および削除ができます。登録した Android アプリケーションについては、配布、配布したアプリケーションの削除、インストールの指示、およびアンインストールの指示ができます。

一覧で Android アプリケーションを選択すると、インフォメーションエリア下部に配布状態ごとのスマートデバイス一覧がタブで表示されます。各タブで確認できる情報および実行できる操作を次に示します。

| タブ名 | 説明 |
|---|---|
| ［未配布スマートデバイス一覧］タブ | Android アプリケーションを配布していないスマートデバイスを一覧で確認できます。表示されているスマートデバイスに対して、Android アプリケーションの配布やインストールの指示を実行できます。 |
| ［配布済みスマートデバイス一覧］タブ | Android アプリケーションを配布したスマートデバイスを一覧で確認できます。表示されているスマートデバイスに対して、Android アプリケーションのインストールの指示や Android アプリケーションの削除を実行できます。 |
| ［インストール済みスマートデバイス一覧］タブ | Android アプリケーションをインストールしたスマートデバイスを一覧で確認できます。表示されているスマートデバイスに対して、Android アプリケーションのアンインストールの指示および Android アプリケーションの削除を実行できます。 |

**重要**

JP1/ITDM2 - SDM で管理できる Android アプリケーションは、拡張子が.apk のファイルだけです。

**関連項目**

- 9. アプリケーションを管理する
- 14.6.2 ［Android アプリケーション］画面

## 2.6.4 iOS アプリケーションの管理

登録されている iOS アプリケーションを一覧で確認し、iOS アプリケーションの登録、編集、および削除ができます。また、インストールの指示およびアンインストールの指示ができます。

配布画面の［iOS アプリケーション］画面では、iOS アプリケーションの一覧および iOS 端末への配布状態のサマリが表示されます。この画面から、iOS アプリケーションの登録、登録した情報の編集、および削除ができます。登録した iOS アプリケーションについては、インストールの指示およびアンインストールの指示ができます。

一覧で iOS アプリケーションを選択すると、インフォメーションエリア下部に配布状態ごとのスマートデバイス一覧がタブで表示されます。各タブで確認できる情報および実行できる操作を次に示します。

| タブ名 | 説明 |
|---|---|
| ［未インストールスマートデバイス一覧］タブ | iOS アプリケーションを配布していないスマートデバイスを一覧で確認できます。表示されているスマートデバイスに対して、iOS アプリケーションの配布とインストールの指示を実行できます。 |
| ［インストール済みスマートデバイス一覧］タブ | iOS アプリケーションをインストールしたスマートデバイスを一覧で確認できます。表示されているスマートデバイスに対して、iOS アプリケーションのアンインストールの指示と iOS アプリケーションの削除を実行できます。 |

**重要**

JP1/ITDM2 - SDM で管理できる iOS アプリケーションは、拡張子が.ipa のファイルだけです。

iOS アプリケーション（In House: 企業内利用向け）を配布する場合、iOS アプリケーションは Apple Developer Enterprise Program ライセンスが定める範囲で利用してください。

**関連項目**

- 9. アプリケーションを管理する

- 14.6.4 ［iOS アプリケーション］画面

## 2.7　イベントの表示

JP1/ITDM2 - SDM の運用中に、早急な対処が必要な事象が発生した場合、その事象がイベントとして出力されます。また、各種機能の処理結果なども出力されます。管理者は、これらのイベントを確認することで運用中に発生した事象を把握できます。

### 2.7.1　出力されるイベント

出力されるイベントは重大度で 3 種類に分けられます。イベントを定期的に確認して、問題がある場合は対処してください。

イベントは、その内容によって次の 3 種類の重大度に分けられます。

（緊急）

すぐに対策が必要なイベントです。イベントの内容を確認して早急に対策してください。

（警戒）

すぐに対策する必要はありませんが、対策が必要なイベントです。イベントの内容を確認して、必要に応じて対策してください。

（情報）

システムの処理結果に関するイベントです。対策は不要です。

イベントの内容によっては早急に対処が必要な場合があります。重大度が「緊急」、「警戒」の優先順位でイベントを確認し、エラーの内容から原因を特定して対処してください。

**ヒント**

イベントが発生したら管理者にメールで通知するように設定できます。

**関連項目**

- 2.7.2 イベントの種類
- 2.7.3 イベントの形式
- 11.1 イベント通知の設定をする手順
- 11.2 メールサーバを設定する手順
- 14.7 イベント画面

### 2.7.2　イベントの種類

出力されるイベントの種類について説明します。

### イベントの種類

| 項番 | イベントの種類 | 説明 |
|---|---|---|
| 1 | セキュリティ | セキュリティポリシーの変更と適用、セキュリティポリシーの判定結果など、セキュリティ管理に関するイベントです。 |
| 2 | スマートデバイス | スマートデバイスの情報の追加と削除など、スマートデバイスの管理に関するイベントです。 |
| 3 | 配布 | スマートデバイスへのアプリケーションの配布やインストール結果など、配布に関するイベントです。 |
| 4 | 設定 | ユーザーアカウントの管理や、イベントが発生した際のメール通知など、設定に関するイベントです。 |
| 5 | 不審操作 | ユーザーがセキュリティポリシーで禁止されているアプリケーションを使用した、セキュリティポリシーで禁止されている通話先に電話したなどの、不審操作に関するイベントです。 |
| 6 | エラー | 各機能で発生したエラーに関するイベントです。 |

### 関連項目

- 2.7.1 出力されるイベント
- 2.7.3 イベントの形式

## 2.7.3　イベントの形式

出力されるイベントの形式について説明します。

### イベントの形式

| 項番 | 項目 | 説明 |
|---|---|---|
| 1 | 確認状態 | イベントの確認状態です。クリックすると状態が切り替わります。<br>• 未確認<br>• 確認済み |
| 2 | 重大度 | イベントの重大度です。次のどれかが表示されます。<br>• 緊急<br>• 警戒<br>• 情報 |
| 3 | 登録日時 | スマートデバイスマネージャーにイベントが登録された日時が表示されます。 |
| 4 | 種類 | イベントの種類です。次のどれかが表示されます。<br>• セキュリティ<br>• スマートデバイス<br>• 配布<br>• 設定 |

| 項番 | 項目 | 説明 |
|---|---|---|
| 4 | 種類 | • 不審操作<br>• エラー |
| 5 | イベント番号 | イベントの内容に応じた識別番号が表示されます。 |
| 6 | 発生元 | スマートデバイスやセキュリティポリシーなど、イベントの対象を特定する情報です。次のどれかが表示されます。発生元をクリックすると、リンク先の画面に遷移します。<br>• スマートデバイス名称（リンク先：[管理対象のスマートデバイス一覧]画面または［管理対象外のスマートデバイス一覧］画面）<br>• セキュリティ（リンク先：[セキュリティポリシー一覧］画面）<br>• 配布（リンク先：[配布アプリケーション一覧］画面）<br>• 設定（リンク先：設定画面） |
| 7 | 内容 | イベントの詳細情報が表示されます。 |

**関連項目**

- 2.7.1 出力されるイベント
- 2.7.2 イベントの種類

# 3 システムの構築

ここでは、JP1/ITDM2 - SDM のコンポーネントのインストール、SSL 通信用証明書の設定、スマートデバイスへの JP1/ITDM2 - SDM（スマートデバイスエージェント）の導入などについて説明します。

## 3.1　システムを構築する流れ

システムを構築するには、JP1/ITDM2 - SDM を構築したあとで、管理対象とするスマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入します。

JP1/ITDM2 - SDM を使用するには、スマートデバイスマネージャー、通信サーバ、およびメッセージングサーバの 3 つを構築し、スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入します。ここでは、基本的な構成であるイントラネット環境にスマートデバイスマネージャーを、DMZ 環境に通信サーバおよびメッセージングサーバを構築する流れについて記載します。

1. イントラネット環境のホストに JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする

   JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールしたホストがスマートデバイスマネージャーとなります。

2. JP1/ITDM2 - SDM（通信サーバ）をインストールする

   JP1/ITDM2 - SDM（通信サーバ）をインストールしたホストが通信サーバとなります。

3. JP1/ITDM2 - SDM（メッセージングサーバ）をインストールする

   JP1/ITDM2 - SDM（メッセージングサーバ）をインストールしたホストがメッセージングサーバとなります。

4. ルータのポート開放設定および各サーバのファイアウォールを設定する
5. SSL 通信用証明書を取得する
6. スマートデバイスマネージャーに SSL 通信用証明書を設定する
7. 通信サーバに SSL 通信用証明書を設定する
8. 操作画面にログインしてユーザーアカウントの情報を設定する
9. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する

> **重要**
>
> iOS 端末を管理する場合、次の条件を満たす必要があります。詳細は、Apple 社の情報を参照してください。
>
> - Apple Developer Enterprise Program ライセンスの取得

**関連項目**

- 3.5 JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする手順
- 3.6 JP1/ITDM2 - SDM（通信サーバ）をインストールする手順
- 3.7 JP1/ITDM2 - SDM（メッセージングサーバ）をインストールする手順
- 3.8 ルータのポート開放および各サーバのファイアウォールの設定について
- 3.11 SSL 通信用証明書の取得

- 3.12 スマートデバイスマネージャーでの SSL 通信用証明書の設定
- 3.13 通信サーバでの SSL 通信用証明書の設定
- 3.14 スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ
- 5.1 ログインする手順
- 5.2 ユーザーアカウント情報を設定する手順

## 3.2 前提 OS

JP1/ITDM2 - SDM の前提 OS について説明します。

| 対象 | 前提 OS |
|---|---|
| スマートデバイスマネージャー（JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールするホスト） | Windows Server 2008 R2 |
| | Windows Server 2012 |
| | Windows Server 2012 R2 |
| | Windows Server 2016 |
| 通信サーバ（JP1/ITDM2 - SDM（通信サーバ）をインストールするホスト） | Windows Server 2008 R2 |
| | Windows Server 2012 |
| | Windows Server 2012 R2 |
| | Windows Server 2016 |
| メッセージングサーバ（JP1/ITDM2 - SDM（メッセージングサーバ）をインストールするホスト） | Windows Server 2008 R2 |
| | Windows Server 2012 |
| | Windows Server 2012 R2 |
| | Windows Server 2016 |
| JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールするスマートデバイス | Android 4.1 |
| | Android 4.3 |
| | Android 5.0 |
| | Android 6.0 |
| | iOS 7.1 |
| | iOS 8.1 |
| | iOS 8.3 |
| | iOS 8.4 |
| | iOS 9.1 |
| | iOS 9.2 |
| | iOS 9.3 |
| | iOS 10.0 |
| | iOS 10.1 |
| | iOS 10.2 |

## 3.3 前提プログラム

JP1/ITDM2 - SDM の前提プログラムについて説明します。

- Internet Explorer 8 以降
- Firefox 24 以降

## 3.4 JP1/ITDM2 - SDM を構成するコンポーネント

JP1/ITDM2 - SDM を構成するコンポーネントについて説明します。

JP1/ITDM2 - SDM（スマートデバイスマネージャー）

イントラネット内のホストにインストールします。JP1/ITDM2 - SDM（スマートデバイスマネージャー）がインストールされたホストをスマートデバイスマネージャーと呼びます。

JP1/ITDM2 - SDM（通信サーバ）

DMZ 内のグローバル IP アドレスを持つホストにインストールします。JP1/ITDM2 - SDM（通信サーバ）がインストールされたホストを通信サーバと呼びます。

JP1/ITDM2 - SDM（メッセージングサーバ）

DMZ 内のグローバル IP アドレスを持つホストにインストールします。通信サーバと同一のホストにインストールすることもできます。JP1/ITDM2 - SDM（メッセージングサーバ）がインストールされたホストをメッセージングサーバと呼びます。

JP1/ITDM2 - SDM（スマートデバイス Android エージェント）

Android 端末にインストールする、エージェント機能を提供するプログラムです。

JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）

iOS 端末にインストールする、エージェント機能を提供するプログラムです。

**関連項目**

- 3.5 JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする手順
- 3.6 JP1/ITDM2 - SDM（通信サーバ）をインストールする手順
- 3.7 JP1/ITDM2 - SDM（メッセージングサーバ）をインストールする手順
- 3.14 スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ

## 3.5 JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする手順

イントラネット環境のホストに JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールします。JP1/ITDM2 - SDM（スマートデバイスマネージャー）がインストールされたホストをスマートデバイスマネージャーと呼びます。

**前提条件**

Administrator 権限を持つユーザーで OS にログオンしている必要があります。

**操作手順**

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Smart Device Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。
   使用許諾契約の条項に同意しない場合、［キャンセル］を選択すると、JP1/ITDM2 - SDM のインストール中断ダイアログが表示されます。
   - インストールを中断するときは、［はい］ボタンをクリックして終了します。
   - インストールを継続するときは、［いいえ］ボタンをクリックします。
5. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。
6. ［サーバ選択］ダイアログで、［スマートデバイスマネージャー］を選択して［次へ］ボタンをクリックします。
7. ［インストールタイプ］ダイアログで、インストールタイプを選択して［次へ］ボタンをクリックします。
   簡単インストールを選択した場合は、手順 9 へ進んでください。
8. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。

> **重要**
>
> インストール先のフォルダは、ドライブで始まり、次の要素で構成される文字列で指定してください。また、パス名の長さを末尾の¥を含めて 42 文字（バイト）以内にしてください。
>
> 英数字、「_」（アンダーバー）、「.」（ピリオド）、空白文字、「(」（左括弧）、「)」（右括弧）、パス区切りの「¥」

9. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、[インストール] ボタンをクリックします。

   インストールが実行されます。インストール内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。

10. インストールが完了したら、[完了] ボタンをクリックします。

    JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストールが完了します。ログオフを要求するメッセージが表示されますので、いったんログオフしてください。

11. スマートデバイスマネージャーの環境設定ファイルを設定します。

12. スマートデバイスマネージャーのサービス「JP1/ITDM2 - Smart Device Manager Server Service」を再起動します。

**関連項目**

- 3.1 システムを構築する流れ
- 16.2 スマートデバイスマネージャー環境設定ファイル（manager.properties）

## 3.6 JP1/ITDM2 - SDM（通信サーバ）をインストールする手順

JP1/ITDM2 - SDM（通信サーバ）をインストールします。JP1/ITDM2 - SDM（通信サーバ）がインストールされたホストを通信サーバと呼びます。

**前提条件**

- DMZ 内のグローバル IP アドレスを持つホストにインストールします。
- Administrator 権限を持つユーザーで OS にログオンしている必要があります。

**操作手順**

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Smart Device Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。

   使用許諾契約の条項に同意しない場合、［キャンセル］を選択すると、JP1/ITDM2 - SDM のインストール中断ダイアログが表示されます。

   - インストールを中断するときは、［はい］ボタンをクリックして終了します。
   - インストールを継続するときは、［いいえ］ボタンをクリックします。
5. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。
6. ［サーバ選択］ダイアログで、［通信サーバ］を選択して［次へ］ボタンをクリックします。
7. ［データベースの接続先］ダイアログで、IP アドレスまたはドメイン名を指定して［次へ］ボタンをクリックします。

   **ヒント**

   データベース接続先アドレスは、sdmnetchange コマンドで変更できます。
8. ［インストールタイプ］ダイアログで、インストールタイプを選択して［次へ］ボタンをクリックします。

   簡単インストールを選択した場合は、手順 10 へ進んでください。
9. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。

**重要**

インストール先のフォルダは、ドライブで始まり、次の要素で構成される文字列で指定してください。また、パス名の長さを末尾の¥を含めて 42 文字（バイト）以内にしてください。

英数字、「_」（アンダーバー）、「.」（ピリオド）、空白文字、「(」（左括弧）、「)」（右括弧）、パス区切りの「¥」

10. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、［インストール］ボタンをクリックします。

インストールが実行されます。インストール内容に問題がある場合は、［戻る］ボタンをクリックして設定を修正してください。

11. インストールが完了したら、［完了］ボタンをクリックします。

JP1/ITDM2 - SDM（通信サーバ）のインストールが完了します。ログオフを要求するメッセージが表示されますので、いったんログオフしてください。

12. 通信サーバの動作環境を変更する場合、通信サーバの環境設定ファイルを変更します。

13. 環境設定ファイルを変更した場合、通信サーバのサービス「JP1/ITDM2 - Smart Device Manager (Communication Server Service)」を再起動します。

**メモ**

JP1/ITDM2 - SDM（通信サーバ） 11-10 より前のバージョンからバージョンアップインストールするとき、httpsd.conf ファイルの編集が必要です。

**関連項目**

- 3.1 システムを構築する流れ
- 3.19.1 通信サーバをバージョンアップインストールするときの作業
- 15. sdmnetchange（スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更）
- 16.6 通信サーバ環境設定ファイル（CommunicationServerEngine.properties）

## 3.7 JP1/ITDM2 - SDM（メッセージングサーバ）をインストールする手順

JP1/ITDM2 - SDM（メッセージングサーバ）をインストールします。JP1/ITDM2 - SDM（メッセージングサーバ）がインストールされたホストをメッセージングサーバと呼びます。

**前提条件**

- DMZ 内のグローバル IP アドレスを持つホストにインストールします。
- Administrator 権限を持つユーザーで OS にログオンしている必要があります。

**操作手順**

1. 提供媒体を CD/DVD ドライブにセットします。
2. 表示される［日立総合インストーラ］ダイアログで、［JP1/IT Desktop Management 2 - Smart Device Manager］を選択して、［インストール実行］ボタンをクリックします。
3. インストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［使用許諾契約］ダイアログで、内容を確認してから［使用許諾契約の条項に同意します］を選択し、［次へ］ボタンをクリックします。

   使用許諾契約の条項に同意しない場合、［キャンセル］を選択すると、JP1/ITDM2 - SDM のインストール中断ダイアログが表示されます。

   - インストールを中断するときは、［はい］ボタンをクリックして終了します。
   - インストールを継続するときは、［いいえ］ボタンをクリックします。
5. ［ユーザー登録］ダイアログで、ユーザー名と会社名を入力して［次へ］ボタンをクリックします。
6. ［サーバ選択］ダイアログで、［メッセージングサーバ］を選択して［次へ］ボタンをクリックします。
7. ［インストールタイプ］ダイアログで、インストールタイプを選択して［次へ］ボタンをクリックします。

   簡単インストールを選択した場合は、手順 9 へ進んでください。
8. ［インストール先のフォルダ］ダイアログで、インストール先のフォルダを指定して［次へ］ボタンをクリックします。

   **重要**

   インストール先のフォルダは、ドライブで始まり、次の要素で構成される文字列で指定してください。また、パス名の長さを末尾の¥を含めて 42 文字（バイト）以内にしてください。

   英数字、「_」（アンダーバー）、「.」（ピリオド）、空白文字、「(」（左括弧）、「)」（右括弧）、パス区切りの「¥」
9. インストール内容を確認するダイアログで、インストール内容に問題がないことを確認し、［インストール］ボタンをクリックします。

インストールが実行されます。インストール内容に問題がある場合は、[戻る] ボタンをクリックして設定を修正してください。

10. インストールが完了したら、[完了] ボタンをクリックします。
    JP1/ITDM2 - SDM（メッセージングサーバ）のインストールが完了します。ログオフを要求するメッセージが表示されますので、いったんログオフしてください。

11. メッセージングサーバの動作環境を変更する場合、メッセージングサーバの環境設定ファイルを変更します。

12. 環境設定ファイルを変更した場合、メッセージングサーバのサービス「JP1/ITDM2 - Smart Device Manager (Messaging Server Service)」を再起動します。

**関連項目**

- 3.1 システムを構築する流れ
- 16.7 メッセージングサーバ設定ファイル（SdMessagingServer.ini）

# 3.8　ルータのポート開放および各サーバのファイアウォールの設定について

ルータのポート開放および各サーバのファイアウォールの設定が必要です。

使用するポート番号と接続方向を次に示します。

| ポート番号 | 接続方向 | | | | | |
|---|---|---|---|---|---|---|
| | インターネット→DMZ | インターネット←DMZ | DMZ→イントラネット | DMZ←イントラネット | イントラネット←インターネット | イントラネット→インターネット |
| 26080/tcp | − | − | − | − | ○ | − |
| 26055/tcp | ○ | − | − | ○ | − | − |
| 2195/tcp | − | ○ | − | − | − | − |
| 80/tcp | − | ○ | − | − | − | − |
| 26079/tcp | ○ | − | − | − | − | − |
| 26067/tcp | − | − | ○ | − | − | − |
| 26068-26077/tcp | − | − | − | ○ | − | − |
| 5223/tcp | − | − | − | − | − | ○ |

（凡例）

○：該当する接続方向

−：該当しない接続方向

各ポート番号について説明します。

- 26080：管理画面用ポートです。
- 26055：HTTPS 通信用ポートです。
- 2195：APNs サーバとの通信用ポートです。iOS 端末を管理する場合だけ必要です。
- 80：HTTP 通信用ポートです。iOS 端末を管理する場合だけ必要です。
- 26079：Android 端末とメッセージングサーバとの HTTP 通信用ポートです。
- 26067：通信サーバとスマートデバイスマネージャー内の DB との通信用ポート（DB 受信ポート）です。
- 26068-26077：通信サーバとスマートデバイスマネージャー内の DB との通信用ポート（通信サーバ受信ポート）です。
- 5223：iOS 端末と APNs サーバとの通信用ポートです。Wifi 接続されている iOS 端末を管理する場合だけ必要です。

### 関連項目

- 3.1 システムを構築する流れ
- 付録 C ポート番号一覧

# 3.9 SSL 通信用証明書の種類

JP1/ITDM2 - SDM で SSL 通信をするために必要な SSL 通信用証明書の種類について説明します。

### JP1/ITDM2 - SDM で必要な SSL 通信用証明書

- 通信サーバの SSL 通信用証明書
  次に示す証明書を証明書発行機関から取得します。
  - SSL 通信用ルート証明書
  - SSL 通信用サーバ証明書
- スマートデバイスマネージャーの SSL 通信用証明書
  次に示す証明書を証明書発行機関から取得します。
  - SSL 通信用ルート証明書
  - SSL 通信用サーバ証明書
- APNs サーバの SSL 通信用証明書（iOS 端末を管理する場合）
  iOS 端末を管理する場合は、次に示す証明書が必要です。
  - SSL 通信用ルート証明書
  - SSL 通信用クライアント証明書（MDM 用）
    ファイル名は「APNsMDMPushDev.p12」で PKCS#12 形式です。

    **重要**

    この証明書は 1 年ごとに更新する必要があります。

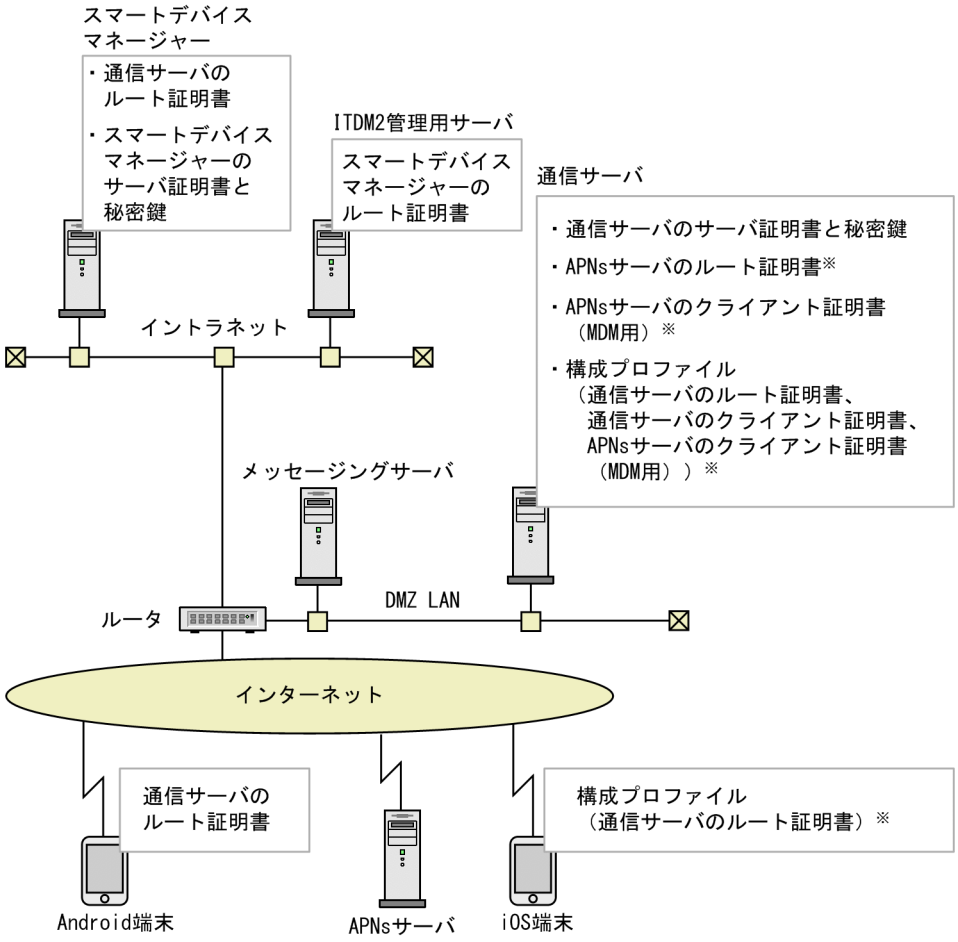
### 関連項目

- 3.11 SSL 通信用証明書の取得
- 3.12 スマートデバイスマネージャーでの SSL 通信用証明書の設定
- 3.13 通信サーバでの SSL 通信用証明書の設定
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順

## 3.10 SSL 通信用証明書の配置

JP1/ITDM2 - SDM で SSL 通信をするためには、SSL 通信用証明書を所定のサーバまたはスマートデバイスに配置する必要があります。

SSL 通信用証明書の配置場所を次の図に示します。




注※　iOS端末を管理する場合に必要です。

## 3.11　SSL 通信用証明書の取得

管理するスマートデバイスの OS によって、取得する SSL 通信用証明書が異なります。

SSL 通信用証明書の取得に関する作業と、その必要性を次に示します。

| 項番 | 作業 | | 必要性 |
|---|---|---|---|
| 1 | 通信サーバの SSL 通信用証明書の取得 | | 必須 |
| 2 | スマートデバイスマネージャーの SSL 通信用証明書の取得 | | 必須 |
| 3 | APNs サーバの SSL 通信用ルート証明書の取得 | | iOS 端末を管理する場合だけ |
| 4 | APNs サーバの SSL 通信用クライアント証明書（MDM 用）の取得 | MDM 用証明書要求ファイルのダウンロード | iOS 端末を管理する場合だけ |
| | | MDM 用署名済み証明書要求ファイルの作成 | |
| | | MDM 用クライアント証明書の作成 | |

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ
- 3.11.2 スマートデバイスマネージャーの SSL 通信用証明書を取得する流れ
- 3.11.3 APNs サーバの SSL 通信用ルート証明書を取得する手順（iOS 端末を管理する場合）
- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）
- 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）

## 3.11.1　通信サーバの SSL 通信用証明書を取得する流れ

通信サーバの SSL 通信用証明書（SSL 通信用ルート証明書および SSL 通信用サーバ証明書）は、証明書発行機関から取得します。

通信サーバの SSL 通信用証明書を取得するまでの流れを次に示します。

1. Web サーバの秘密鍵を作成する（keygen コマンド）
   作成した Web サーバの秘密鍵のファイルは、SSLCertificateKeyFile ディレクティブに指定します。
2. 証明書発行要求（CSR）を作成する（certutil reqgen コマンド）

3. 証明書発行要求（CSR）の内容を表示する（certutil req コマンド）
   必要に応じて証明書発行要求（CSR）の内容を確認します。
4. 証明書発行要求（CSR）を認証局（CA）に提出する
5. 認証局（CA）から署名済みの証明書を取得する

> **ヒント**
>
> 取得した証明書の内容はcertutil cert コマンドで確認できます。

> **ヒント**
>
> 取得した証明書の"-----BEGINCERTIFICATE-----"から、"-----END CERTIFICATE----"の部分を別ファイルに保存します（標準提供の httpsd.conf では httpsd.pem）。このファイルを SSLCertificateFile ディレクティブに定義することで、SSL が利用できるようになります。

**関連項目**

- 3.12.1 スマートデバイスマネージャーで通信サーバの SSL 通信用ルート証明書を設定する手順
- 3.13.2 通信サーバで SSL 通信用サーバ証明書を設定する手順
- 付録 G.1 Web サーバの秘密鍵の作成（keygen）
- 付録 G.2 証明書発行要求（CSR）の作成（certutil reqgen）
- 付録 G.3 証明書発行要求（CSR）の内容表示（certutil req）
- 付録 G.4 証明書の内容表示（certutil cert）
- 付録 G.5 証明書の形式変換（certutil cert）

## 3.11.2 スマートデバイスマネージャーの SSL 通信用証明書を取得する流れ

スマートデバイスマネージャーの SSL 通信用証明書（SSL 通信用ルート証明書および SSL 通信用サーバ証明書）は、証明書発行機関から取得します。

スマートデバイスマネージャーの SSL 通信用証明書を取得するまでの流れを次に示します。

1. Web サーバの秘密鍵を作成する（keygen コマンド）
   作成した Web サーバの秘密鍵のファイルは、SSLCertificateKeyFile ディレクティブに指定します。
2. 証明書発行要求（CSR）を作成する（certutil reqgen コマンド）
3. 証明書発行要求（CSR）の内容を表示する（certutil req コマンド）
   必要に応じて証明書発行要求（CSR）の内容を確認します。
4. 証明書発行要求（CSR）を認証局（CA）に提出する

5. 認証局（CA）から署名済みの証明書を取得する

> **ヒント**
>
> 取得した証明書の内容は`certutil cert` コマンドで確認できます。

> **ヒント**
>
> 取得した証明書の"-----BEGINCERTIFICATE-----"から、"-----END CERTIFICATE----"の部分を別ファイルに保存します（標準提供の httpsd.conf では httpsd.pem）。このファイルを SSLCertificateFile ディレクティブに定義することで、SSL が利用できるようになります。

> **重要**
>
> 取得した証明書は、JP1/IT Desktop Management 2 の管理用サーバにも設定する必要があります。

**関連項目**

- 3.12.2 スマートデバイスマネージャーで SSL 通信用サーバ証明書を設定する手順
- 付録 G.1 Web サーバの秘密鍵の作成（keygen）
- 付録 G.2 証明書発行要求（CSR）の作成（certutil reqgen）
- 付録 G.3 証明書発行要求（CSR）の内容表示（certutil req）
- 付録 G.4 証明書の内容表示（certutil cert）
- 付録 G.5 証明書の形式変換（certutil cert）

## 3.11.3 APNs サーバの SSL 通信用ルート証明書を取得する手順（iOS 端末を管理する場合）

APNs サーバでは Entrust のサーバ証明書を使用しているため、Entrust のルート証明書が必要です。APNs サーバの SSL 通信用ルート証明書を Entrust のサイトから取得します。この手順は、iOS 端末を管理する場合だけ実施します。

**操作手順**

1. Entrust のサイトにアクセスします。
2. [Personal Use and Secure Server Installation] を選択し、[Download Certificates] ボタンをクリックします。
3. [Root Certificates] をクリックして、「entrust_2048_ca.cer」をダウンロードします。

**関連項目**

- 3.13.1 通信サーバで APNs サーバの SSL 通信用ルート証明書を設定する手順（iOS 端末を管理する場合）

## 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）

MDM 用クライアント証明書（APNsMDMPushDev.p12）は、iOS Dev Center から取得します。

MDM 用クライアント証明書を取得する流れを次に示します。なお、これらの手順は、iOS 端末を管理する場合だけ実施します。

1. MDM 用証明書要求ファイルをダウンロードする
2. MDM 用署名済み証明書要求ファイルを作成する
3. MDM 用クライアント証明書を作成する

**関連項目**

- 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）
- 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）
- 3.13.3 通信サーバで APNs サーバの SSL 通信用クライアント証明書を設定する手順（iOS 端末を管理する場合）
- 3.13.4 通信サーバで構成プロファイルを作成する手順（iOS 端末を管理する場合）

## 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）

MDM 用署名済み証明書要求ファイルを作成するために、MDM 用証明書要求ファイル（mdm.cer）をダウンロードします。この手順は、iOS 端末を管理する場合だけ実施します。

**前提条件**

- Apple Developer Enterprise Program のライセンスを購入する必要があります。
- Apple 社に連絡し、MDM ベンダーの登録を行う必要があります。
- Mac PC 上で作業する必要があります。

### 操作手順

1. iOS Dev Center にログインし、[iOS Developer Program] から [Certificates, Identifiers & Profiles] をクリックします。
2. [Certificates] をクリックします。
3. [+（Add)] ボタンをクリックします。
4. [Production] から [MDM CSR] を選択し、[Continue] ボタンをクリックします。
5. 証明書要求のアップロードについて説明する画面で、[Continue] ボタンをクリックします。
6. キーチェーンアクセスから CSR（証明書署名要求）を作成します。

   証明書情報として次の事項を設定します。

   [ユーザーのメールアドレス]

   iOS 開発ライセンス登録時のメールアドレスを入力します。

   [通称]

   任意の名称を設定します。

   > **ヒント**
   >
   > 設定した通称は、MDM 用署名済み証明書要求ファイルを作成する際に使用します。

   [要求の処理]

   [ディスクに保存] を選択します。

   [鍵ペア情報を設定]

   チェックします。
7. 作成した CSR（証明書署名要求ファイル）をアップロードします。
8. 作成された MDM 用証明書要求ファイル（mdm.cer）をダウンロードします。

### 次の作業

MDM 用署名済み証明書要求ファイルを作成します。

### 関連項目

- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）

## 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）

MDM 用クライアント証明書を作成するために、MDM 用証明書要求ファイルの形式を変更し、MDM 用署名済み証明書要求ファイルを作成します。この手順は、iOS 端末を管理する場合だけ実施します。

**前提条件**

- Apple Developer Enterprise Program のライセンスを購入する必要があります。
- Apple 社に連絡し、MDM ベンダーの登録を行う必要があります。
- Mac PC 上で作業する必要があります。
- MDM 用証明書要求ファイル（mdm.cer）をダウンロードしておく必要があります。

**操作手順**

1. ダウンロードした MDM 用証明書要求ファイル（mdm.cer）をダブルクリックしてキーチェーンアクセスにインポートし、PKCS#12 形式でエクスポートします。

   ファイル名は「vendor.p12」でエクスポートします。

   > **ヒント**
   >
   > パスワードを設定してエクスポートしてください。ここで設定したパスワードを手順 6 で登録します。

2. Apple 社から次に示すルート証明書および中間証明書を取得します。

   - Apple Inc. Root Certificate（AppleIncRootCertificate.cer）
   - WWDR Certificate（AppleWWDRCA.cer）

   > **重要**
   >
   > ルート証明書および中間証明書の名称は変更されることがあります。詳細は、Apple 社の情報を参照してください。

3. ターミナルから OS 提供の次のコマンドを実行し、cer ファイルを pem フォーマットに変換します。

```
openssl x509 -inform der -in mdm.cer -out mdm.pem
openssl x509 -inform der -in AppleWWDRCA.cer -out intermediate.pem
openssl x509 -inform der -in AppleIncRootCertificate.cer -out root.pem
```

4. ターミナルから次のコマンドを実行し、カスタマー証明書要求を作成します。

   - 秘密鍵の作成

```
openssl genrsa -des3 -out customerPrivateKey.pem 2048
```

   - カスタマー証明書要求の作成

```
openssl req -new -key customerPrivateKey.pem -out customer.csr
```

- カスタマー証明書要求の der ファイルフォーマットへの変換

```
openssl req -inform pem -outform der -in customer.csr -out customer.der
```

5. 作成した次の 5 つのファイルを通信サーバにコピーします。
   - customer.der
   - vendor.p12
   - mdm.pem
   - intermediate.pem
   - root.pem
6. コマンドプロンプトから次のコマンドを実行し、MDM 用署名済み証明書要求ファイルを作成します。

```
sdmcreatemdmcertreq -f "ファイル群の格納フォルダ" -o "MDM用署名済み証明書要求ファイル出力先フォルダ" -a 証明書要求ファイル作成時に設定した通称 -p vendor.p12エクスポート時に設定したパスワード
```

**次の作業**

MDM 用クライアント証明書を作成します。

**関連項目**

- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）
- 15. sdmcreatemdmcertreq（MDM 用署名済み証明書要求ファイルの作成）

## 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）

MDM 用署名済み証明書要求ファイルをアップロードして、MDM 用クライアント証明書を作成します。この手順は、iOS 端末を管理する場合だけ実施します。

**前提条件**

- Apple Developer Enterprise Program のライセンスを購入する必要があります。
- Apple 社に連絡し、MDM ベンダーの登録を行う必要があります。
- MDM 用証明書要求ファイルをダウンロードおよび作成した Mac PC 上で作業する必要があります。

- MDM 用署名済み証明書要求ファイルを作成しておく必要があります。

**操作手順**

1. Apple Push Certificates Portal にログインします。
2. [Create a Certificate] ボタンをクリックします。
3. ライセンス条項に同意するチェックボックスにチェックし、[Accept] ボタンをクリックします。
4. アップロードするファイルに「plist_encoded」を選択し、[Upload] ボタンをクリックします。
   正常にアップロードが成功すると MDM 証明書が作成されます。
5. [Download] ボタンをクリックし、証明書ファイル（mdm_vendor.pem）を取得します。
6. インフォメーションアイコン（Certificate Info）をクリックし、Subject DN の UID を確認します。

> **ヒント**
>
> UID は、iOS 端末にクライアント証明書を配布するために、通信サーバで構成プロファイルを作成する際に必要です。

7. 次のコマンドを実行し、秘密鍵と pem ファイルから「APNsMDMPushDev.p12」を作成します。

```
openssl pkcs12 -export -inkey customerPrivateKey.pem -in mdm_vendor.pem -out
APNsMDMPushDev.p12
```

**関連項目**

- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）
- 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）
- 3.13.4 通信サーバで構成プロファイルを作成する手順（iOS 端末を管理する場合）

## 3.12　スマートデバイスマネージャーでの SSL 通信用証明書の設定

スマートデバイスマネージャーで、通信サーバおよびスマートデバイスマネージャーの SSL 通信用証明書を設定する手順について説明します。

### 3.12.1　スマートデバイスマネージャーで通信サーバの SSL 通信用ルート証明書を設定する手順

スマートデバイスマネージャーに、通信サーバの SSL 通信用ルート証明書を設定します。

**操作手順**

1. 次のコマンドを実行し、ルート証明書をインストールします。

```
"JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥bin¥keytool.exe" -importcert -alias エイリアス名※ -file 証明書のパス -keystore "JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥jre¥lib¥security¥cacerts" -storepass changeit
```

インストールされたルート証明書を確認する場合、次のコマンドを実行します。

```
"JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥bin¥keytool.exe" -list -v -storepass changeit -keystore "JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥jre¥lib¥security¥cacerts"
```

キーストアから証明書を削除する場合、次のコマンドを実行します。

```
"JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥bin¥keytool.exe" -delete -alias エイリアス名※ -keystore "JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥jre¥lib¥security¥cacerts" -storepass changeit
```

注※　エイリアス名は任意です。

**重要**

keytool.exe コマンドが異常終了する場合、キーストアファイルが読み取り専用属性となっている場合があります。この場合は、キーストアファイルの読み取り専用属性を解除したあと、コマンドを再度実行してください。

キーストアファイルのパスと読み取り専用属性の解除手順を次に示します。

キーストアファイルパス："JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥jdk¥jre¥lib¥security¥cacerts"

1. キーストアファイルを右クリックして［プロパティ］を選択する。
2. ［全般］タブの［属性］から［読み取り専用］のチェックを外す。

3. [OK] をクリックする。

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ

## 3.12.2 スマートデバイスマネージャーで SSL 通信用サーバ証明書を設定する手順

SSL 通信用サーバ証明書、および秘密鍵をスマートデバイスマネージャーに設定します。

**操作手順**

1. SSL 通信用サーバ証明書および秘密鍵を次のフォルダに格納します。
   JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥httpsd¥conf¥ssl¥server
2. httpsd.conf ファイルに定義を追加します。
   httpsd.conf ファイルの格納先は次のとおりです。
   JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥httpsd¥conf
   次に示すような特定行のコメントアウトや追記をします。

```
ServerName localhostまたはホスト名

#--途中省略--
Listen 26080
<VirtualHost localhostまたはホスト名:26080>
<Location /jp1itdm2sdm>
     Allow from all
</Location>
</VirtualHost>

Listen 26056
<VirtualHost localhost:26056>
<Location /rest>
     Allow from command
</Location>
</VirtualHost>

#--以下のコメントアウトを解除する--
Listen 26055
<VirtualHost ホスト名:26055>
    SSLEnable
    SSLProtocol TLSv1 TLSv11 TLSv12
    SSLCertificateFile "JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ/mgr/uC/httpsd/conf/ssl/server/newcert.pem"
    SSLCertificateKeyFile "JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール
```

```
先フォルダ/mgr/uC/httpsd/conf/ssl/server/newkeyRSA.pem”
    #SSLCertificateKeyPassword ”JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインス
トール先フォルダ/mgr/uC/httpsd/conf/ssl/server/.keypasswd”
    LoadModule proxy_module modules/mod_proxy.so
    LoadModule proxy_http_module modules/mod_proxy_http.so
    <Location /server01/api/v1.0>
        ProxyPass http://localhost:26057/rest/itdmsdapi
        Allow from all
    </Location>
    <Location /server01/api/version>
        ProxyPass http://localhost:26057/rest/itdmsdapi/version
        Allow from all
    </Location>
</VirtualHost>

Listen 26057
<VirtualHost localhost:26057>
<Location /rest>
     Allow from all
</Location>
</VirtualHost>
#--ここまで--

Include ”JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォル
ダ/mgr/uC/CC/web/redirector/mod_jk.conf”
```

（凡例）

httpsd.pem：サーバ証明書のファイル名（PEM 形式）

httpsdkey.pem：秘密鍵のファイル名（PEM 形式）

.keypasswd：パスワードファイル名

> **重要**
>
> Web サーバの秘密鍵作成時にパスワードを設定した場合、パスワードの作成コマンド（sslpasswd コマンド）でパスワードファイルを作成し、SSLCertificateKeyPassword ディレクティブを設定する必要があります。

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.2 スマートデバイスマネージャーの SSL 通信用証明書を取得する流れ
- 付録 G.6 パスワードファイルの作成（sslpasswd）

## 3.13　通信サーバでの SSL 通信用証明書の設定

通信サーバで、APNs サーバおよび通信サーバの SSL 通信用証明書を設定する手順について説明します。また、iOS 端末にクライアント証明書を配布するために、構成プロファイルを作成する手順についても説明します。

### 3.13.1　通信サーバで APNs サーバの SSL 通信用ルート証明書を設定する手順（iOS 端末を管理する場合）

通信サーバに、APNs サーバの SSL 通信用ルート証明書を設定します。この手順は、iOS 端末を管理する場合だけ実施します。

**操作手順**

1. 次のコマンドを実行し、ルート証明書をインストールします。

```
”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥bin¥keytool.exe” -importcert -alias エイリアス名※ -file 証明書のパス -keystore ”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥jre¥lib¥security¥cacerts” -storepass changeit
```

インストールされたルート証明書を確認する場合、次のコマンドを実行します。

```
”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥bin¥keytool.exe” -list -v -storepass changeit -keystore ”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥jre¥lib¥security¥cacerts”
```

キーストアから証明書を削除する場合、次のコマンドを実行します。

```
”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥bin¥keytool.exe” -delete -alias エイリアス名※ -keystore ”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥jre¥lib¥security¥cacerts” -storepass changeit
```

注※　エイリアス名は任意です。

**重要**

keytool.exe コマンドが異常終了する場合、キーストアファイルが読み取り専用属性となっている場合があります。この場合は、キーストアファイルの読み取り専用属性を解除したあと、コマンドを再度実行してください。

キーストアファイルのパスと読み取り専用属性の解除手順を次に示します。

キーストアファイルパス：”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥jdk¥jre¥lib¥security¥cacerts”

1. キーストアファイルを右クリックして［プロパティ］を選択する。
2. ［全般］タブの［属性］から［読み取り専用］のチェックを外す。

3. [OK] をクリックする。

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.3 APNs サーバの SSL 通信用ルート証明書を取得する手順（iOS 端末を管理する場合）

## 3.13.2 通信サーバで SSL 通信用サーバ証明書を設定する手順

通信サーバに、通信サーバの SSL 通信用サーバ証明書、および秘密鍵を設定します。

**操作手順**

1. SSL 通信用サーバ証明書および秘密鍵を次のフォルダに格納します。
   JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥conf¥ssl¥server
2. httpsd.conf ファイルに定義を追加します。
   httpsd.conf ファイルの格納先は次のとおりです。
   JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥conf
   次に示すような特定行の追記をします。

```
ServerName ホスト名

#--途中省略--
Listen 26055
<VirtualHost ホスト名:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLCertificateFile "JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/uC/
httpsd/conf/ssl/server/newcert.pem"
    SSLCertificateKeyFile "JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/uC/
httpsd/conf/ssl/server/newkeyRSA.pem"
</VirtualHost>
Include "JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/uC/CC/web/redirector/
mod_jk.conf"
```

（凡例）

httpsd.pem：サーバ証明書のファイル名（PEM 形式）

httpsdkey.pem：秘密鍵のファイル名（PEM 形式）

.keypasswd：パスワードファイル名

> **重要**
>
> Web サーバの秘密鍵作成時にパスワードを設定した場合、パスワードの作成コマンド（sslpasswd コマンド）でパスワードファイルを作成し、SSLCertificateKeyPassword ディレクティブを設定する必要があります。

3. 通信サーバのサービス「JP1/ITDM2 - Smart Device Manager Web Server」を再起動します。

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ
- 付録 G.6 パスワードファイルの作成（sslpasswd）

## 3.13.3 通信サーバで APNs サーバの SSL 通信用クライアント証明書を設定する手順（iOS 端末を管理する場合）

通信サーバに、APNs サーバの MDM 用クライアント証明書と MDM 用クライアント証明書のパスワードを記載したファイルを格納します。この手順は、iOS 端末を管理する場合だけ実施します。

**操作手順**

1. 通信サーバの次のフォルダに、MDM 用クライアント証明書（ファイル名「APNsMDMPushDev.p12」、PKCS#12 形式）、および MDM 用クライアント証明書のパスワードを記載したファイル（ファイル名「password」）を格納します。
   JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥conf
2. 通信サーバのサービス「JP1/ITDM2 - Smart Device Manager (Communication Server Service)」を再起動します。

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）

## 3.13.4 通信サーバで構成プロファイルを作成する手順（iOS 端末を管理する場合）

iOS 端末にクライアント証明書を配布するために、通信サーバで構成プロファイルを作成します。この手順は、iOS 端末を管理する場合だけ実施します。

### (1) iPhone 構成ユーティリティを使用する場合の手順

**前提条件**

この手順は、Apple 社が提供する iPhone 構成ユーティリティのバージョン 3.6 を基に説明しています。

**操作手順**

1. Apple 社が提供する iPhone 構成ユーティリティをインストールします。

2. 画面左［ライブラリ］－［構成プロファイル］を選択し、画面上部の［新規］ボタンをクリックします。

3.「一般」を次のとおりに設定します。

| 項目名 | 設定値 |
|---|---|
| 名前 | 任意 |
| 識別子 | 任意 |
| 組織 | 任意 |
| 説明 | 任意 |
| 同意メッセージ | 任意 |
| セキュリティ | 「常に確認」を選択します。 |
| プロファイルを自動的に削除します | 「しない」を選択します。 |

4.「資格情報」の項目で、iOS 端末が通信サーバに接続するためのルート証明書を選択後、資格情報名を入力し、追加します（iOS 端末に通信サーバのルート証明書がインストールされていない場合）。

> **ヒント**
>
> iOS 端末に個別にルート証明書を設定することもできます。

5.「資格情報」の項目で、iOS 端末が APNs サーバに接続するためのクライアント証明書（APNsMDMPushDev.p12）を選択後、資格情報名、証明書に対するパスワードを入力し、追加します。

6.「モバイルデバイス管理」を次のとおりに設定します。

| 項目名 | 設定値 |
|---|---|
| サーバ URL | https://**通信サーバホスト名**:26055/CommunicationServerWeb/ios/server |
| チェックイン URL | https://**通信サーバホスト名**:26055/CommunicationServerWeb/ios/checkin |
| トピック | Apple Push Certificates Portal で作成した MDM 証明書の Subject DN 内 UID を設定します。 |
| 固有名 | リストから手順 5 で設定した APNs サーバに接続するためのクライアント証明書の資格情報名を選択します。 |
| メッセージに署名 | チェックします。 |
| 削除時にチェックアウト | チェックします。 |
| アクセス権 | すべての項目にチェックします。 |
| Apple プッシュ通知サービス | チェックを外します。 |

7. 画面上部の［書き出す］ボタンをクリックし、［構成プロファイルに署名］を選択して、構成プロファイルをエクスポートします。
   ファイル名は「mdmprofile.mobileconfig」を指定します。

8. 構成プロファイルを通信サーバの次のフォルダに格納します。
   JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥conf

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ
- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）

## (2) 構成プロファイル作成ツールを使用する場合の手順

**操作手順**

1. 構成プロファイル作成ツールを起動します。
   構成プロファイル作成ツールの格納先を次に示します。

   **JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ**¥cms¥bin¥sdmgeneratemobileconf.exe

2. 「一般」を次のとおりに設定します。

| 項目名 | 項目の説明 | 必須項目 |
|---|---|---|
| 名前 | プロファイルの表示名 | ○ |
| 識別子 | プロファイルの一般識別子 | ○ |
| 組織 | プロファイルの組織名称 | － |
| 説明 | プロファイルの内容や目的の概要 | ○ |
| 同意メッセージ | プロファイルのインストール時に表示されるメッセージ | － |
| セキュリティ | プロファイル削除時のセキュリティ<br>常に確認<br>　iOS 端末の入力によりプロファイルを削除できる<br>認証<br>　任意のパスワードを入力することによりプロファイルを削除できる<br>しない<br>　プロファイルを削除できない | ○ |

（凡例）
○：必須

－：任意

3.「資格情報」の項目で、iOS 端末が通信サーバに接続するためのクライアント証明書を選択後、資格情報名、証明書に対するパスワードを入力し、追加します。

4.「モバイルデバイス管理」を次のとおりに設定します。

| 項目名 | 設定値 | 必須項目 |
|---|---|---|
| サーバ URL | https://通信サーバホスト名:26055/CommunicationServerWeb/ios/server | ○ |
| チェックイン URL | https://通信サーバホスト名:26055/CommunicationServerWeb/ios/checkin | ○ |
| トピック | Apple Push Certificates Portal で作成した MDM 証明書の Subject DN 内 UID を設定します。 | ○ |

（凡例）

○：必須

5.［生成］ボタンをクリックし、構成プロファイルをエクスポートします。

ファイル名には「mdmprofile.mobileconfig」を指定してください。

6. 構成プロファイルを通信サーバの次のフォルダに格納します。

JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥conf

**関連項目**

- 3.1 システムを構築する流れ
- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ
- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.7 MDM 用クライアント証明書を作成する手順（iOS 端末を管理する場合）

# 3.14 スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ

組織内で利用するスマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入し、スマートデバイスの管理を始めるまでの流れを説明します。

1. セキュリティ方針を策定する
2. セキュリティのルールを登録する
3. 組織内のスマートデバイスを把握する

   スマートデバイスの管理台帳などを作成し、その情報を基に JP1/ITDM2 - SDM で管理対象とするスマートデバイスを決定してください。また、管理対象のスマートデバイスの登録情報を入手してください。
4. プロビジョニングを設定する
5. スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する
6. スマートデバイスに SSL 通信用ルート証明書を設定する（必要な証明書がプリインストールされていなかった場合だけ）
7. スマートデバイスの情報を JP1/ITDM2 - SDM に登録する
8. JP1/ITDM2 - SDM で APNs サーバとの SSL 通信用パスワードを設定する
9. JP1/ITDM2 - SDM（スマートデバイスエージェント）の導入計画を立てる

   JP1/ITDM2 - SDM（スマートデバイスエージェント）の導入には、次の 2 種類の方法があります。適宜選択してください。

   - 管理者が JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールしてから利用者に配布する
   - スマートデバイスを配布したあと、利用者に JP1/ITDM2 - SDM（スマートデバイスエージェント）のインストールを依頼する
10. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールする

    管理者または利用者がスマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールします。
11. JP1/ITDM2 - SDM（スマートデバイスエージェント）のインストール状況を確認する

    スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）がインストールされると、JP1/ITDM2 - SDM にインベントリ情報が定期的に通知されます。管理対象のスマートデバイスから一定期間インベントリ情報が通知されない場合、イベントが発行されます。したがって、イベントの発行状況を確認すれば、スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）が導入されているかを把握できます。
12. JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入するようメールなどで通知する（JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入していない利用者がいる場合だけ）

**関連項目**

- 2.4.1 セキュリティのルールの種類
- 3.14.1 組織のセキュリティ方針の策定について
- 3.14.2 プロビジョニングの設定について
- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）
- 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）
- 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順
- 7.1 セキュリティポリシーを利用する
- 7.2 Android ポリシーを利用する
- 7.3 iOS プロファイルを利用する
- 8.1 スマートデバイスの JP1/ITDM2 - SDM への登録

## 3.14.1　組織のセキュリティ方針の策定について

組織のスマートデバイスのセキュリティを管理するために、組織のセキュリティ方針を策定します。

セキュリティ方針を策定するポイントを次に示します。

- スマートデバイスのロック解除パスワードを、推測されにくいものに設定するように徹底したい場合、パスワードのポリシーを作成する
- 利用者が通話できる電話番号を業務に必要なものに制限したい場合、通話を許可する電話番号のリストを作成する
- インストール必須または使用禁止にしたいアプリケーションがある場合、必須または禁止にするアプリケーションのリストを作成する
- Web 閲覧を許可または禁止したいサイトがある場合、閲覧許可または禁止するサイトのリストを作成する
- スマートデバイスの機能で抑止したいもの（カメラの利用禁止など）がある場合、抑止する機能のリストを作成する

これらのポイントは組織内の部署や業務内容によって異なることが想定されます。各部門のセキュリティ管理者と連携して、各業務の内容に合致したセキュリティ方針を策定してください。

また、強固なセキュリティ管理を実現するためには、最新のセキュリティ対策の傾向を把握し、定期的にセキュリティ方針を見直すことを推奨します。

**関連項目**

- 2.4 セキュリティの管理

## 3.14.2 プロビジョニングの設定について

プロビジョニングとは、スマートデバイス上で稼働する JP1/ITDM2 - SDM（スマートデバイスエージェント）の設定情報のことです。

設定情報を次に示します。

- 接続先通信サーバの URL
- 接続先メッセージングサーバの URL
- インベントリ取得間隔
- GPS 情報取得間隔
- 低電圧時にインベントリを送信する際のバッテリー容量

プロビジョニングの設定は、Provisioning 情報設定ファイル（provisioning.properties）を更新し、サービスを再起動することで有効になります。

**関連項目**

- 16.3 Provisioning 情報設定ファイル（provisioning.properties）

## 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順

必要な SSL 通信用ルート証明書がスマートデバイスにプリインストールされているかどうか確認します。

**操作手順**

1. スマートデバイスで次のとおりに操作します。

   iOS 端末の場合

   ［設定］－［一般］－［情報］－［トラストストア］から、Apple 社のサイトにアクセスします。
   Apple 社のサイトで、iOS 端末にプリインストールされているルート証明書の一覧を確認します。

Android 端末の場合

ルート証明書の一覧を確認します。ルート証明書一覧の表示手順は機種、OS によって異なります。表示方法については各端末のメーカーにご確認ください。Android 4.1.1 の場合の表示手順の例を次に示します。

［設定］－［セキュリティ］－［信頼できる認証情報］

**次の作業**

必要な SSL 通信用ルート証明書がプリインストールされていた場合は、スマートデバイスに対するルート証明書の設定は不要です。

必要な SSL 通信用ルート証明書がプリインストールされていなかった場合は、証明書を取得し、スマートデバイスに設定します。

**関連項目**

- 3.11.1 通信サーバの SSL 通信用証明書を取得する流れ
- 3.11.3 APNs サーバの SSL 通信用ルート証明書を取得する手順（iOS 端末を管理する場合）
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順

## 3.14.4　Android 端末で SSL 通信用ルート証明書を設定する手順

通信サーバの SSL 通信用ルート証明書を Android 端末にインストールします。この手順は、SSL 通信用ルート証明書がインストールされていない場合だけ実施します。

**操作手順**

1. ルート証明書ファイルを端末の内部ストレージまたは SD カードのルートディレクトリに配置します。

   ルート証明書ファイルの拡張子は.cer または.crt です。

2. ストレージからのインストールまたは SD カードからのインストールを選択します。

   ストレージからインストールする場合

   ［設定］－［ユーザー設定］－［セキュリティ］－［認証情報ストレージ］－［ストレージからのインストール］

   SD カードからインストールする場合

   ［設定］－［ユーザー設定］－［セキュリティ］－［認証情報ストレージ］－［SD カードからのインストール］

3. インストールするルート証明書を選択します。

4. 証明書に名称を設定し、［OK］ボタンをタップします。

   インストールが完了します。

5. 証明書がインストールされたか確認します。

［設定］－［ユーザー設定］－［セキュリティ］－［認証情報ストレージ］－［信頼できる認証情報］の［ユーザー］タブで確認できます。

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順

## 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順

通信サーバの SSL 通信用ルート証明書、および APNs サーバの SSL 通信用ルート証明書を iOS 端末にインストールします。この手順は、必要な SSL 通信用ルート証明書がインストールされていない場合だけ実施します。

**操作手順**

1. iPhone 構成ユーティリティを起動します。
2. ［ライブラリ］－［構成プロファイル］をタップし、［新規］をタップします。
3. ［資格情報］をタップし、右側の［構成］ボタンをタップします。
4. 取得したルート証明書を選択します。
5. ［一般］をタップし、任意の［名前］および［識別子］を入力します。
6. ［デバイス］の［デバイス名の iPhone（または iPad)］から、［構成プロファイル］タブを選択し、［インストール］ボタンをタップします。
7. 表示されるプロファイルのインストール画面で［インストール］ボタンをタップします。
8. インストールに関する確認メッセージで［インストール］ボタンをタップします。
9. インストール完了画面で［完了］ボタンをタップします。

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順

## 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）

Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）（アプリ名：JP1ITDM2SDM）をインストールし、JP1/ITDM2 - SDM（スマートデバイス Android エージェント）の設定をします。この手順は、Android 端末を使用する場合の手順です。

**操作手順**

1. Google Play ストアアプリを起動します。
2. Play ストアアイコンをタップし、［マイアプリ］を選択します。
3. カテゴリとして［すべて］を選択します。
4. JP1/ITDM2 - SDM（スマートデバイス Android エージェント）（アプリ名：JP1ITDM2SDM）を選択して、アプリの詳細ページにある［インストール］ボタンをタップします。
   JP1/ITDM2 - SDM（スマートデバイス Android エージェント）がインストールされます。
5. Android 端末で JP1/ITDM2 - SDM（スマートデバイス Android エージェント）を起動します。
6. 通信サーバ設定画面で、接続先通信サーバホスト名および名称を入力し、［OK］ボタンをタップします。
   通信サーバには「**ホスト名**:26055」の形式で指定してください。また、名称には、JP1/ITDM2 - SDM に登録したスマートデバイスの名称を指定してください。
   サーバに正常に接続できると、それを示すダイアログが表示されます。
7. ダイアログで［OK］ボタンをタップします。

## 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）

Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）（アプリ名：JP1ITDM2SDM）をインストールし、JP1/ITDM2 - SDM（スマートデバイス Android エージェント）の設定をします。この手順は、PC を使用する場合の手順です。

**操作手順**

1. PC で Google Play の［マイアプリ］ページにアクセスします。
2. アプリを選択して、その詳細ページを表示します。
3. ［インストール］または［インストール済み］と表示されているボタンをクリックし、アプリのインストール先となる端末を選択します。
4. ［インストール］をクリックします。
   JP1/ITDM2 - SDM（スマートデバイス Android エージェント）がインストールされます。
5. Android 端末で JP1/ITDM2 - SDM（スマートデバイス Android エージェント）を起動します。
6. 通信サーバ設定画面で、接続先通信サーバホスト名および名称を入力し、［OK］ボタンをタップします。
   通信サーバには「**ホスト名**:26055」の形式で指定してください。また、名称には、JP1/ITDM2 - SDM に登録したスマートデバイスの名称を指定してください。

サーバに正常に接続できると、それを示すダイアログが表示されます。

7. ダイアログで［OK］ボタンをタップします。

## 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順

iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）（アプリ名：JP1ITDM2SDM）をインストールし、JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）の設定をします。

**操作手順**

1. App Store から JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）（アプリ名：JP1ITDM2SDM）をダウンロードし、インストールします。

2. iOS 端末で JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）を起動します。

3. 通信サーバ設定画面で、接続先通信サーバホスト名および名称を入力し、［OK］ボタンをタップします。
   通信サーバには「**ホスト名**:26055」の形式で指定してください。また、名称には、JP1/ITDM2 - SDM に登録したスマートデバイスの名称を指定してください。
   サーバに正常に接続できると、それを示すダイアログが表示されます。

4. ダイアログで［OK］ボタンをタップします。

## 3.15　サーバから JP1/ITDM2 - SDM をアンインストールする手順

JP1/ITDM2 - SDM を再インストールする場合などに、サーバから、JP1/ITDM2 - SDM（スマートデバイスマネージャー）、JP1/ITDM2 - SDM（通信サーバ）または JP1/ITDM2 - SDM（メッセージングサーバ）をアンインストールします。

### 前提条件

- アンインストール対象のサーバに、Administrator 権限のユーザーアカウントでログインしておく必要があります。
- JP1/ITDM2 - SDM のプログラムが起動している場合、停止しておくことを推奨します。

### 操作手順

1. Windows のコントロールパネルで［プログラムと機能］を選択します。
   アンインストールするプログラムを選択するダイアログボックスが表示されます。
2. アンインストールする JP/ITDM2 - SDM プログラムを選択し、［アンインストール］ボタンをクリックします。
3. アンインストール開始のダイアログで［次へ］ボタンをクリックします。
4. ［サーバ選択］ダイアログでアンインストール対象のサーバコンポーネントを選択し、［次へ］ボタンをクリックします。
5. ［プログラムの削除］ダイアログで［削除］ボタンをクリックします。
   選択したプログラムがアンインストールされます。
6. インストール先フォルダ下にファイルやフォルダが残っている場合、必要に応じてフォルダやファイルを削除します。

> **重要**
>
> アンインストール中にファイルやフォルダを開いている場合、フォルダやファイルが残ったままとなります。アンインストール前に、ファイルやフォルダを閉じておくことを推奨します。

### 関連項目

- 付録 A フォルダ一覧

## 3.16 Android 端末から JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールする手順（Android 端末の設定メニューを使用する場合）

Android 端末の設定メニューで、Android 端末の JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールします。

**操作手順**

1. [設定] メニューから［アプリ］または［アプリケーションマネージャ］に移動します。
2. JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のアプリ（アプリ名：JP1ITDM2SDM）をタップします。
3. [アンインストール] を選択します。
   JP1/ITDM2 - SDM（スマートデバイス Android エージェント）がアンインストールされます。

## 3.17 Android 端末から JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールする手順（Google Play ストアアプリを使用する場合）

Google Play ストアアプリで、Android 端末の JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をアンインストールします。

**操作手順**

1. Google Play ストアアプリを起動します。
2. Play ストアアイコン－［マイアプリ］をタップします。
3. ［インストール済み］と表示されている JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のアプリ（アプリ名：JP1ITDM2SDM）をタップし、アプリの詳細ページで［アンインストール］をタップします。
   JP1/ITDM2 - SDM（スマートデバイス Android エージェント）がアンインストールされます。

## 3.18　iOS 端末から JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をアンインストールする手順

iOS 端末から、JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をアンインストールします。

**操作手順**

1. JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）のアプリ（アプリ名：JP1ITDM2SDM）を一定時間長押しします。
2. アイコン左上に［×］が表示されたら、［×］をタップします。
3. [削除］をタップし、アプリを削除します。
   JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）がアンインストールされます。

## 3.19　バージョンアップインストール時の作業

バージョンアップインストール時の追加作業について説明します。

### 3.19.1　通信サーバをバージョンアップインストールするときの作業

JP1/ITDM2 - SDM（通信サーバ） 11-10 より前のバージョンからバージョンアップインストールするとき、インストール作業に加え、httpsd.conf ファイルに定義の追加が必要です。

httpsd.conf の格納先

JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥conf

(1) 標準配布を使用する場合

<VirtualHost localhost:26055>の中に、次の設定を追加します（下線部）。

```
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/～/newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/～/newkeyRSA.pem"
    <Location /download/>
         Allow from all
    </Location>
</VirtualHost>
```

(2) 標準配布で配布アプリケーションの最大同時ダウンロード数を制限する場合

次の設定を追加します（下線部）。

```
LoadModule hws_qos_modules/mod_hws_qos.so
QOSCookieServers 0
:
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/～/newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/～/newkeyRSA.pem"
    <Location /download/>
            Allow from all
            QOSRejectionServers 5
    </Location>
</VirtualHost>
```

(3) 標準配布でアクセス認証をする場合

次の設定を追加します。

```
<Directory "JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/uC/httpsd/htdocs/
download">
    AuthType Basic
    AuthName "realm"
```

```
    AuthUserFile "JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/conf/
htpasswd"
    Require valid-user
</Directory>
```

### 関連項目

- 16.2 スマートデバイスマネージャー環境設定ファイル（manager.properties）

# 4 製品を使った運用方法

ここでは、JP1/ITDM2 - SDM を使ったスマートデバイスの管理やスマートデバイスの紛失の対処など、運用方法について説明します。

## 4.1　スマートデバイスに対する遠隔操作について

JP1/ITDM2 - SDM では、スマートデバイスマネージャーから GUI やコマンドによって、スマートデバイスに対して、アプリケーションの配布、セキュリティルールの適用、ロックなどの遠隔操作が実施できます。

多数のスマートデバイスに対してアプリケーションの配布、セキュリティルールの適用、インベントリの収集（定期的なインベントリ収集も含む）などの遠隔操作を実施する場合は、それぞれの実行時間帯をずらして計画してください。

なお、スマートデバイスの OS によっても、遠隔操作の考え方が異なります。

**関連項目**

- 4.1.1 Android 端末の管理について
- 4.1.2 iOS 端末の管理について

### 4.1.1　Android 端末の管理について

Android 端末では、スマートデバイスマネージャーから Android 端末に対して遠隔操作を実施する際、Android 端末の電源が入っている場合だけ遠隔操作を実施できます。

Android 端末の電源が入っていない場合、即時失敗となるため、時間をおいてから再度遠隔操作を実施してください。

また、アプリケーションを配布する場合、Android 端末側での操作が行われないと、電源が入っていても失敗するケースがありますので、注意してください。

**関連項目**

- 4.9 Android 端末にアプリケーションを配布・インストールする流れ

### 4.1.2　iOS 端末の管理について

iOS 端末では、スマートデバイスマネージャーから iOS 端末に対して遠隔操作を実施する際、iOS 端末の電源状態に関係なく、iOS 端末に対して遠隔操作を実施できます。ただし、要求を行ってから 24 時間以上経過しても端末の電源が入らなかった場合、その遠隔操作は失敗となります。

なお、多数の iOS 端末に対して同時に遠隔操作を実施する場合、24 時間後に結果を確認し、失敗している iOS 端末に対してだけ、再度遠隔操作を実施してください。

また、アプリケーションの配布と iOS プロファイルの適用の場合、iOS 端末側での操作や iOS 端末の状態によって、電源が入っていても失敗するケースがあります。

### アプリケーションを配布する場合

iOS 端末側にインストールの許可を求めるダイアログが表示されます。ダイアログでインストールを許可しないと、インストールが実施されません。

### iOS プロファイルを適用する場合

パスワード付きロックが設定されている iOS 端末にプロファイルを適用するには、iOS プロファイルの適用時に iOS 端末のロックが解除されている必要があります。

### 関連項目

- 4.10 iOS 端末にアプリケーションをインストールする流れ
- 4.13.2 iOS プロファイルを適用する流れ

## 4.2 運用中にできること

JP1/ITDM2 - SDM の運用中にできることを説明します。

| 運用中にできること | 概要 |
|---|---|
| スマートデバイスを準備する | JP1/ITDM2 - SDM で管理するスマートデバイスを準備します。新規に購入したスマートデバイスを利用する場合と、保管されていたスマートデバイスを利用する場合とで、準備する内容が異なります。 |
| スマートデバイスを新規に配布する | 新規にスマートデバイスの利用申請があった場合、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リプレースする | スマートデバイスの入れ替えなどに伴って組織内のスマートデバイスをリプレースします。 |
| スマートデバイスの利用者を変更する | 利用者が異動する場合など、ほかの利用者にスマートデバイスを引き継げます。 |
| スマートデバイスを保管する | 利用者の異動やスマートデバイスの入れ替えなどによって、利用しなくなったスマートデバイスを保管します。 |
| スマートデバイスを滅却する | 故障などの理由で、今後使用する予定がないスマートデバイスを滅却します。 |
| Android 端末にアプリケーションを配布・インストールを指示する | 配布したいアプリケーションを複数の Android 端末に一括して配布できます。 |
| iOS 端末にアプリケーションのインストールを指示する | 配布したいアプリケーションを複数の iOS 端末に一括してインストールを指示できます。 |
| スマートデバイスから利用者の操作でアプリケーションをインストールする | 管理者があらかじめ用意したアプリケーションを、利用者の操作によってインストールできます。 |
| 不要となったアプリケーションを削除する | 不要となったアプリケーションを Android 端末からアンインストールおよび削除できます。 |
| セキュリティのルールを管理する | スマートデバイスを管理するために、組織のセキュリティ方針を基にセキュリティのルールを作成します。セキュリティのルールに違反した利用があると、イベントが発行され、スマートデバイスの不正利用を検知できます。 |
| スマートデバイスの紛失に対処する | 利用者がスマートデバイスを紛失した場合は、紛失したスマートデバイスをロック、または初期化してスマートデバイスの不正利用を防ぎます。 |
| 利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合に対処する | 利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合は、Android 端末のパスワードを変更、または iOS 端末のパスコードをリセットできます。 |
| 発生したイベントをメールで通知する | JP1/ITDM2 - SDM で発生したイベントやスマートデバイスで発生したイベントを、管理者にメールで通知できます。管理者は、JP1/ITDM2 - SDM の操作画面にログインしなくても、JP1/ITDM2 - SDM の障害やスマートデバイスの不正利用などを確認できます。 |
| Android 端末にメッセージを通知する | Android 端末の利用者に連絡事項などがある場合に、JP1/ITDM2 - SDM から Android 端末にメッセージを通知できます。 |

**関連項目**

- 4.3 スマートデバイスの準備について
- 4.4 スマートデバイスを新規に配布する流れ
- 4.5 スマートデバイスをリプレースする流れ
- 4.6 スマートデバイスの利用者を変更する流れ
- 4.7 スマートデバイスを保管する流れ
- 4.8 スマートデバイスを滅却する流れ
- 4.9 Android 端末にアプリケーションを配布・インストールする流れ
- 4.10 iOS 端末にアプリケーションをインストールする流れ
- 4.11 スマートデバイスから利用者の操作でアプリケーションをインストールする流れ
- 4.12 不要となったアプリケーションを削除する流れ
- 4.13 セキュリティのルールの管理について
- 4.14 スマートデバイス紛失時の対処について
- 4.15 利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合の対処について
- 4.16 発生したイベントをメールで通知する流れ
- 8.11 Android 端末にメッセージを通知する手順

## 4.3　スマートデバイスの準備について

スマートデバイスを JP1/ITDM2 - SDM で管理し、利用するためにスマートデバイスの準備をします。

配布するスマートデバイスが新規に購入するものか、JP1/ITDM2 - SDM に登録されているものかによって、準備の内容が異なります。

**関連項目**

- 4.3.1 新規に購入したスマートデバイスを準備する流れ
- 4.3.2 すでに JP1/ITDM2 - SDM に登録されているスマートデバイスを準備する流れ

### 4.3.1　新規に購入したスマートデバイスを準備する流れ

新規に購入したスマートデバイスを利用する場合、JP1/ITDM2 - SDM に登録し、スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールします。

新規のスマートデバイスを準備する流れを次に示します。

1. スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する
2. スマートデバイスに SSL 通信用ルート証明書を設定する（必要な証明書がプリインストールされていなかった場合だけ）
3. スマートデバイスを JP1/ITDM2 - SDM に登録する

   利用者に合ったセキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを設定し、スマートデバイスを管理対象として登録します。
4. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールする

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）
- 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）
- 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順
- 8.1 スマートデバイスの JP1/ITDM2 - SDM への登録

### 4.3.2 すでに JP1/ITDM2 - SDM に登録されているスマートデバイスを準備する流れ

保管しているスマートデバイスを利用する場合、スマートデバイスのスペックなどを確認します。問題なく使用できるスマートデバイスであれば、管理対象外から管理対象にし、スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールします。

すでにあるスマートデバイスを準備する流れを次に示します。

1. スマートデバイスを確認する

   スペックなどを確認して、問題なく使用できるスマートデバイスかを確認します。スマートデバイス画面の［スマートデバイス］－［管理対象外のスマートデバイス一覧］で確認します。
2. スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する
3. スマートデバイスに SSL 通信用ルート証明書を設定する（必要な証明書がプリインストールされていなかった場合だけ）
4. スマートデバイスを管理対象にする
5. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールする

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）
- 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）
- 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順
- 8.3 管理対象外のスマートデバイスを管理対象にする
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 4.4　スマートデバイスを新規に配布する流れ

運用後に、新規にスマートデバイスの利用申請があった場合、スマートデバイスを準備して利用者に配布します。

スマートデバイスを新規に配布する流れを次に示します。

1. スマートデバイスを準備する

   **ヒント**

   配布するスマートデバイスの一覧を作成すると、スマートデバイス配布時のチェックリストとして使用できます。スマートデバイスの一覧はスマートデバイスの情報を CSV ファイルにエクスポートし、作成します。

2. スマートデバイスを利用者に配布する
3. 最新のインベントリ情報が取得できるかを確認する

   スマートデバイスを配布したあと、スマートデバイスのインベントリ情報が JP1/ITDM2 - SDM に取得できるかを確認します。取得できない場合は、JP1/ITDM2 - SDM（スマートデバイスエージェント）が正しくインストールされているかを確認します。

**関連項目**

- 4.3 スマートデバイスの準備について
- 8.2 スマートデバイス一覧をエクスポートする手順
- 8.6 スマートデバイスから最新のインベントリ情報を取得する手順

## 4.5　スマートデバイスをリプレースする流れ

スマートデバイスの入れ替えなど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/ITDM2 - SDM 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回収・配布します。

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. リプレースするスマートデバイスを特定する

   スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］で、リプレースが必要なスマートデバイスがないか調査します。このとき、フィルタを利用すると表示する情報を絞り込めます。

2. スマートデバイスを準備する

   > **ヒント**
   >
   > リプレースするスマートデバイスの一覧を作成すると、スマートデバイスリプレース時のチェックリストとして使用できます。スマートデバイスの一覧はスマートデバイスの情報を CSV ファイルにエクスポートし、作成します。

3. スマートデバイスを回収する

   > **ヒント**
   >
   > 回収したスマートデバイスを今後再利用する場合、スマートデバイスを保管します。回収したスマートデバイスを今後再利用しない場合、スマートデバイスを滅却します。

4. 回収したスマートデバイスの SIM カードを、配布するスマートデバイスに移す

   SIM カードを含めてスマートデバイスをリプレースする場合および SIM カードを使用していない場合は、この作業は不要です。

5. スマートデバイスを利用者に配布する

6. インベントリ情報が取得できるかを確認する

   スマートデバイスを配布したあと、スマートデバイスのインベントリ情報が JP1/ITDM2 - SDM に取得できるかを確認します。取得できない場合は、JP1/ITDM2 - SDM（スマートデバイスエージェント）が正しくインストールされているかを確認します。

**関連項目**

- 4.3 スマートデバイスの準備について
- 4.7 スマートデバイスを保管する流れ
- 4.8 スマートデバイスを滅却する流れ
- 8.2 スマートデバイス一覧をエクスポートする手順
- 8.6 スマートデバイスから最新のインベントリ情報を取得する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.6　スマートデバイスの利用者を変更する流れ

利用者が異動する場合など、ほかの利用者にスマートデバイスを引き継ぐときは、スマートデバイスをいったん初期化してから、JP1/ITDM2 - SDM 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. 必要な情報を入手する

   利用者変更に必要な次の情報を入手します。

   - 名称
   - 変更前の利用者名と部署
   - 変更後の利用者名と部署

2. 利用者を変更するスマートデバイスを特定する

   入手した情報を基に、スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］で、利用者を変更する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表示する情報を絞り込めます。

3. 現在の利用者からスマートデバイスを回収する
4. 回収したスマートデバイスを初期化する
5. スマートデバイスを管理対象外にする
6. スマートデバイスを JP1/ITDM2 - SDM から削除する
7. スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する
8. スマートデバイスに SSL 通信用ルート証明書を設定する（必要な証明書がプリインストールされていなかった場合だけ）
9. スマートデバイスを JP1/ITDM2 - SDM に登録する

   利用者に合ったセキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを設定し、スマートデバイスを管理対象として登録します。

10. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールする
11. スマートデバイスを新しい利用者に配布する
12. インベントリ情報が取得できるかを確認する

    スマートデバイスを配布したあと、スマートデバイスのインベントリ情報が JP1/ITDM2 - SDM に取得できるかを確認します。取得できない場合は、JP1/ITDM2 - SDM（スマートデバイスエージェント）が正しくインストールされているかを確認します。

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順

- 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）
- 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）
- 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順
- 8.1 スマートデバイスの JP1/ITDM2 - SDM への登録
- 8.3 管理対象外のスマートデバイスを管理対象にする
- 8.4 管理対象のスマートデバイスを管理対象外にする手順
- 8.5 スマートデバイスを JP1/ITDM2 - SDM から削除する手順
- 8.7 スマートデバイスを初期化する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.7　スマートデバイスを保管する流れ

利用者の異動やスマートデバイスの入れ替えなどによって利用しなくなったスマートデバイスは、初期化して保管します。

スマートデバイスを保管する流れを次に示します。

1. 利用しなくなったスマートデバイスを回収する
2. 回収したスマートデバイスを初期化する

> **重要**
>
> 初期化されたスマートデバイスは、JP1/ITDM2 - SDM（スマートデバイスエージェント）が削除され、設定していたセキュリティポリシーと Android ポリシー、またはセキュリティポリシーと iOS プロファイルの設定情報も破棄されます。

**関連項目**

- 8.7 スマートデバイスを初期化する手順

## 4.8　スマートデバイスを滅却する流れ

故障などの理由で、今後使用する予定がないスマートデバイスは、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. 滅却するスマートデバイスを決定する

   **ヒント**

   滅却するスマートデバイスの一覧を作成すると、スマートデバイス滅却時のチェックリストとして使用できます。スマートデバイスの一覧はスマートデバイスの情報を CSV ファイルにエクスポートし、作成します。

2. 滅却するスマートデバイスを初期化する

   すでに初期化してある場合は、この作業は不要です。

3. スマートデバイスを管理対象外にする

   管理対象外にする際は、[強制的に対象外にする。] をチェックしてください。

   また、JP1/IT Desktop Management 2 で資産管理を実施している場合は、JP1/IT Desktop Management 2 で資産を滅却状態にしてください。

4. スマートデバイスを廃棄する

5. 廃棄したスマートデバイスを JP1/ITDM2 - SDM から削除する

   JP1/IT Desktop Management 2 で資産管理を実施している場合は、JP1/IT Desktop Management 2 で資産を削除してください。

**関連項目**

- 8.2 スマートデバイス一覧をエクスポートする手順
- 8.4 管理対象のスマートデバイスを管理対象外にする手順
- 8.5 スマートデバイスを JP1/ITDM2 - SDM から削除する手順
- 8.7 スマートデバイスを初期化する手順

## 4.9 Android 端末にアプリケーションを配布・インストールする流れ

配布したいアプリケーションを JP1/ITDM2 - SDM に登録し、複数の Android 端末に一括してインストールします。

事前にアプリケーションを配布し、別途インストールを指示することもできます。

アプリケーションの配布には、ネットワークに負荷がかかるため、事前に配布計画を立てる必要があります。

アプリケーションを配布・インストールする流れを次に示します。

1. 組織のセキュリティ方針にのっとったアプリケーションを選定する
2. アプリケーションの配布計画を立てる

   アプリケーションの配布・インストールを指示すると、Android 端末での操作を伴わずにアプリケーションが配布されます。多数の Android 端末に同時に配布を行うとネットワークの負荷が集中するため、50 台ずつ 5 分ほど間隔を空けて実行するようにスケジュールを立ててください。

   なお、配布した結果を確認するには、インベントリ情報を収集する必要があります。

   (例)

   ```
   01:00～03:00  アプリケーションのインストール指示を行う。
   22:00～24:00  配布した端末からインベントリを収集する。
   ```

3. 配布するアプリケーションを JP1/ITDM2 - SDM に登録する
4. 配布するアプリケーションを通信サーバに配置する

   **重要**

   正しく配置したことを確認するため、アプリケーションの配布、またはインストールを指示する前に、テスト用端末などにインストールできるかどうかを確認します。

   インストールできない場合は、アプリケーション登録時のパッケージ名や通信サーバに配置したファイル名が正しいかを確認してください。

   **メモ**

   簡易配布の場合、この作業は不要です。

5. 利用者に Android 端末の電源を入れておくよう通知する

   配布またはインストールを指示するとき、Android 端末の電源が入っていないと失敗となります。このため、事前に電源を入れておくよう通知してください。

6. Android 端末にアプリケーションの配布、またはインストールを指示する

   配布計画に従って、アプリケーションの配布またはインストールの指示を実施してください。1 回の指示で対象とする Android 端末は 50 台程度とし、実行後 5 分程度間隔を空けて実行することをお勧めします。

7. インベントリ情報を収集する

   配布またはインストールの指示後、24 時間を目安にインベントリ情報を収集してください。

8. アプリケーションの配布またはインストール結果を確認する

   アプリケーションの配布・インストール状況は［Android アプリケーション］画面および `sdmexportdistributestatus` コマンドで確認できます。配布・インストールが失敗している場合は、対象の Android 端末に対して、再度配布またはインストールを指示してください。

**関連項目**

- 8.6 スマートデバイスから最新のインベントリ情報を取得する手順
- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.6 Android 端末にアプリケーションを配布する手順
- 9.7 Android 端末にアプリケーションのインストールを指示する手順
- 14.6.2 ［Android アプリケーション］画面
- 15. sdmexportdistributestatus（アプリケーション配布状況の出力）

## 4.10　iOS 端末にアプリケーションをインストールする流れ

企業内向けに開発した iOS アプリケーションを、複数の iOS 端末に一括してインストールします。

iOS アプリケーションのインストールは、iOS 端末利用者の操作が必要です。また、アプリケーションの配布には、ネットワークに負荷がかかるため、事前に配布計画を立てる必要があります。

**重要**

JP1/ITDM2 - SDM で配布できる iOS アプリケーションは、ユーザーが企業内向けに開発したアプリケーションだけです。AppStore の iOS アプリケーションは、JP1/ITDM2 - SDM では配布できません。

アプリケーションをインストールする流れを次に示します。

1. 組織のセキュリティ方針にのっとったアプリケーションを選定する
2. アプリケーションの配布計画を立てる

   アプリケーションのインストールを指示すると、iOS 端末利用者がアプリケーションのインストールを許可したあとにアプリケーションが配布されます。多数の iOS 端末から同時にアクセスされると、ネットワークの負荷が集中するため、拠点ごとに時間帯を分けるようなスケジュールを立ててください。

   （例）

   ```
   01:00～02:00  拠点Aにアプリケーションのインストール指示を行う。
                 拠点Aは午前中にインストールを行う。
   13:00～14:00  拠点Bにアプリケーションのインストール指示を行う。
                 拠点Bは午後にインストールを行う。
   22:00～24:00  配布した端末からインベントリを収集する。
   ```

   1 回の指示で対象とする iOS 端末は 50 台程度とし、実行後 5 分程度間隔を空けて実行することをお勧めします。
3. 配布するアプリケーションを JP1/ITDM2 - SDM に登録する
4. 配布するアプリケーションを通信サーバに配置する

**重要**

正しく配置したことを確認するため、アプリケーションの配布、またはインストールを指示する前に、テスト用端末などにインストールできるかどうかを確認します。

インストールできない場合は、アプリケーション登録時のパッケージ名や通信サーバに配置したファイル名が正しいかを確認してください。

**メモ**

簡易配布の場合、この作業は不要です。

5. iOS 端末にアプリケーションのインストールを指示する

   配布計画に従って、インストールの指示を実施してください。

6. インベントリ情報を収集する

   インストールの指示後、24 時間を目安にインベントリ情報を収集してください。

7. アプリケーションのインストール結果を確認する

   アプリケーションのインストール状況は［iOS アプリケーション］画面および `sdmexportdistributestatus` コマンドで確認できます。

   インストール指示後、24 時間経過してもインストールが完了しない場合は、インストールが失敗となります。対象の iOS 端末に対して、再度インストールを指示してください。

**関連項目**

- 8.6 スマートデバイスから最新のインベントリ情報を取得する手順
- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.9 iOS 端末にアプリケーションのインストールを指示する手順
- 14.6.4 ［iOS アプリケーション］画面
- 15. sdmexportdistributestatus（アプリケーション配布状況の出力）

## 4.11 スマートデバイスから利用者の操作でアプリケーションをインストールする流れ

利用者の操作でインストールできるアプリケーションを JP1/ITDM2 - SDM に登録および設定することで、利用者が任意のタイミングでアプリケーションをインストールできます。

スマートデバイスから利用者の操作でアプリケーションをインストールする流れを次に示します。

1. ネットワークに負荷がかからないように、アプリケーションの最大同時ダウンロード数を検討する
2. 組織のセキュリティ方針にのっとったアプリケーションを選定する
3. 配布するアプリケーションを JP1/ITDM2 - SDM に登録する
4. 配布するアプリケーションを通信サーバに配置する

> **メモ**
>
> 簡易配布の場合、この作業は不要です。

5. 利用者の操作でインストールできるアプリケーションを設定する
6. 利用者に対して、アプリケーションがインストールできることをメールなどで通知する
   通知する内容を次に示します。
   - アプリケーション名
   - バージョン
7. 利用者が、任意のタイミングでアプリケーションをインストールする

> **ヒント**
>
> アプリケーションのインストール状況は［Android アプリケーション］画面、［iOS アプリケーション］画面および`sdmexportdistributestatus` コマンドで確認できます。

8. 必要に応じて、インストールされていないスマートデバイスの利用者に対して、アプリケーションをインストールするようメールなどで通知する

**関連項目**

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.11 利用者の操作でインストールできるアプリケーションを管理する
- 9.12 Android 端末から利用者の操作でアプリケーションをインストールする手順
- 9.13 iOS 端末から利用者の操作でアプリケーションをインストールする手順
- 9.14 配布アプリケーションの最大同時ダウンロード数を制限する手順
- 14.6.2 ［Android アプリケーション］画面

- 14.6.4 ［iOS アプリケーション］画面
- 15. sdmexportdistributestatus（アプリケーション配布状況の出力）

## 4.12　不要となったアプリケーションを削除する流れ

特定のアプリケーションが不要になった場合は、スマートデバイスからアプリケーションをアンインストールおよび削除し、JP1/ITDM2 - SDM からアプリケーションを削除します。

JP1/ITDM2 - SDM から不要となったアプリケーションを削除する流れを次に示します。

1. スマートデバイスのアプリケーションについて削除、およびアンインストールを指示する
2. 配布アプリケーションを JP1/ITDM2 - SDM から削除する
3. 不要となったアプリケーションを通信サーバから削除する

> **メモ**
>
> 簡易配布の場合、この作業は不要です。

**関連項目**

- 9.4 アプリケーションを JP1/ITDM2 - SDM から削除する手順
- 9.5 不要となったアプリケーションを通信サーバから削除する手順
- 9.8 Android 端末に配布したアプリケーションをアンインストールする手順
- 9.10 iOS 端末に配布したアプリケーションをアンインストールする手順

## 4.13　セキュリティのルールの管理について

組織のセキュリティ方針を基にセキュリティのルールを作成して、スマートデバイスを管理します。セキュリティのルールに違反した利用があると、JP1/ITDM2 - SDM のイベントが発行されます。管理者は発行されたイベントを確認することで、スマートデバイスの不正利用を検知できます。

セキュリティのルールの管理方法について次に示します。

セキュリティのルールを登録する

組織のセキュリティ方針を基にセキュリティのルールを登録します。セキュリティのルールは複数登録できます。部署ごとに異なるセキュリティのルールを登録したり、特別な管理が必要なスマートデバイスのセキュリティのルールを登録したりできます。

セキュリティのルールをスマートデバイスに適用する

セキュリティのルールを適用すると、管理者はスマートデバイスのセキュリティ状況を把握したり、スマートデバイスの機能を業務に必要なものだけに制限したりできます。

セキュリティのルールを編集する

組織のセキュリティ方針が変更になった場合は、セキュリティのルールを編集します。

セキュリティのルールを削除する

管理体制の変更やセキュリティのルールの統合に伴って、不要になったセキュリティのルールがある場合は削除します。

**関連項目**

- 2.4 セキュリティの管理
- 4.13.1 Android ポリシーを適用する流れ
- 4.13.2 iOS プロファイルを適用する流れ
- 7.1 セキュリティポリシーを利用する
- 7.2 Android ポリシーを利用する
- 7.3 iOS プロファイルを利用する

## 4.13.1　Android ポリシーを適用する流れ

Android ポリシーを、Android 端末に適用します。

Android ポリシーを、Android 端末に適用する流れを次に示します。

1. 組織のセキュリティ方針を基に、Android ポリシーの内容を策定する
2. Android ポリシーを追加する
3. Android 端末に Android ポリシーを適用する

1 回の適用で対象とする Android 端末は 50 台程度とすることをお勧めします。

4. Android ポリシーの適用結果を確認する

   適用結果は、スマートデバイス画面の［セキュリティ］タブの［Android ポリシー/iOS プロファイル適用日時］が適用操作以降の日時になっているかで確認できます。また、適用対象の Android 端末が多い場合は、`sdmioutils exportdevice` コマンドで確認することをお勧めします。

   適用できなかった Android 端末に対しては、再度適用を実施してください。

**関連項目**

- 7.2.1 Android ポリシーを追加する手順
- 7.2.4 Android ポリシーを適用する手順
- 15. sdmioutils exportdevice（スマートデバイス情報のエクスポート）

## 4.13.2 iOS プロファイルを適用する流れ

iOS プロファイルを、複数の iOS 端末に一括して適用します。

パスワード付きロックが設定されている iOS 端末にプロファイルを適用するには、iOS プロファイルの適用時に iOS 端末のロックが解除されている必要があります。

定期的にリトライが実施されますが、全台に適用されるまでには時間がかかるため、余裕を持った適用計画を立ててください。

iOS プロファイルを適用する流れを次に示します。

1. 組織のセキュリティ方針を基に、iOS プロファイルの内容を策定する
2. Apple Configurator を使用して iOS プロファイルを作成する
3. iOS プロファイルを追加する
4. iOS 端末に iOS プロファイルを適用する

   1 回の指示で対象とする iOS 端末は 50 台程度とすることをお勧めします。

5. iOS プロファイルの適用結果を確認する

   適用結果は、スマートデバイス画面の［セキュリティ］タブの［Android ポリシー/iOS プロファイル適用日時］が適用操作以降の日時になっているかで確認できます。また、適用対象の iOS 端末が多い場合は、`sdmioutils exportdevice` コマンドで確認することをお勧めします。

   適用指示後、24 時間経過しても適用されない場合は、適用失敗となります。適用できなかった iOS 端末に対しては、再度適用を実施してください。

**関連項目**

- 7.3.1 iOS プロファイルを追加する手順
- 7.3.4 iOS プロファイルを適用する手順

- 15. sdmioutils exportdevice（スマートデバイス情報のエクスポート）

## 4.14　スマートデバイス紛失時の対処について

利用者がスマートデバイスを紛失した場合は、紛失したスマートデバイスをロック、または初期化します。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格納されている機密情報の漏えいにつながるおそれがあります。スマートデバイスの紛失が発生した場合はすぐに対策が必要です。

スマートデバイスの紛失に対処する方法には、次の 2 種類があります。

紛失したスマートデバイスをロックする

スマートデバイスをロックして使用できない状態にします。この方法は、スマートデバイスの拾得者が不正にスマートデバイスを操作できないようにする場合に適用します。

紛失したスマートデバイスをロックしただけでは、スマートデバイス内の情報は削除されません。拾得者にロックを解除された場合、情報漏えいにつながるおそれがあります。

紛失したスマートデバイスを初期化する

スマートデバイスを初期化し、工場出荷状態にします。紛失したスマートデバイスを初期化すると、スマートデバイス内の情報は削除されます。この方法は、主に次の場合に適用します。

- 紛失したあと、一定期間が経過してもスマートデバイスが発見されない場合
- 情報漏えいの防止を最優先にする場合

**関連項目**

- 4.14.1 紛失したスマートデバイスをロックする流れ
- 4.14.2 紛失したスマートデバイスを初期化する流れ

## 4.14.1　紛失したスマートデバイスをロックする流れ

スマートデバイスの紛失に対して、スマートデバイスをロックし、使用できない状態にします。

スマートデバイスをロックする流れを次に示します。

1. 利用者からスマートデバイスを紛失した旨の連絡を受ける

   連絡を受けた際、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を特定する

   入手した情報を基に、スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］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表示する情報を絞り込めます。

3. スマートデバイスをロックする

**関連項目**

- 8.8 スマートデバイスをロックする手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.14.2 紛失したスマートデバイスを初期化する流れ

スマートデバイスの紛失に対して、スマートデバイスを初期化し、工場出荷状態にします。

スマートデバイスを初期化する流れを次に示します。

1. 利用者からスマートデバイスを紛失した旨の連絡を受ける
   連絡を受けた際、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を特定する
   入手した情報を基に、スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］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表示する情報を絞り込めます。
3. スマートデバイスを初期化する

**関連項目**

- 8.7 スマートデバイスを初期化する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.15　利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合の対処について

利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合、JP1/ITDM2 - SDM（スマートデバイスエージェント）によってスマートデバイスが初期化されているかどうかで、対処方法が異なります。

スマートデバイスが初期化されていない場合

利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合、管理者が Android 端末のパスワードを変更、または iOS 端末のパスコードをリセットします。そのあと、利用者に Android 端末のパスワードまたは iOS 端末のパスコードを再設定するように指示します。

スマートデバイスが初期化されている場合

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、JP1/ITDM2 - SDM（スマートデバイスエージェント）によってスマートデバイスが初期化される場合があります。初期化されたスマートデバイスを利用するには、再度 JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する必要があります。

**関連項目**

- 4.15.1 Android 端末のパスワードを変更する流れ
- 4.15.2 iOS 端末のパスコードをリセットする流れ
- 4.15.3 JP1/ITDM2 - SDM（スマートデバイスエージェント）によって初期化されたスマートデバイスを管理対象にする流れ

### 4.15.1　Android 端末のパスワードを変更する流れ

利用者が Android 端末のパスワードを忘れた場合、管理者が Android 端末のパスワードを変更します。そのあと、利用者に Android 端末のパスワードを再設定するように指示します。

Android 端末のパスワードを変更する流れを次に示します。

1. 利用者から Android 端末のパスワードを忘れた旨の連絡を受ける

   連絡を受けた際、Android 端末を特定するために、利用者名、契約電話番号などの情報を入手します。
2. Android 端末を特定する

   入手した情報を基に、スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］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表示する情報を絞り込めます。
3. Android 端末のパスワードを変更する
4. パスワードを変更した Android 端末の利用者に、変更したパスワードを連絡し、パスワードを再設定するように指示する

**関連項目**

- 8.9 Android 端末のパスワードを変更する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.15.2 iOS 端末のパスコードをリセットする流れ

利用者が iOS 端末のパスコードを忘れた場合、管理者が iOS 端末のパスコードをリセットします。そのあと、利用者に iOS 端末のパスコードを再設定するように指示します。

iOS 端末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 iOS 端末のパスコードを忘れた旨の連絡を受ける
   連絡を受けた際、iOS 端末を特定するために、利用者名、契約電話番号などの情報を入手します。
2. iOS 端末を特定する
   入手した情報を基に、スマートデバイス画面の［スマートデバイス］－［管理対象のスマートデバイス一覧］で iOS 端末を特定します。このとき、フィルタを利用すると表示する情報を絞り込めます。
3. iOS 端末のパスコードをリセットする
4. パスコードをリセットされた iOS 端末の利用者に、パスコードを再設定するように指示する

**関連項目**

- 8.10 iOS 端末のパスコードをリセットする手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.15.3 JP1/ITDM2 - SDM（スマートデバイスエージェント）によって初期化されたスマートデバイスを管理対象にする流れ

利用者がスマートデバイスに間違ったパスワードを連続で入力した場合、JP1/ITDM2 - SDM（スマートデバイスエージェント）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 JP1/ITDM2 - SDM で管理するには、スマートデバイスを JP1/ITDM2 - SDM の管理対象にする必要があります。

初期化されたスマートデバイスを管理対象に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
   連絡を受けた際、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、スマートデバイス画面の［スマートデバイス］－［管理対象外のスマートデバイス一覧］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表示する情報を絞り込めます。

3. 特定したスマートデバイスの情報を確認する

   スマートデバイスの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も確認します。

4. 利用者からスマートデバイスを回収する
5. スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する
6. スマートデバイスに SSL 通信用ルート証明書を設定する（必要な証明書がプリインストールされていなかった場合だけ）
7. スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）をインストールする
8. スマートデバイスを新しい利用者に配布する
9. インベントリ情報が取得できるかを確認する

   スマートデバイスを配布したあと、スマートデバイスのインベントリ情報が JP1/ITDM2 - SDM に取得できるかを確認します。取得できない場合は、JP1/ITDM2 - SDM（スマートデバイスエージェント）が正しくインストールされているかを確認します。

**関連項目**

- 3.14.3 スマートデバイスにプリインストールされている SSL 通信用ルート証明書を確認する手順
- 3.14.4 Android 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.5 iOS 端末で SSL 通信用ルート証明書を設定する手順
- 3.14.6 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（Android 端末の場合）
- 3.14.7 Android 端末に JP1/ITDM2 - SDM（スマートデバイス Android エージェント）をインストールする手順（PC の場合）
- 3.14.8 iOS 端末に JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）をインストールする手順
- 8.6 スマートデバイスから最新のインベントリ情報を取得する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面

## 4.16　発生したイベントをメールで通知する流れ

JP1/ITDM2 - SDM で発生したイベントやスマートデバイスで発生したイベントを、管理者にメールで通知できます。

イベントをメールで通知する流れを次に示します。

1. イベント通知の設定をする
2. メールサーバを設定する
3. イベントメールフォーマット情報ファイルでイベントメールの形式を定義する

**関連項目**

- 11.1 イベント通知の設定をする手順
- 11.2 メールサーバを設定する手順
- 16.4 イベントメールフォーマット情報ファイル（eventmail.properties）

# 5 操作を開始・終了する

ここでは、JP1/ITDM2 - SDM の操作を開始・終了する方法について説明します。

## 5.1　ログインする手順

ログイン画面では、ユーザーアカウントの認証に成功すると JP1/ITDM2 - SDM にログインできます。

### 操作手順

1. Web ブラウザのアドレスバーに次の URL を入力します。
   http://スマートデバイスマネージャーの 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※/jp1itdm2sdm/
   注※　デフォルトのポート番号は「26080」です。
   ログイン画面が表示されます。
2. ユーザー ID とパスワードを入力します。
   デフォルトのユーザー ID は「system」、パスワードは「manager」です。
3. [ログイン] ボタンをクリックします。
   ビルトインアカウントのデフォルトの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。

### 操作結果

ユーザーアカウントの認証に成功すると操作画面が表示されます。

**ヒント**

パスワードの有効期限は、設定日から 180 日間です。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。設定日から 180 日が経過すると、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。

**重要**

続けて 3 回、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。

### 関連項目

- 2.3.1 ユーザーアカウントのロック
- 5.2 ユーザーアカウント情報を設定する手順
- 5.3 デフォルトパスワードを変更する手順
- 6.7 ユーザーアカウントのロックを解除する手順
- 14.2 ログイン画面

- 14.2.1 ［パスワードの変更］ダイアログ
- 付録 C ポート番号一覧

## 5.2　ユーザーアカウント情報を設定する手順

JP1/ITDM2 - SDM 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、ユーザーアカウント情報を設定してください。

### 操作手順

1. [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ます。
2. 表示されるダイアログでログインしているユーザーアカウントの情報を設定し、[OK] ボタンをクリックします。

> **ヒント**
>
> 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］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。

> **ヒント**
>
> ユーザーアカウントにメールアドレスを設定すると、そのメールアドレスに対してイベントの発生を通知できます。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、メールアドレスの設定を推奨します。なお、イベントの発生の通知を受け取るには、メールアドレスの設定のほかに、イベント通知の設定が必要です。

### 関連項目

- 6.1 ユーザーアカウントを追加する手順
- 11.1 イベント通知の設定をする手順
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 5.3　デフォルトパスワードを変更する手順

JP1/ITDM2 - SDM 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、デフォルトパスワードの変更が要求されます。

### 操作手順

1. ビルトインアカウント、または新規に作成したユーザーアカウントでログインします。
2. 表示されるダイアログでパスワードを変更し、［OK］ボタンをクリックします。

> **重要**
>
> 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。変更後のパスワードは次回ログイン時から適用されます。

> **ヒント**
>
> パスワードの有効期限は、設定日から 180 日間です。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。設定日から 180 日が経過すると、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。

### 関連項目

- 5.1 ログインする手順
- 14.2.1 ［パスワードの変更］ダイアログ

## 5.4　ログアウトする手順

JP1/ITDM2 - SDM 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。

### 操作手順

1. [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。

> **ヒント**
>
> 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。

### 関連項目

- 5.1 ログインする手順

# 6 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。

# 6.1　ユーザーアカウントを追加する手順

JP1/ITDM2 - SDM でスマートデバイスを複数人で管理する場合などに、管理者のユーザーアカウントを追加できます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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。

> **ヒント**
>
> 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。

### 操作結果

ユーザーアカウントが追加され、［ユーザーアカウントの管理］画面に表示されます。

### 関連項目

- 2.3.2 ユーザーアカウントの権限
- 2.3.3 参照権限で実行できない操作一覧
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.2 ［ユーザーアカウントの追加］ダイアログ

## 6.2　自分のユーザーアカウントを編集する手順

自分のユーザーアカウントのパスワードや権限などを変更したい場合に、ユーザーアカウントの情報を編集できます。

### 操作手順

1. 画面上部の［実行］メニューから［自分のアカウント編集］を選択します。
   ［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も同じダイアログが表示されます。
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。

### 関連項目

- 2.3.2 ユーザーアカウントの権限
- 2.3.3 参照権限で実行できない操作一覧
- 6.3 ほかの管理者のユーザーアカウントを編集する手順
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 6.3　ほかの管理者のユーザーアカウントを編集する手順

ほかの管理者のユーザーアカウントのパスワードや権限など、ユーザーアカウントの情報を編集できます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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。

### 関連項目

- 2.3.2 ユーザーアカウントの権限
- 2.3.3 参照権限で実行できない操作一覧
- 6.2 自分のユーザーアカウントを編集する手順
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 6.4　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。ただし、ビルトインアカウントとログイン中のユーザーアカウントは削除できません。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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。

   ユーザーアカウントは複数選択できます。
4. 表示されるダイアログで［OK］ボタンをクリックします。

### 関連項目

- 14.8.1 ［ユーザーアカウントの管理］画面

## 6.5　自分のパスワードを変更する手順

［パスワードの変更］ダイアログが表示されるのとは別に、自分のユーザーアカウントのパスワードを、必要に応じて変更できます。

**操作手順**

1. 画面上部の［実行］メニューから［自分のアカウント編集］を選択します。
   ［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も同じダイアログが表示されます。
2. 表示されるダイアログの［パスワードを変更する］をチェックします。
3. ［パスワード］および［パスワード確認］を入力して、［OK］ボタンをクリックします。

> **ヒント**
>
> パスワードの有効期限は、設定日から 180 日間です。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。設定日から 180 日が経過すると、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。

**関連項目**

- 6.6 ほかの管理者のパスワードを初期化する手順
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 6.6　ほかの管理者の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などに、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。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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の［パスワードを変更する］をチェックします。
5. ［パスワード］と［パスワード確認］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のパスワードが変更されます。
6. 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/ITDM2 - SDM 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。

### 関連項目

- 6.5 自分のパスワードを変更する手順
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 6.7　ユーザーアカウントのロックを解除する手順

3 回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。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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. 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］の［解除］を選択し、［OK］ボタンをクリックします。

> **ヒント**
>
> システム管理権限を持つ別のユーザーアカウントがない場合は、スマートデバイスマネージャーを再起動してください。スマートデバイスマネージャーを再起動するとユーザーアカウントのロックが解除されます。

### 関連項目

- 2.3.1 ユーザーアカウントのロック
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

# 7 セキュリティ状況を管理する

ここでは、組織内のスマートデバイス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。

## 7.1　セキュリティポリシーを利用する

スマートデバイスの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が必要です。セキュリティポリシーには、利用を監視する電話番号、Web サイト、およびアプリケーションを設定できます。ここでは、セキュリティポリシーを利用する手順について説明します。

### 7.1.1　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一覧］画面に、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を、スマートデバイスに適用することで、対象のスマートデバイスの利用状況を監視できるようになります。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

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］－［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. ［セキュリティポリシーの追加］ダイアログ上部の［セキュリティポリシー名］を入力します。
5. ［セキュリティポリシーの追加］ダイアログ左側のセキュリティ設定項目で、［電話番号］、［Web サイト］または［アプリケーション］を選択します。
6. ［追加］ボタンをクリックします。
7. 表示されたダイアログでルールを設定し、［OK］ボタンをクリックします。

> **ヒント**
>
> ［電話番号］および［URL］には、「*」（アスタリスク）を指定できます。例えば、［電話番号］に「1111111*」と入力した場合、上 7 桁が「1111111」で始まる電話番号が対象になります。なお、［電話番号］には「#」（シャープ）から始まる着信短縮ダイヤルも指定できます。

8. 設定したい項目に応じて手順 5～7 を繰り返します。
9. ［セキュリティポリシーの追加］ダイアログで［OK］ボタンをクリックします。

**操作結果**

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一覧］画面に表示されます。

**関連項目**

- 2.4.3 セキュリティポリシーに設定できる項目
- 7.1.2 セキュリティポリシーを編集する手順
- 7.1.3 セキュリティポリシーを削除する手順
- 7.1.4 セキュリティポリシーを適用する手順
- 14.4.1 ［セキュリティポリシー一覧］画面
- 14.4.2 ［セキュリティポリシーの追加］ダイアログ

## 7.1.2 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対策の傾向を取り入れる場合などに、セキュリティポリシーを編集できます。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

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］－［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. ［セキュリティポリシーの編集］ダイアログ左側のセキュリティ設定項目で、［電話番号］、［Web サイト］または［アプリケーション］を選択します。
5. 表示されたダイアログでルールを編集します。
   - 新しくルールを追加したい場合

     ［追加］ボタンをクリックし、表示されたダイアログでルールを追加し、［OK］ボタンをクリックします。
   - すでにあるルールを編集したい場合

     編集したいルールの［編集］ボタンをクリックし、表示されたダイアログでルールを編集し、［OK］ボタンをクリックします。
   - すでにあるルールを削除したい場合

     削除したいルールを選択し、［削除］ボタンをクリックし、表示されたダイアログで［OK］ボタンをクリックします。ルールは複数選択できます。

**ヒント**

［電話番号］および［URL］には、「*」（アスタリスク）を指定できます。例えば、［電話番号］に「1111111*」と入力した場合、上7桁が「1111111」で始まる電話番号が対象になります。なお、［電話番号］には「#」（シャープ）から始まる着信短縮ダイヤルも指定できます。

**ヒント**

［通話履歴］タブ、［WEB 閲覧履歴］タブ、および［ソフトウェア］タブの操作メニューからもセキュリティポリシーにルールを追加できます。

6. 編集したい項目に応じて手順 4〜5 を繰り返します。

7. ［セキュリティポリシーの編集］ダイアログで［OK］ボタンをクリックします。

**関連項目**

- 2.4.3 セキュリティポリシーに設定できる項目
- 7.1.1 セキュリティポリシーを追加する手順
- 7.1.3 セキュリティポリシーを削除する手順
- 7.1.4 セキュリティポリシーを適用する手順
- 14.4.1 ［セキュリティポリシー一覧］画面
- 14.4.3 ［セキュリティポリシーの編集］ダイアログ

## 7.1.3 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スマートデバイスの削減などで、不要になったセキュリティポリシーを削除できます。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 削除するセキュリティポリシーが適用されているスマートデバイスに、別のセキュリティポリシーを適用しておく必要があります。

**操作手順**

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］ − ［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、［削除］ボタンをクリックします。
   セキュリティポリシーは複数選択できます。
4. 表示されるダイアログで［OK］ボタンをクリックします。

**関連項目**

- 7.1.1 セキュリティポリシーを追加する手順
- 7.1.2 セキュリティポリシーを編集する手順
- 14.4.1 ［セキュリティポリシー一覧］画面

## 7.1.4 セキュリティポリシーを適用する手順

スマートデバイスの利用状況を監視したい場合は、セキュリティポリシーを適用します。適用したセキュリティポリシーに基づいて、スマートデバイスの不正利用などを把握できるようになります。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアの［スマートデバイス］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適用したいスマートデバイスを選択します。
   スマートデバイスは複数選択できます。

> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。

4. ［操作メニュー］の［セキュリティポリシーを適用する］を選択します。
5. 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て、［OK］ボタンをクリックします。

**関連項目**

- 7.1.1 セキュリティポリシーを追加する手順
- 7.1.2 セキュリティポリシーを編集する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

- 14.5.9 ［セキュリティポリシーを適用する］ダイアログ

## 7.2　Android ポリシーを利用する

Android 端末のセキュリティ状況を管理するためには Android ポリシーが必要です。Android ポリシーでは、パスワードのルールを設定したり、カメラ機能の利用を制限したりできます。ここでは Android ポリシーを利用する手順について説明します。

### 7.2.1　Android ポリシーを追加する手順

セキュリティ画面の［Android ポリシー一覧］画面に、Android ポリシーを追加できます。追加した Android ポリシーを、Android 端末に適用することで、対象の Android 端末の利用状況を監視できるようになります。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

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］－［Android 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ルールを設定して、［OK］ボタンをクリックします。

**操作結果**

Android ポリシーが追加され、［Android ポリシー一覧］画面に表示されます。

**関連項目**

- 2.4.5 Android ポリシーに設定できる項目
- 7.2.2 Android ポリシーを編集する手順
- 7.2.3 Android ポリシーを削除する手順
- 7.2.4 Android ポリシーを適用する手順
- 14.4.11 ［Android ポリシー一覧］画面
- 14.4.12 ［Android ポリシーの追加］ダイアログ

### 7.2.2　Android 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対策の傾向を取り入れる場合などに、Android ポリシーを編集できます。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

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］－［Android 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 Android 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ルールを編集して、［OK］ボタンをクリックします。

**関連項目**

- 2.4.5 Android ポリシーに設定できる項目
- 7.2.1 Android ポリシーを追加する手順
- 7.2.3 Android ポリシーを削除する手順
- 7.2.4 Android ポリシーを適用する手順
- 14.4.11 ［Android ポリシー一覧］画面
- 14.4.13 ［Android ポリシーの編集］ダイアログ

## 7.2.3 Android 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 Android 端末の削減などで不要になった Android ポリシーを削除します。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 削除する Android ポリシーが適用されている Android 端末に、別の Android ポリシーを適用しておく必要があります。

**操作手順**

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］－［Android 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 Android ポリシーを選択し、［削除］ボタンをクリックします。
   Android ポリシーは複数選択できます。
4. 表示されるダイアログで［OK］ボタンをクリックします。

**関連項目**

- 7.2.1 Android ポリシーを追加する手順
- 7.2.2 Android ポリシーを編集する手順
- 14.4.11 ［Android ポリシー一覧］画面

## 7.2.4 Android ポリシーを適用する手順

Android 端末の利用状況を監視したい場合は、Android ポリシーを適用します。適用した Android ポリシーに基づいて、Android 端末の不正利用などを把握できるようになります。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアの［スマートデバイス］を選択します。
3. インフォメーションエリアで Android ポリシーを適用したい Android 端末を選択します。
   Android 端末は複数選択できます。

   > **ヒント**
   >
   > フィルタを利用すると表示する情報を絞り込めます。

4. ［操作メニュー］の［Android ポリシーを適用する］を選択します。
5. 表示されるダイアログで Android ポリシーを選択して、［OK］ボタンをクリックします。

**操作結果**

Android 端末への適用が完了すると、［セキュリティ］タブの［Android ポリシー/iOS プロファイル適用日時］が更新されます。

**関連項目**

- 7.2.1 Android ポリシーを追加する手順
- 7.2.2 Android ポリシーを編集する手順
- 14.4.11 ［Android ポリシー一覧］画面
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.2 ［管理対象のスマートデバイス一覧］画面で表示されるタブ
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

- 14.5.10 ［Android ポリシーを適用する］ダイアログ

## 7.3　iOS プロファイルを利用する

iOS 端末のセキュリティ状況を管理するためには iOS プロファイルが必要です。iOS プロファイルでは、パスコードのルールを設定したり、カメラ機能の利用を制限したりできます。ここでは iOS プロファイルを利用する手順について説明します。

### 7.3.1　iOS プロファイルを追加する手順

セキュリティ画面の［iOS プロファイル一覧］画面に、iOS プロファイルを追加できます。追加した iOS プロファイルを、iOS 端末に適用することで、対象の iOS 端末の利用状況を監視できるようになります。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- Apple 社が提供する iPhone 構成ユーティリティを使用して、事前にプロファイルを作成しておく必要があります。

**操作手順**

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］－［iOS プロファイル一覧］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プロファイル名、インポートファイルのファイルパスを設定します。
5. ［OK］ボタンをクリックします。

**操作結果**

iOS プロファイルが追加され、［iOS プロファイル一覧］画面に表示されます。

**関連項目**

- 2.4.7 iOS プロファイルに設定できる項目について
- 7.3.2 iOS プロファイルをエクスポートする手順
- 7.3.3 iOS プロファイルを削除する手順
- 7.3.4 iOS プロファイルを適用する手順
- 14.4.15 ［iOS プロファイル一覧］画面
- 14.4.16 ［iOS プロファイルの追加］ダイアログ

## 7.3.2　iOS プロファイルをエクスポートする手順

iOS プロファイルを XML 形式でエクスポートできます。

### 操作手順

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］－［iOS プロファイル一覧］を選択します。
3. インフォメーションエリアで、エクスポートしたい iOS プロファイルの［エクスポート］ボタンをクリックします。
4. 表示された画面で、保存先とファイル名を指定し、［保存］ボタンをクリックします。

### 操作結果

指定した保存先に、指定したファイル名の iOS プロファイルが XML 形式で保存されます。

> **ヒント**
>
> エクスポートしたファイルは、拡張子を.mobileconfig に変更すると、Apple 社が提供する iPhone 構成ユーティリティにインポートできます。必要に応じて構成プロファイルを編集し、iOS プロファイルとして再度登録できます。

### 関連項目

- 7.3.1 iOS プロファイルを追加する手順
- 7.3.3 iOS プロファイルを削除する手順
- 7.3.4 iOS プロファイルを適用する手順
- 14.4.15 ［iOS プロファイル一覧］画面

## 7.3.3　iOS プロファイルを削除する手順

組織のセキュリティ方針の変更や管理対象の iOS 端末の削減などで、不要になった iOS プロファイルを削除します。

### 前提条件

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 削除する iOS プロファイルが適用されている iOS 端末に、別の iOS プロファイルを適用しておく必要があります。

**操作手順**

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］－［iOS プロファイル一覧］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 iOS プロファイルを選択し、［削除］ボタンをクリックします。
   iOS プロファイルは複数選択できます。
4. 表示されるダイアログで［OK］ボタンをクリックします。

**関連項目**

- 7.3.1 iOS プロファイルを追加する手順
- 7.3.2 iOS プロファイルをエクスポートする手順
- 14.4.15 ［iOS プロファイル一覧］画面

## 7.3.4 iOS プロファイルを適用する手順

iOS 端末の利用状況を監視したい場合は、iOS プロファイルを適用します。適用した iOS プロファイルに基づいて、iOS 端末の不正利用などを把握できるようになります。

> **メモ**
>
> iOS プロファイルの適用は、`sdmapplyprofile` コマンドでも実施できます。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- iOS プロファイルの適用時は iOS 端末のロックを解除しておく必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアの［スマートデバイス］を選択します。
3. インフォメーションエリアで、iOS プロファイルを適用したい iOS 端末を選択します。
   iOS 端末は複数選択できます。

   > **ヒント**
   >
   > フィルタを利用すると表示する情報を絞り込めます。

4. ［操作メニュー］の［iOS プロファイルを適用する］を選択します。

5. 表示されるダイアログで iOS プロファイルを選択して、［OK］ボタンをクリックします。

**操作結果**

iOS 端末への適用が完了すると、［セキュリティ］タブの［Android ポリシー/iOS プロファイル適用日時］が更新されます。

> **ヒント**
>
> 1 つの iSO 端末に対して、複数の iOS プロファイルを適用できます。

> **重要**
>
> iOS プロファイルの適用時は iOS 端末のロックを解除しておく必要があります。

**関連項目**

- 7.3.1 iOS プロファイルを追加する手順
- 7.3.2 iOS プロファイルをエクスポートする手順
- 7.3.3 iOS プロファイルを削除する手順
- 14.4.15 ［iOS プロファイル一覧］画面
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.2 ［管理対象のスマートデバイス一覧］画面で表示されるタブ
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面
- 14.5.11 ［iOS プロファイルの適用］ダイアログ

## 7.3.5 iOS プロファイルを適用解除する手順

適用する iOS プロファイルを変更したい場合は、iOS プロファイルの適用を解除します。

> **メモ**
>
> iOS プロファイルの適用解除は、`sdmapplyprofile` コマンドでも実施できます。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

1. スマートデバイス画面を表示します。

2. メニューエリアで［スマートデバイス］を選択します。

3. インフォメーションエリアで、iOS プロファイルの適用を解除したい iOS 端末を選択します。
   iOS 端末は複数選択できます。

> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。

4. ［操作メニュー］の［iOS プロファイルの適用を解除する］を選択します。

5. 表示されるダイアログで iOS プロファイルを選択して、［OK］ボタンをクリックします。

**関連項目**

- 7.3.3 iOS プロファイルを削除する手順
- 7.3.4 iOS プロファイルを適用する手順
- 14.4.15 ［iOS プロファイル一覧］画面
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.2 ［管理対象のスマートデバイス一覧］画面で表示されるタブ
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 7.3.6 iOS プロファイル情報を編集する手順

iOS プロファイル名や説明を変更したい場合に、iOS プロファイル情報を編集できます。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

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］－［iOS プロファイル一覧］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 iOS プロファイルの［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 iOS プロファイル名や説明を変更します。

5. ［OK］ボタンをクリックします。

**操作結果**

iOS プロファイル情報が変更され、［iOS プロファイル一覧］画面に反映されます。

**関連項目**

- 2.4.7 iOS プロファイルに設定できる項目について
- 7.3.1 iOS プロファイルを追加する手順
- 7.3.2 iOS プロファイルをエクスポートする手順
- 7.3.3 iOS プロファイルを削除する手順
- 7.3.4 iOS プロファイルを適用する手順
- 14.4.15 ［iOS プロファイル一覧］画面
- 14.4.17 ［iOS プロファイル情報の編集］ダイアログ

# 8 スマートデバイスを管理する

ここでは、組織内のスマートデバイス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。

## 8.1　スマートデバイスの JP1/ITDM2 - SDM への登録

管理対象としたいスマートデバイスを JP1/ITDM2 - SDM に登録します。

スマートデバイスを登録する方法には次の 2 種類があります。

- 手動でスマートデバイスを登録する方法
  スマートデバイスの情報を 1 台ずつ登録します。
- CSV ファイルでスマートデバイスを登録する方法
  複数のスマートデバイスの情報が入力された CSV ファイルをインポートし、一括登録します。

**関連項目**

- 2.5 スマートデバイスの管理
- 8.1.1 手動でスマートデバイスを登録する手順
- 8.1.2 CSV ファイルでスマートデバイスを登録する手順

### 8.1.1　手動でスマートデバイスを登録する手順

手動でスマートデバイスの情報を 1 台ずつ JP1/ITDM2 - SDM に登録します。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- スマートデバイスを管理対象として登録する場合は、セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを作成しておく必要があります。
- 次の情報を入手しておく必要があります。
  - 利用者名
  - 利用者の所属部署

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. ［操作メニュー］の［スマートデバイスを追加する］を選択します。
4. ［スマートデバイスの追加］ダイアログで、登録するスマートデバイスの情報を入力します。
   ダイアログ上部の［追加］ボタンをクリックすると、スマートデバイスの情報を入力できる行が追加され、複数のスマートデバイスの情報を登録できます。

**重要**

［名称］には、次に示す文字以外は使用できません。

- 0-9（ASCII コード 0x30-0x39）
- A-Z（ASCII コード 0x41-0x5a）
- a-z（ASCII コード 0x61-0x7a）
- _（アンダーバー）（ASCII コード 0x5f）
- -（ハイフン）（ASCII コード 0x2d）
- .（ピリオド）（ASCII コード 0x2e）

**重要**

［名称］に、すでに JP1/ITDM2 - SDM に登録されている名称を指定すると、登録済みのスマートデバイスの情報が上書きされます。

**ヒント**

［スマートデバイスの追加］ダイアログの［エクスポート］ボタンをクリックすることで、入力した情報を CSV ファイルで出力できます。

5. ［OK］ボタンをクリックします。

### 操作結果

JP1/ITDM2 - SDM にスマートデバイスが登録されます。なお、セキュリティのルールを適用したかによって、スマートデバイスの管理の状態が変わります。

- セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを入力し、登録した場合
  スマートデバイスが管理対象となり、［管理対象のスマートデバイス一覧］画面に表示されます。
- セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを入力しないで登録した場合
  スマートデバイスが管理対象外となり、［管理対象外のスマートデバイス一覧］画面に表示されます。

### 関連項目

- 8.1.2 CSV ファイルでスマートデバイスを登録する手順
- 8.2 スマートデバイス一覧をエクスポートする手順
- 8.3 管理対象外のスマートデバイスを管理対象にする
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

- 14.5.13 ［スマートデバイスの追加］ダイアログ

## 8.1.2 CSV ファイルでスマートデバイスを登録する手順

複数のスマートデバイスの情報が入力された CSV ファイルをインポートし、一括登録します。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- CSV ファイルを作成しておく必要があります。
- スマートデバイスを管理対象として登録する場合は、セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを作成しておく必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. ［操作メニュー］の［スマートデバイス一覧をインポートする］を選択します。
4. 表示されるダイアログで、スマートデバイスの情報が入力された CSV ファイルを選択し、［OK］ボタンをクリックします。

**重要**

CSV ファイルに指定する［名称］には、次に示す文字以外は使用できません。

- 0-9（ASCII コード 0x30-0x39）
- A-Z（ASCII コード 0x41-0x5a）
- a-z（ASCII コード 0x61-0x7a）
- _（アンダーバー）（ASCII コード 0x5f）
- -（ハイフン）（ASCII コード 0x2d）
- .（ピリオド）（ASCII コード 0x2e）

**重要**

CSV ファイルに指定する［名称］に、すでに JP1/ITDM2 - SDM に登録されている名称を指定すると、登録済みのスマートデバイスの情報が上書きされます。

### 操作結果

JP1/ITDM2 - SDM にスマートデバイスが登録されます。なお、セキュリティのルールを適用したかによって、スマートデバイスの管理の状態が変わります。

- セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを入力し、登録した場合
  スマートデバイスが管理対象となり、[管理対象のスマートデバイス一覧]画面に表示されます。
- セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを入力しないで登録した場合
  スマートデバイスが管理対象外となり、[管理対象外のスマートデバイス一覧]画面に表示されます。

### 関連項目

- 8.1.1 手動でスマートデバイスを登録する手順
- 8.2 スマートデバイス一覧をエクスポートする手順
- 8.3 管理対象外のスマートデバイスを管理対象にする
- 14.5.1 [管理対象のスマートデバイス一覧]画面
- 14.5.3 [管理対象外のスマートデバイス一覧]画面
- 14.5.13 [スマートデバイスの追加]ダイアログ
- 付録 E インポート・エクスポートファイルの出力形式

## 8.2　スマートデバイス一覧をエクスポートする手順

すべてのスマートデバイスを、CSV ファイルにエクスポートできます。エクスポートした CSV ファイルは、スマートデバイスを滅却する際のチェックリストなどとして使えます。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. ［操作メニュー］の［スマートデバイス一覧をエクスポートする］を選択します。
4. 表示された画面で、保存先とファイル名を指定し、［保存］ボタンをクリックします。

**操作結果**

指定した保存先に、指定したファイル名で CSV ファイルが保存されます。

> **ヒント**
>
> エクスポートした CSV ファイルは、編集してインポートできます。

**関連項目**

- 8.1.2 CSV ファイルでスマートデバイスを登録する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 付録 E インポート・エクスポートファイルの出力形式

## 8.3　管理対象外のスマートデバイスを管理対象にする

管理対象外として登録されているスマートデバイスに、セキュリティのルールを適用し、管理対象にします。スマートデバイスを管理対象とすることで、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ます。

なお、以前に管理対象だったスマートデバイスを再度管理対象とする場合は、スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にしたあと、スマートデバイス側で再度通信サーバへ接続するための設定が必要です。

**関連項目**

- 8.3.1 スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にする手順
- 8.3.2 Android 端末で再度管理対象とするための手順
- 8.3.3 iOS 端末で再度管理対象とするための手順

### 8.3.1　スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にする手順

管理対象外として登録されているスマートデバイスに、セキュリティのルールを適用し、管理対象にします。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- セキュリティポリシーおよび Android ポリシー、またはセキュリティポリシーおよび iOS プロファイルを追加しておく必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象外のスマートデバイス一覧］を選択します。
3. 管理対象とするスマートデバイスを選択します。
   スマートデバイスは複数選択できます。
4. ［操作メニュー］の［セキュリティポリシーを適用する］を選択します。
5. 表示されるダイアログで、適用する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。
6. ［操作メニュー］の［Android ポリシーを適用する］または［iOS プロファイルを適用する］を選択します。
   スマートデバイスの登録時に設定した OS の種類によって、［Android ポリシーを適用する］または［iOS プロファイルを適用する］のどちらかが選択できます。

7. 表示されるダイアログで、適用する Android ポリシー、または iOS プロファイルを選択して、[OK] ボタンをクリックします。

**操作結果**

選択したスマートデバイスが管理対象となり、[管理対象のスマートデバイス一覧] 画面に表示されます。

**関連項目**

- 2.5.1 管理対象のスマートデバイスの管理
- 8.3.2 Android 端末で再度管理対象とするための手順
- 8.3.3 iOS 端末で再度管理対象とするための手順
- 8.4 管理対象のスマートデバイスを管理対象外にする手順
- 14.5.1 [管理対象のスマートデバイス一覧] 画面
- 14.5.3 [管理対象外のスマートデバイス一覧] 画面
- 14.5.9 [セキュリティポリシーを適用する] ダイアログ
- 14.5.10 [Android ポリシーを適用する] ダイアログ
- 14.5.11 [iOS プロファイルの適用] ダイアログ

## 8.3.2 Android 端末で再度管理対象とするための手順

以前に管理対象だった Android 端末を再度管理対象とする場合は、スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にしたあと、Android 端末で通信サーバへの接続設定を行います。

**操作手順**

1. Android 端末で JP1/ITDM2 - SDM（スマートデバイス Android エージェント）を起動します。
2. [通信サーバ] をタップし、通信サーバ設定画面を開きます。
3. 通信サーバ設定画面で、接続先通信サーバホスト名および名称を入力し、[OK] ボタンをタップします。
   通信サーバには「**ホスト名:ポート番号**（デフォルト：26055）」の形式で指定してください。また、名称には、JP1/ITDM2 - SDM に登録したスマートデバイスの名称を指定してください。
   サーバに正常に接続できると、それを示すダイアログが表示されます。
4. ダイアログで [OK] ボタンをタップします。

**関連項目**

- 8.4 管理対象のスマートデバイスを管理対象外にする手順

## 8.3.3　iOS 端末で再度管理対象とするための手順

以前に管理対象だった iOS 端末を再度管理対象とする場合は、スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にしたあと、iOS 端末で通信サーバへの接続設定を行います。

### 操作手順

1. iOS 端末で［設定］－［一般］－［プロファイルとデバイス管理］の構成プロファイルを削除します。
   すでに削除されている場合は、この作業は不要です。
2. iOS 端末で JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）を起動します。
3. ［通信サーバ］をタップし、通信サーバ設定画面を開きます。
4. ［通信サーバを削除］をタップし、通信サーバ設定削除確認画面を開きます。
5. ［OK］ボタンをタップします。
6. ［確認］ダイアログで［OK］ボタンをタップします。
7. 通信サーバ設定画面で、接続先通信サーバホスト名および名称を入力し、［OK］ボタンをタップします。
   通信サーバには「**ホスト名:ポート番号**（デフォルト：26055）」の形式で指定してください。また、名称には、JP1/ITDM2 - SDM に登録したスマートデバイスの名称を指定してください。
   サーバに正常に接続できると、それを示すダイアログが表示されます。
8. ダイアログで［OK］ボタンをタップします。

### 関連項目

- 8.4 管理対象のスマートデバイスを管理対象外にする手順

## 8.4　管理対象のスマートデバイスを管理対象外にする手順

管理対象のスマートデバイスのうち、管理する必要がないスマートデバイスは、セキュリティのルールを外し、管理対象外にできます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. 管理対象外にするスマートデバイスを選択します。
   スマートデバイスは複数選択できます。
4. ［操作メニュー］の［管理対象外にする］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。

> **ヒント**
>
> ［強制的に管理対象外にする。］をチェックすると、スマートデバイスと接続できない場合でも強制的に管理対象外にできます。

### 操作結果

選択したスマートデバイスが管理対象外となり、［管理対象外のスマートデバイス一覧］画面に表示されます。

### 関連項目

- 2.5.2 管理対象外のスマートデバイスの管理
- 8.3 管理対象外のスマートデバイスを管理対象にする
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面
- 14.5.8 ［管理対象外にする］ダイアログ

# 8.5　スマートデバイスを JP1/ITDM2 - SDM から削除する手順

管理対象外のスマートデバイスのうち、故障や入れ替えのため不要になったスマートデバイスを JP1/ITDM2 - SDM から削除できます。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- スマートデバイスを管理対象外にする必要があります。
- スマートデバイスの初期化が必要な場合、JP1/ITDM2 - SDM から削除する前に初期化してください。スマートデバイスを JP1/ITDM2 - SDM から削除しても、スマートデバイスは初期化されません。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象外のスマートデバイス一覧］を選択します。
3. 削除するスマートデバイスを選択します。
   スマートデバイスは複数選択できます。
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。

**関連項目**

- 8.7 スマートデバイスを初期化する手順
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 8.6　スマートデバイスから最新のインベントリ情報を取得する手順

スマートデバイスから、最新のインベントリ情報を取得できます。

> **メモ**
>
> インベントリ情報の収集は、sdmgetinventory コマンドでも実施できます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］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スマートデバイスを選択します。
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. 表示されるダイアログで［OK］ボタンをクリックします。

### 操作結果

選択したスマートデバイスの［管理対象のスマートデバイス一覧］画面に表示されるタブの情報が更新されます。

### 関連項目

- 2.5.1 管理対象のスマートデバイスの管理
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.2 ［管理対象のスマートデバイス一覧］画面で表示されるタブ

## 8.7　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滅却する場合などに、スマートデバイスを初期化し、工場出荷状態にできます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. インフォメーションエリアで初期化するスマートデバイスを選択します。
   スマートデバイスは複数選択できます。
4. ［操作メニュー］の［初期化する］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。

> **重要**
>
> スマートデバイスを初期化すると、インストールされていた JP1/ITDM2 - SDM（スマートデバイスエージェント）は削除されます。また、セキュリティポリシーと Android ポリシー、またはセキュリティポリシーと iOS プロファイルの設定情報は破棄されます。

### 関連項目

- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.5 ［スマートデバイスの初期化］ダイアログ

## 8.8　スマートデバイスをロックする手順

スマートデバイスを紛失した場合などに、スマートデバイスをロックできます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］を選択します。
3. インフォメーションエリアでロックするスマートデバイスを選択します。
   スマートデバイスは複数選択できます。
4. ［操作メニュー］の［ロックする］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。

> **ヒント**
>
> Android 端末の場合、［スマートデバイスのロック］ダイアログでロックとパスワードの変更を同時にできます。

### 関連項目

- 8.9 Android 端末のパスワードを変更する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.6 ［スマートデバイスのロック］ダイアログ

## 8.9 Android 端末のパスワードを変更する手順

利用者がスマートデバイスのパスワードを忘れた場合などに、Android 端末をロックし、パスワードを変更できます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］－［Android スマートデバイス］を選択します。
3. インフォメーションエリアでロックする Android 端末を選択します。
   Android 端末は複数選択できます。
4. ［操作メニュー］の［ロックする］を選択します。
5. ［スマートデバイスのロック］ダイアログの［ロックするパスワードを変更する］をチェックします。
6. 新しいパスワードとパスワード確認を入力します。
7. ［OK］ボタンをクリックします。
   Android 端末がロックされ、パスワードが変更されます。
8. 利用者にパスワードを再設定するように連絡します。

> **重要**
>
> Android 端末を複数選択してパスワードを変更した場合、パスワードはすべて同一になります。異なるパスワードを設定したい場合は、1 台ずつパスワードを変更してください。

### 関連項目

- 8.10 iOS 端末のパスコードをリセットする手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.6 ［スマートデバイスのロック］ダイアログ

## 8.10　iOS 端末のパスコードをリセットする手順

iOS 端末の利用者がパスコードを忘れた場合などに、iOS 端末のパスコードをリセットできます。

**前提条件**

システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］－［iOS スマートデバイス］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する iOS 端末を選択します。
   iOS 端末は複数選択できます。
4. ［操作メニュー］の［パスコードをリセットする］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。
6. 利用者にパスコードを再設定するように連絡します。

**関連項目**

- 8.9 Android 端末のパスワードを変更する手順
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.7 ［スマートデバイスのパスコードのリセット］ダイアログ

## 8.11　Android 端末にメッセージを通知する手順

Android 端末の利用者に連絡事項などがある場合に、JP1/ITDM2 - SDM から Android 端末にメッセージを通知できます。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. スマートデバイス画面を表示します。
2. メニューエリアで［スマートデバイス］－［管理対象のスマートデバイス一覧］－［Android スマートデバイス］を選択します。
3. インフォメーションエリアで、メッセージを通知する Android 端末を選択します。
   Android 端末は複数選択できます。
4. ［操作メニュー］の［メッセージを通知する］を選択します。
5. 表示されるダイアログで、通知するメッセージを入力します。
6. ［OK］ボタンをクリックします。

### 関連項目

- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.15 ［スマートデバイスへのメッセージ通知］ダイアログ

## 8.12　スマートデバイスのログを取得する手順

スマートデバイスにインストールされている JP1/ITDM2 - SDM（スマートデバイスエージェント）が出力しているログを取得できます。

### 操作手順

1. スマートデバイスで JP1/ITDM2 - SDM（スマートデバイスエージェント）（アプリ名：JP1ITDM2SDM）を起動します。
2. [ログ送信] をタップします。

### 操作結果

スマートデバイスのログが次のファイルに格納されます。

JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥log¥agent¥名称※1_yyyyMMdd_hhmmss※2.log

注※1　選択したスマートデバイスの名称です。

注※2　yyyy：年、MM：月、dd：日、hh：時、mm：分、ss：秒

### 関連項目

- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 付録 F サポートに必要な情報の格納先または入手方法

# 9 アプリケーションを管理する

ここでは、JP1/ITDM2 - SDM でアプリケーションを管理する方法について説明します。

## 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順

アプリケーションをスマートデバイスに配布したい場合に、配布するアプリケーションを JP1/ITDM2 - SDM に登録します。

> **重要**
>
> 運用中に標準配布から簡易配布に切り替える場合、すべてのアプリケーションを再登録する必要があります。

**前提条件**

- 登録できるアプリケーションは Android アプリケーション（拡張子が.apk のファイル）および iOS アプリケーション（拡張子が.ipa のファイル）です。
- システム管理権限を持つユーザーアカウントでログインする必要があります。

**操作手順**

1. 配布画面を表示します。
2. メニューエリアで［Android アプリケーション］または［iOS アプリケーション］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、アプリケーションの情報を入力して、［OK］ボタンをクリックします。

> **重要**
>
> パッケージ名には、次の文字は指定できません。
>
> 「<」、「>」、「&」、「|」、「^」、「%」

> **ヒント**
>
> 利用者の操作でインストールできるアプリケーションとして設定する場合、スマートデバイスで表示されるアプリケーションの説明には、［説明］に入力した内容が表示されます。
>
> スマートデバイスで、アプリケーションの説明は最大 5 行まで表示されますが、表示できる文字数はスマートデバイスの機種に依存します。［説明］は、100 文字以内で入力することをお勧めします。

**操作結果**

配布するアプリケーションが JP1/ITDM2 - SDM に登録され、登録したアプリケーションの情報が配布画面に表示されます。

**重要**

iOS アプリケーション（in-house、internal use applications）を配布する場合、iOS アプリケーションは Apple Developer Enterprise Program ライセンスが定める範囲で利用してください。

**関連項目**

- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.3 登録したアプリケーションの情報を編集する手順
- 9.4 アプリケーションを JP1/ITDM2 - SDM から削除する手順
- 9.6 Android 端末にアプリケーションを配布する手順
- 9.9 iOS 端末にアプリケーションのインストールを指示する手順
- 9.11 利用者の操作でインストールできるアプリケーションを管理する
- 9.12 Android 端末から利用者の操作でアプリケーションをインストールする手順
- 9.13 iOS 端末から利用者の操作でアプリケーションをインストールする手順
- 14.6.1 ［配布アプリケーション一覧］画面
- 14.6.2 ［Android アプリケーション］画面
- 14.6.4 ［iOS アプリケーション］画面
- 14.6.6 ［Android アプリケーションの追加］ダイアログ
- 14.6.9 ［iOS アプリケーションの追加］ダイアログ

## 9.2 配布するアプリケーションを通信サーバに配置する手順

配布するアプリケーションを JP1/ITDM2 - SDM に登録したあと、通信サーバにアプリケーションを配置します。

> **メモ**
>
> 簡易配布の場合、この操作は不要です。

### 前提条件

- 配置できるアプリケーションは Android アプリケーション（拡張子が.apk のファイル）および iOS アプリケーション（拡張子が.ipa のファイル）です。
- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。

### 操作手順

1. 配布するアプリケーションを通信サーバの次のフォルダに配置します。

```
JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥htdocs¥download
```

2. ファイル名を次の規則に従ってリネームします。

| アプリケーション | ファイル名 |
|---|---|
| Android アプリケーション | パッケージ名バージョン.apk |
| iOS アプリケーション | パッケージ名バージョン.ipa |

パッケージ名

配布するアプリケーションを JP1/ITDM2 - SDM に登録するときのアプリケーション情報入力時に指定したパッケージ名を指定します。

バージョン

配布するアプリケーションを JP1/ITDM2 - SDM に登録するときのアプリケーション情報入力時に指定したバージョンを指定します。

（例）iOS アプリケーション（パッケージ名「packageA」、バージョン「1.0」）の場合

```
packageA1.0.ipa
```

### 関連項目

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順

## 9.3　登録したアプリケーションの情報を編集する手順

登録したアプリケーションの情報を編集します。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［配布アプリケーション一覧］を選択します。

> **ヒント**
>
> メニューエリアで［Android アプリケーション］または［iOS アプリケーション］を選択すると、表示するアプリケーションをアプリケーションの種類で絞り込めます。

3. インフォメーションエリアで編集したいアプリケーションの［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、アプリケーションの情報を編集して、［OK］ボタンをクリックします。

> **重要**
>
> アプリケーションの情報の編集でパッケージ名を変更した場合、通信サーバに配置しているアプリケーションのファイル名を変更する必要があります。

> **ヒント**
>
> 利用者の操作でインストールできるアプリケーションとして設定する場合、スマートデバイスで表示されるアプリケーションの説明には、［説明］に入力した内容が表示されます。
>
> スマートデバイスで、アプリケーションの説明は最大 5 行まで表示されますが、表示できる文字数はスマートデバイスの機種に依存します。［説明］は、100 文字以内で入力することをお勧めします。

### 関連項目

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.4 アプリケーションを JP1/ITDM2 - SDM から削除する手順
- 9.6 Android 端末にアプリケーションを配布する手順
- 9.9 iOS 端末にアプリケーションのインストールを指示する手順
- 9.11 利用者の操作でインストールできるアプリケーションを管理する

- 9.12 Android 端末から利用者の操作でアプリケーションをインストールする手順
- 9.13 iOS 端末から利用者の操作でアプリケーションをインストールする手順
- 14.6.1 ［配布アプリケーション一覧］画面
- 14.6.2 ［Android アプリケーション］画面
- 14.6.4 ［iOS アプリケーション］画面
- 14.6.7 ［Android アプリケーションの編集］ダイアログ
- 14.6.10 ［iOS アプリケーションの編集］ダイアログ

## 9.4　アプリケーションを JP1/ITDM2 - SDM から削除する手順

アプリケーションが不要になった場合などは、アプリケーションを JP1/ITDM2 - SDM から削除します。

### 前提条件

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 削除するアプリケーションが配布、またはインストールされているスマートデバイスに、削除するアプリケーションのアンインストールを指示してください。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［配布アプリケーション一覧］を選択します。

> **ヒント**
>
> メニューエリアで［Android アプリケーション］または［iOS アプリケーション］を選択すると、表示するアプリケーションをアプリケーションの種類で絞り込めます。

3. インフォメーションエリアで削除するアプリケーションを選択します。
4. インフォメーションエリア上部の［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。

### 関連項目

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.3 登録したアプリケーションの情報を編集する手順
- 9.5 不要となったアプリケーションを通信サーバから削除する手順
- 9.8 Android 端末に配布したアプリケーションをアンインストールする手順
- 9.10 iOS 端末に配布したアプリケーションをアンインストールする手順
- 14.6.1 ［配布アプリケーション一覧］画面
- 14.6.2 ［Android アプリケーション］画面
- 14.6.4 ［iOS アプリケーション］画面

## 9.5　不要となったアプリケーションを通信サーバから削除する手順

不要となったアプリケーションを通信サーバから削除します。

> **メモ**
>
> 簡易配布の場合、この操作は不要です。

### 前提条件

- 不要となったアプリケーションを JP1/ITDM2 - SDM から削除しておく必要があります。
- 通信サーバのサービスは起動しておく必要があります。

### 操作手順

1. 通信サーバの次のフォルダから、不要となったアプリケーションを削除します。

   **JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ**¥cms¥uC¥httpsd¥htdocs¥download

   アプリケーションのファイル名を次に示します。

| アプリケーション | ファイル名 |
|---|---|
| Android アプリケーション | パッケージ名バージョン.apk |
| iOS アプリケーション | パッケージ名バージョン.ipa |

   （例）iOS アプリケーション（パッケージ名「packageA」、バージョン「1.0」）の場合

   ```
   packageA1.0.ipa
   ```

   > **メモ**
   >
   > アプリケーションの削除後、通信サーバのサービスの再起動は不要です。

### 関連項目

- 9.8 Android 端末に配布したアプリケーションをアンインストールする手順
- 9.10 iOS 端末に配布したアプリケーションをアンインストールする手順

## 9.6 Android 端末にアプリケーションを配布する手順

利用者に必要に応じてアプリケーションのインストールをしてほしい場合などに、アプリケーションを管理対象の Android 端末に配布します。

> **メモ**
>
> アプリケーションの配布は、sdmdistributeapp コマンドでも実施できます。

### 前提条件

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。
- 配布するアプリケーションを通信サーバに配置しておく必要があります。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［Android アプリケーション］を選択します。
3. インフォメーションエリアで配布するアプリケーションを選択します。
4. アプリケーションを配布する Android 端末を、インフォメーションエリア下部、［未配布スマートデバイス一覧］タブから選択します。
   Android 端末は複数選択できます。
5. インフォメーションエリア下部の操作メニューから［アプリケーション配布］を選択します。
6. 表示されるダイアログで［OK］ボタンをクリックします。

### 操作結果

選択した Android 端末にアプリケーションが配布されます。利用者が配布された未インストール配布アプリケーション一覧からインストールできます。

アプリケーションが配布されると、［Android アプリケーション］画面のインフォメーションエリア下部、［配布済みスマートデバイス一覧］タブに Android 端末の情報が表示されます。

### 関連項目

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.3 登録したアプリケーションの情報を編集する手順
- 9.7 Android 端末にアプリケーションのインストールを指示する手順

- 14.6.2 ［Android アプリケーション］画面

## 9.7 Android 端末にアプリケーションのインストールを指示する手順

Android 端末にアプリケーションをインストールするよう利用者に指示します。なお、配布していないアプリケーションについてインストールを指示する場合は、アプリケーションの配布とインストールの指示が実行されます。

> **メモ**
>
> アプリケーションの配布とインストールの指示は、sdmdistributeapp コマンドでも実施できます。

**前提条件**

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。
- 配布するアプリケーションを通信サーバに配置しておく必要があります。

**操作手順**

1. 配布画面を表示します。
2. メニューエリアで［Android アプリケーション］を選択します。
3. インフォメーションエリアでインストールを指示するアプリケーションを選択します。
4. アプリケーションをインストールする Android 端末を選択します。
   - 配布済みのアプリケーションのインストールを指示する場合
     インフォメーションエリア下部、［配布済みスマートデバイス一覧］タブからアプリケーションをインストールする Android 端末を選択します。Android 端末は複数選択できます。
   - 未配布のアプリケーションのインストールを指示する場合
     インフォメーションエリア下部、［未配布スマートデバイス一覧］タブからアプリケーションをインストールする Android 端末を選択します。Android 端末は複数選択できます。
5. インフォメーションエリア下部の操作メニューから［アプリケーションインストール］を選択します。
6. 表示されるダイアログで［OK］ボタンをクリックします。

**操作結果**

配布したアプリケーションのインストール指示が Android 端末に表示されます。

利用者側でアプリケーションがインストールされると、［Android アプリケーション］のインフォメーションエリア下部、［インストール済みスマートデバイス一覧］タブに Android 端末の情報が表示されます。

**関連項目**

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.3 登録したアプリケーションの情報を編集する手順
- 9.6 Android 端末にアプリケーションを配布する手順
- 14.6.2 ［Android アプリケーション］画面

## 9.8　Android 端末に配布したアプリケーションをアンインストールする手順

配布されている、またはインストールされているアプリケーションのアンインストールおよびアプリケーションのデータの削除を Android 端末に指示します。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［Android アプリケーション］を選択します。
3. インフォメーションエリアでアンインストールの指示をするアプリケーションを選択します。
4. アプリケーションのアンインストールを指示する Android 端末を、インフォメーションエリア下部の［配布済みスマートデバイス一覧］タブ、または［インストール済みスマートデバイス一覧］タブから選択します。
   Android 端末は複数選択できます。
5. インフォメーションエリア下部の操作メニューから［アプリケーション削除］を選択します。
6. 表示されるダイアログで［OK］ボタンをクリックします。

### 操作結果

配布したアプリケーションがインストールされていない場合
　アプリケーションのデータが削除されます。

配布したアプリケーションがインストールされていた場合
　アンインストールの指示が Android 端末に表示されます。利用者がアンインストールすると、アプリケーションのデータが削除されます。

Android 端末でアプリケーションのアンインストールおよびアプリケーションのデータの削除が完了すると、［Android アプリケーション］画面のインフォメーションエリア下部、［未配布スマートデバイス一覧］タブに Android 端末の情報が表示されます。

### 関連項目

- 9.6 Android 端末にアプリケーションを配布する手順
- 9.7 Android 端末にアプリケーションのインストールを指示する手順
- 14.6.2 ［Android アプリケーション］画面

## 9.9 iOS 端末にアプリケーションのインストールを指示する手順

iOS 端末にアプリケーションを配布し、インストールするよう利用者に指示します。

> **メモ**
>
> インストールの指示は、sdmdistributeapp コマンドでも実施できます。

### 前提条件

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。
- 配布するアプリケーションを通信サーバに配置しておく必要があります。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［iOS アプリケーション］を選択します。
3. インフォメーションエリアでインストールを指示するアプリケーションを選択します。
4. アプリケーションをインストールする iOS 端末を、インフォメーションエリア下部の［未インストールスマートデバイス一覧］タブから選択します。
   iOS 端末は複数選択できます。
5. インフォメーションエリア下部の操作メニューから［アプリケーションインストール］を選択します。
6. 表示されるダイアログで［OK］ボタンをクリックします。

### 操作結果

選択した iOS 端末にアプリケーションが配布され、インストール指示が表示されます。

利用者側でアプリケーションがインストールされると、［iOS アプリケーション］のインフォメーションエリア下部、［インストール済みスマートデバイス一覧］タブに iOS 端末の情報が表示されます。

### 関連項目

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.3 登録したアプリケーションの情報を編集する手順
- 14.6.4 ［iOS アプリケーション］画面

## 9.10　iOS 端末に配布したアプリケーションをアンインストールする手順

インストールされているアプリケーションのアンインストールを iOS 端末に指示します。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

1. 配布画面を表示します。
2. メニューエリアで［iOS アプリケーション］を選択します。
3. インフォメーションエリアでアンインストールの指示をするアプリケーションを選択します。
4. アプリケーションのアンインストールを指示する iOS 端末を、インフォメーションエリア下部の［インストール済みスマートデバイス一覧］タブから選択します。
   iOS 端末は複数選択できます。
5. インフォメーションエリア下部の操作メニューから［アプリケーション削除］を選択します。
6. 表示されるダイアログで［OK］ボタンをクリックします。

### 操作結果

アンインストールの指示が iOS 端末に表示されます。利用者がアンインストールすると、アプリケーションのデータが削除されます。

iOS 端末でアプリケーションのアンインストールおよびアプリケーションのデータの削除が完了すると、［iOS アプリケーション］画面のインフォメーションエリア下部、［未インストールスマートデバイス一覧］タブに iOS 端末の情報が表示されます。

### 関連項目

- 9.9 iOS 端末にアプリケーションのインストールを指示する手順
- 14.6.4 ［iOS アプリケーション］画面

## 9.11　利用者の操作でインストールできるアプリケーションを管理する

管理者は、利用者の操作でインストールできるアプリケーションを管理できます。

利用者の操作でインストールできるアプリケーションを管理するときの事象と操作を次に示します。

| 運用中の事象 | 操作 |
|---|---|
| 利用者の操作でインストールできるアプリケーションを新規に設定する | 1. 配布するアプリケーションを JP1/ITDM2 - SDM に登録する<br>2. 配布するアプリケーションを通信サーバに配置する<br>3. sdmioutils importdeliverypermit -mode all を実行する |
| 配布したいアプリケーションを追加したり、バージョンアップしたりする | 1. 配布するアプリケーションを JP1/ITDM2 - SDM に登録する<br>2. 配布するアプリケーションを通信サーバに配置する<br>3. sdmioutils importdeliverypermit -mode app を実行する |
| 旧バージョンのアプリケーションや不要になったアプリケーションの配布を停止する | 1. sdmioutils deletedeliverypermit -mode app を実行する<br>2. 配布するアプリケーションを通信サーバから削除する<br>3. アプリケーションを JP1/ITDM2 - SDM から削除する |
| スマートデバイスを増やす | 1. sdmioutils importdeliverypermit -mode device を実行する |
| スマートデバイスを滅却する | 1. sdmioutils deletedeliverypermit -mode device を実行する<br>2. スマートデバイスを管理対象外にする |
| 利用者の操作でインストールできるアプリケーションを確認する | 1. sdmioutils exportdeliverypermit を実行する |
| 利用者の操作でインストールできるアプリケーションをバックアップ・リストアする | 1. sdmioutils exportdeliverypermit -mode all を実行して、バックアップを取得する<br>2. sdmioutils importdeliverypermit -mode all を実行して、リストアする。 |

**ヒント**

sdmioutils importdeliverypermit コマンド、およびsdmioutils deletedeliverypermit コマンドで設定を変更する場合は、あらかじめsdmioutils exportdeliverypermit -mode all で設定情報をバックアップしておくことをお勧めします。

**関連項目**

- 8.4 管理対象のスマートデバイスを管理対象外にする手順
- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.4 アプリケーションを JP1/ITDM2 - SDM から削除する手順
- 9.5 不要となったアプリケーションを通信サーバから削除する手順
- 15. sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）

- 15. sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
- 15. sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）

# 9.12 Android 端末から利用者の操作でアプリケーションをインストールする手順

Android 端末から利用者の操作でアプリーションをインストールできます。

**前提条件**

- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。
- 配布するアプリケーションを通信サーバに配置しておく必要があります。
- 利用者の操作でインストールできるアプリケーションを設定しておく必要があります。

**操作手順**

1. Android 端末で JP1/ITDM2 - SDM（スマートデバイス Android エージェント）を起動します。
2. [アプリケーションのインストール] をタップします。
3. [確認] ダイアログが表示された場合は、[OK] ボタンをタップします。
4. 配布アプリケーション一覧画面で、インストールしたいアプリケーションをタップします。
5. [確認] ダイアログで [OK] ボタンをタップします。
   インストールするアプリケーションのダウンロードが開始されます。
6. インストール確認画面で [インストール] ボタンをタップします。

> **重要**
>
> 配布アプリケーション一覧画面に表示されるインストール状態の反映には時間がかかる場合があります。

**関連項目**

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.11 利用者の操作でインストールできるアプリケーションを管理する

# 9.13 iOS 端末から利用者の操作でアプリケーションをインストールする手順

iOS 端末から利用者の操作でアプリーションをインストールできます。

**前提条件**

- 配布するアプリケーションを JP1/ITDM2 - SDM に登録しておく必要があります。
- 配布するアプリケーションを通信サーバに配置しておく必要があります。
- 利用者の操作でインストールできるアプリケーションを設定しておく必要があります。

**操作手順**

1. iOS 端末で JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）を起動します。
2. [アプリケーションのインストール] をタップします。
3. [確認] ダイアログが表示された場合は、[OK] ボタンをタップします。
4. 配布アプリケーション一覧画面で、ダウンロードしたいアプリケーションをタップします。
5. [確認] ダイアログで [OK] ボタンをタップします。
   インストールするアプリケーションのダウンロードが開始されます。
6. インストール確認ダイアログが表示された場合は、[インストール] ボタンをタップします。

> **重要**
>
> 配布アプリケーション一覧画面に表示されるインストール状態の反映には時間がかかる場合があります。

**関連項目**

- 9.1 配布するアプリケーションを JP1/ITDM2 - SDM に登録する手順
- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 9.11 利用者の操作でインストールできるアプリケーションを管理する

## 9.14　配布アプリケーションの最大同時ダウンロード数を制限する手順

利用者の操作でアプリケーションをインストールする場合、複数のスマートデバイスからアプリケーションが同時にダウンロードされることで、ネットワークに負荷がかかり、他の業務に影響を及ぼすおそれがあります。この場合、配布アプリケーションの最大同時ダウンロード数を制限することで、ネットワークの負荷を軽減できます。

**操作手順**

1. 通信サーバで、httpsd.conf ファイルを開きます。

   httpsd.conf ファイルの格納先は次のとおりです。

   JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥conf

2. httpsd.conf ファイル中の QOSRejectionServers ディレクティブの値を変更します。

   QOSRejectionServers ディレクティブの指定方法を次に示します。

| 記述個所 | ディレクティブ名 | 設定範囲 | 説明 |
|---|---|---|---|
| <VirtualHost localhost:26055>内の<Location /download/>の中 | QOSRejectionServers | 5～49<br>デフォルト 5（最大同時ダウンロード数 45） | 最大同時ダウンロード数＝50 - QOSRejectionServers の値で指定します。 |

（指定例）

```
Listen 26055
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/～/newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/～/newkeyRSA.pem"
    <Location /download/>
         Allow from all
         QOSRejectionServers 5
    </Location>
</VirtualHost>
```

3. 通信サーバのサービス「JP1/ITDM2 - Smart Device Manager Web Server」を再起動します。

# 10 イベントを参照する

ここでは、JP1/ITDM2 - SDM が出力したイベントの参照方法について説明します。

# 10.1　イベントの詳細を確認する手順

JP1/ITDM2 - SDM が出力したイベントの詳細を確認します。

### 操作手順

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の重大度を選択します。
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の「内容」のリンクをクリックします。
   詳細を表示したいイベントを選択し、［操作メニュー］の［イベント詳細を表示する］を選択しても［イベント詳細］ダイアログが表示されます。

### 操作結果

［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。

### 関連項目

- 2.7 イベントの表示
- 14.7.1 ［イベント一覧］画面
- 14.7.2 ［イベント詳細］ダイアログ

## 10.2　イベント情報をエクスポートする手順

登録日時が 1 週間以内のイベント情報を CSV ファイルにエクスポートします。エクスポートできる最大件数は 200,000 件です。

### 操作手順

1. イベント画面を表示します。
2. [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。
3. 表示された画面で、保存先とファイル名を指定し、[保存] ボタンをクリックします。

### 操作結果

指定した保存先に、指定したファイル名で CSV ファイルが保存されます。

### 関連項目

- 2.7 イベントの表示
- 14.7.1 ［イベント一覧］画面

# 11 設定をカスタマイズする

ここでは、設定画面でカスタマイズできる項目について説明します。

# 11.1　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、イベントの発生を管理者にメールで通知するように設定します。

### 前提条件

- システム管理権限を持つユーザーアカウントでログインする必要があります。
- メールサーバを設定する必要があります。

### 操作手順

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. 表示される画面で、メールで通知を受け取りたいイベントの重大度と種類、およびイベントを通知するユーザー ID をチェックします。

### 次の作業

イベントメールフォーマット情報ファイルでイベントメールの形式を定義します。

### 関連項目

- 2.7 イベントの表示
- 11.2 メールサーバを設定する手順
- 14.8.4 ［イベント通知の設定］画面
- 16.4 イベントメールフォーマット情報ファイル（eventmail.properties）

## 11.2　メールサーバを設定する手順

イベントの発生などのメールを受け取るためには、JP1/ITDM2 - SDM 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。

### 前提条件

システム管理権限を持つユーザーアカウントでログインする必要があります。

### 操作手順

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、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テストメールが送信されます。メールが正しく送信されているか確認してください。
4. ［適用］ボタンをクリックします。

### 操作結果

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。

### 関連項目

- 11.1 イベント通知の設定をする手順
- 14.8.5 ［メールサーバ設定］画面

# 12 データベースを管理する

ここでは、データベースを管理する方法について説明します。

## 12.1　データベースをバックアップする手順

スマートデバイスマネージャーのリプレースやハードディスクの障害に備え、データベースをバックアップします。

> **重要**
>
> データベースのバックアップに加えて、通信サーバに配置したアプリケーションを退避する必要があります。

**操作手順**

1. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
2. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)
3. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
4. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Server Service
5. スマートデバイスマネージャーで、コマンドプロンプトを起動し、カレントディレクトリをコマンドの格納先に変更します。
6. スマートデバイスマネージャーで、`sdmexportdb` コマンドを実行します。
7. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager Server Service
8. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager Web Server
9. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)
10. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager Web Server

**操作結果**

バックアップデータが保存されます。デフォルトでは次に示すフォルダに格納されます。

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥backup

**関連項目**

- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 15. コマンドを実行する流れ
- 15. sdmexportdb（バックアップの取得）
- 付録 B.1 サービス一覧

## 12.2 データベースをリストアする手順

データベースをバックアップデータ取得時の状態にリストアできます。データベースのリストアには sdmexportdb コマンドで取得したバックアップデータが必要です。

**重要**

データベースのリストアに加えて、配布するアプリケーションを通信サーバに配置する必要があります。

**操作手順**

1. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
2. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)
3. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
4. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Server Service
5. スマートデバイスマネージャーに、sdmexportdb コマンドで取得したバックアップデータをコピーします。
6. スマートデバイスマネージャーで、コマンドプロンプトを起動し、カレントディレクトリをコマンドの格納先に変更します。
7. スマートデバイスマネージャーで、sdmimportdb コマンドを実行します。
8. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager Server Service
9. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager Web Server
10. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager (Communication Server Service)
11. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager Web Server

### 操作結果

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のデータベースがバックアップデータ取得時の状態にリストアされます。

### 関連項目

- 9.2 配布するアプリケーションを通信サーバに配置する手順
- 15. コマンドを実行する流れ
- 15. sdmimportdb（バックアップデータのリストア）
- 付録 B.1 サービス一覧

## 12.3　データベースの接続先ポート番号を変更する手順

スマートデバイスマネージャーのデータベースの接続先ポート番号を変更できます。

**前提条件**

JP1/ITDM2 - SDM の操作画面、およびコマンドをすべて停止しておく必要があります。

**操作手順**

1. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
2. 通信サーバで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)
3. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Web Server
4. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager Server Service
5. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを停止します。
   JP1/ITDM2 - Smart Device Manager (DB Service)
6. スマートデバイスマネージャーで、次に示すファイルをテキストエディタで開きます。
   JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥db¥conf¥pdsys
7. 必要に応じて pd_name_port、および pd_service_port の値を変更します。
   （例）下線部を変更します。

   ```
   set pd_name_port = 26066
   set pd_service_port = 26067
   ```

   pd_name_port は、スマートデバイスマネージャーとスマートデバイスマネージャー内のデータベースの接続で使用するポート番号です。

   pd_service_port は、通信サーバとスマートデバイスマネージャー内のデータベースの接続で使用するポート番号です。
8. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
   JP1/ITDM2 - Smart Device Manager (DB Service)
9. スマートデバイスマネージャーで、コマンドプロンプトを起動し、カレントディレクトリをコマンドの格納先に変更します。
10. スマートデバイスマネージャーで、sdmnetchange コマンドを実行します。

```
sdmnetchange -target Manager -port pd_name_portに指定したポート番号
```

11. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager Server Service
12. スマートデバイスマネージャーで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager Web Server
13. 通信サーバで、コマンドプロンプトを起動し、カレントディレクトリをコマンドの格納先に変更します。
14. 通信サーバで、sdmnetchange コマンドを実行します。

```
sdmnetchange -target Comsrv -port pd_service_portに指定したポート番号
```

15. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager (Communication Server Service)
16. 通信サーバで、Windows の［サービス］画面から、次のサービスを開始します。
    JP1/ITDM2 - Smart Device Manager Web Server
17. スマートデバイスマネージャーで、次に示すファイルをテキストエディタで開きます。
    JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥conf¥sdmdbport.conf
18. ファイルに記載されている値を、手順 7 で pd_name_port に設定したポート番号に変更します。

**操作結果**

データベースの接続先ポート番号が変更されます。

**関連項目**

- 15. コマンドを実行する流れ
- 15. sdmnetchange（スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更）
- 付録 B.1 サービス一覧

# 13 トラブルシューティング

ここでは、JP1/ITDM2 - SDM で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。

## 13.1　スマートデバイスマネージャーでのトラブルシューティングの手順

スマートデバイスマネージャーの運用時にトラブルが発生した場合の対処方法を説明します。

### 操作手順

1. エラーメッセージを確認します。
   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、エラー内容を確認する
   - 出力されたログファイルから、エラー内容を確認する
   - 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する
2. 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、対処します。
   必要に応じてスマートデバイスマネージャーのログ（トラブルシュート情報）を取得してください。

### 関連項目

- 10.1 イベントの詳細を確認する手順
- 15. sdmgetlogs（ログ情報の取得）
- 17. メッセージ
- 付録 F サポートに必要な情報の格納先または入手方法

## 13.2　スマートデバイスでのトラブルシューティングの手順

スマートデバイスの運用時にトラブルが発生した場合の対処方法を説明します。

### 操作手順

1. エラーメッセージを確認します。
   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、対処します。
   必要に応じてスマートデバイスのログ（トラブルシュート情報）を取得してください。

### 関連項目

- 8.12 スマートデバイスのログを取得する手順
- 10.1 イベントの詳細を確認する手順
- 14.3 ホーム画面
- 14.7 イベント画面
- 17. メッセージ

## 13.3　ディスクの空き容量が少ないときの対処方法

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のデータベースは、格納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ります。このような事態を避けるためには、JP1/ITDM2 - SDM（スマートデバイスマネージャー）が使用するディスクの空き容量を定期的に監視して、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/ITDM2 - SDM（スマートデバイスマネージャー）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いる場合は、空き容量を増やすための対処をしてください。

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、スマートデバイスマネージャーをリプレースして対処してください。スマートデバイスマネージャーをリプレースする場合は、バックアップを取得したあとでサーバのリプレースを実施し、JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールしたあとにバックアップファイルをリストアしてください。

**関連項目**

- 3.5 JP1/ITDM2 - SDM（スマートデバイスマネージャー）をインストールする手順
- 12.1 データベースをバックアップする手順
- 12.2 データベースをリストアする手順
- 14.3.3 ［データベースとディスクの状況］パネル

## 13.4　サーバ間での通信エラー発生時のトラブルシューティング

サーバ間で通信エラーが発生する場合の対処方法を説明します。

### 13.4.1　スマートデバイスマネージャーと通信サーバ間で通信エラーが発生する場合の対処方法

スマートデバイスマネージャーと通信サーバ間で通信エラーが発生する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| スマートデバイスマネージャーまたは通信サーバのサービスが停止している。 | Windows の［サービス］画面から該当するサーバのサービスを開始してください。 |
| スマートデバイスマネージャーと通信サーバの間の接続先アドレスおよびポート番号の設定が誤っている。 | ネットワーク設定を見直してください。 |
| 通信サーバでの Web サーバの SSL 通信の設定に不具合がある。 | 通信サーバの SSL 通信の設定を見直してください。 |
| 上記以外の原因（ケーブルの断線やハードウェアの故障など） | システム管理者に連絡してください。 |

**関連項目**

- 3.1 システムを構築する流れ
- 3.8 ルータのポート開放および各サーバのファイアウォールの設定について
- 3.11 SSL 通信用証明書の取得

### 13.4.2　通信サーバとメッセージングサーバ間で通信エラーが発生する場合の対処方法

通信サーバとメッセージングサーバ間で通信エラーが発生する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| 通信サーバまたはメッセージングサーバのサービスが停止している。 | Windows の［サービス］画面から該当するサーバのサービスを開始してください。 |
| 通信サーバとメッセージングサーバの間の接続先アドレスおよびポート番号の設定が誤っている。 | ネットワーク設定を見直してください。 |
| 上記以外の原因（ケーブルの断線やハードウェアの故障など） | システム管理者に連絡してください。 |

**関連項目**

- 3.8 ルータのポート開放および各サーバのファイアウォールの設定について

## 13.5　画面操作時のトラブルシューティング

スマートデバイス一覧およびイベント一覧のエクスポート時にエクスポートファイルのダウンロードが実行されない場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
| --- | --- |
| Internet Explorer の信頼済みサイトの保護モードの設定が無効になっている。 | Internet Explorer 8 で、次の設定をしてください。<br>• 信頼済みサイトへスマートデバイスマネージャーを登録する<br>• 信頼済みサイトのセキュリティ設定を変更する<br>• 保護モードの設定を有効にする<br>詳細については、Microsoft 社の情報を参照してください。 |

## 13.6　データベース障害のトラブルシューティング

データベース障害の対処方法を説明します。

### 13.6.1　データベース接続エラーが発生する場合の対処方法

データベース接続エラーが発生する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| JP1/ITDM2 - Smart Device Manager (DB Service)が停止状態または開始中の状態である。 | • JP1/ITDM2 - Smart Device Manager (DB Service)が停止状態の場合、Windows の［サービス］画面から JP1/ITDM2 - Smart Device Manager (DB Service)を起動してください。<br>• JP1/ITDM2 - Smart Device Manager (DB Service)が開始中の場合、JP1/ITDM2 - Smart Device Manager (DB Service)が開始になるまで待機してください。 |

### 13.6.2　データベースのアクセスエラーが発生する場合の対処方法

データベースのアクセスエラーが発生する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| データベース破壊などの理由でアクセスエラーとなる。 | データベースのリストアコマンドで、データベースの復旧を試みてください。 |

### 13.6.3　データベースのバックアップ、リストアが失敗する場合の対処方法

データベースのバックアップ、リストアが失敗する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| 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。 | 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。<br>アクセス権限が不足している場合、該当フォルダにアクセス権限を付与し、再度データベースのバックアップ、リストアを試みてください。 |
| I/O エラーが発生した。 | 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。<br>ディスク障害が発生している場合、ハードディスクを交換するなど、環境を再構築してください。 |

上記のどちらの対処でも復旧しない場合は、データベースのバックアップデータおよびトラブルシュート情報を取得してください。

**関連項目**

- 15. sdmgetlogs（ログ情報の取得）
- 付録 A.1 スマートデバイスマネージャーに作成されるフォルダ

## 13.7　iOS アプリケーションのインストールでのトラブルシューティング

iOS アプリケーションのインストール時にトラブルが発生した場合の対処方法を説明します。

### 13.7.1　iOS アプリケーションのインストールに失敗する場合の対処方法

iOS アプリケーションのインストールが失敗する場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| バンドル ID が誤っている。 | 開発者が配布ファイルを作成するときに指定したバンドル ID と一致していることを確認してください。 |
| インストールパラメーターが誤っている。 | 正しいインストールパラメーターが指定されているか、Apple 社のホームページなどで確認してください。 |
| 通信サーバに格納した構成プロファイルを iPhone 構成ユーティリティで作成した場合に、［モバイルデバイス管理］の［アクセス権］の下にある［App］がチェックされていない。 | ［App］をチェックして構成プロファイルを作成し、通信サーバに格納してください。 |

### 13.7.2　アプリーションのインストール結果が［iOS アプリケーション］画面に反映されない場合の対処方法

iOS 端末へ iOS アプリケーションのインストールが成功しても、JP1/ITDM2 - SDM の［iOS アプリケーション］画面に反映されない場合に、考えられる原因と対処方法を説明します。

| 原因 | 対処方法 |
|---|---|
| iOS 端末から最新のインベントリ情報が取得されていない。 | 次のどちらかを実施してください。<br>• ［管理対象のスマートデバイス一覧］画面の操作メニューから［最新の情報を取得する］を選択する<br>• iOS 端末の JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）で［インベントリ情報を送信する］をタップする |
| 登録した iOS アプリケーションのバンドル ID やバージョンが誤っている。 | 開発者が配布ファイルを作成するときに指定したバンドル ID やバージョンと一致していることを確認してください。 |

# 14 画面リファレンス

ここでは、JP1/ITDM2 - SDM の画面や画面のボタン、操作メニュー、入力項目などを説明します。

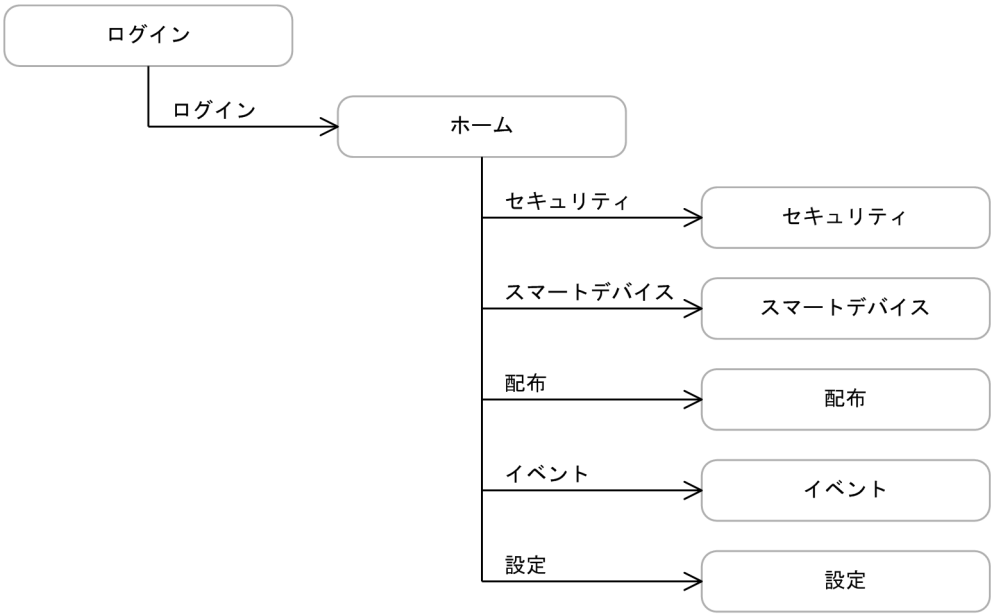
## 14.1　画面遷移図

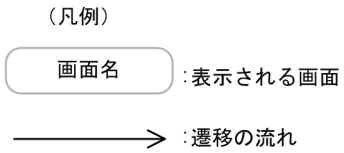
ここでは、JP1/ITDM2 - SDM の画面遷移について説明します。

### 14.1.1　ログイン画面からログイン直後までの画面遷移

JP1/ITDM2 - SDM のログイン画面からログイン直後までの画面遷移を説明します。

**画面遷移**



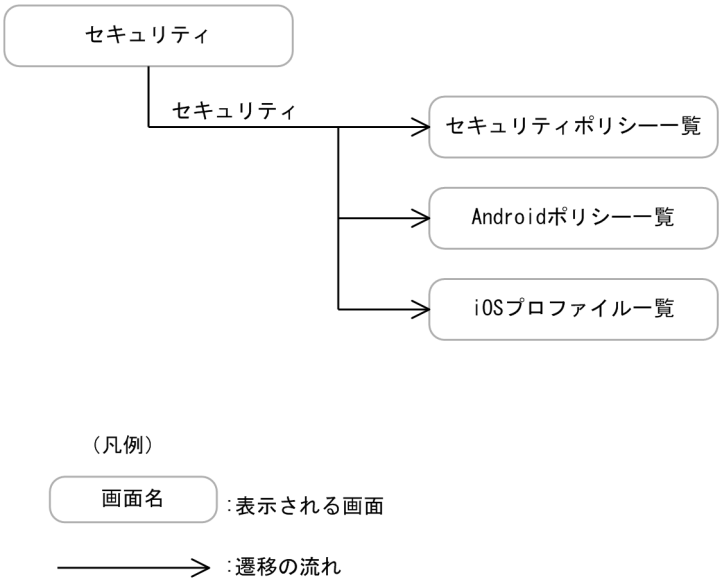

**関連項目**

- 14.2 ログイン画面
- 14.3 ホーム画面
- 14.4 セキュリティ画面
- 14.5 スマートデバイス画面
- 14.6 配布画面
- 14.7 イベント画面
- 14.8 設定画面

## 14.1.2　セキュリティ画面の画面遷移

セキュリティのルールを管理するセキュリティ画面の画面遷移を説明します。

### 画面遷移



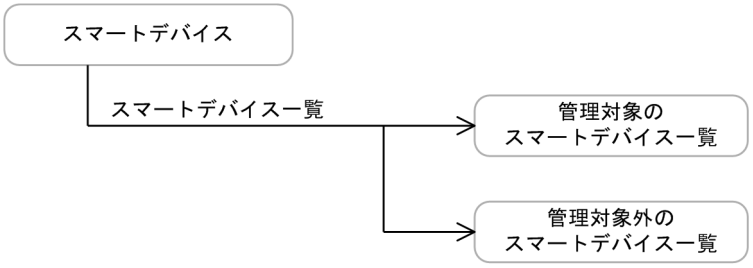

### 関連項目

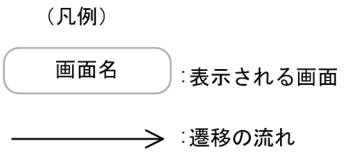
- 14.4 セキュリティ画面
- 14.4.1 ［セキュリティポリシー一覧］画面
- 14.4.11 ［Android ポリシー一覧］画面
- 14.4.15 ［iOS プロファイル一覧］画面

## 14.1.3　スマートデバイス画面の画面遷移

スマートデバイスの情報を管理するスマートデバイス画面の画面遷移を説明します。

### 画面遷移



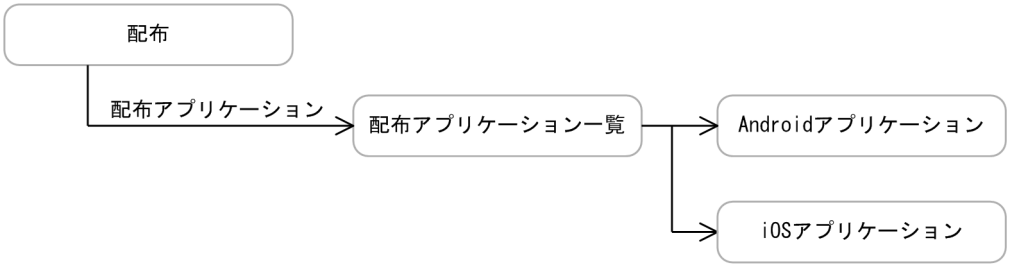

### 関連項目

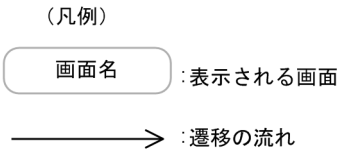
- 14.5 スマートデバイス画面
- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 14.1.4 配布画面の画面遷移

配布するアプリケーションを管理する配布画面の画面遷移を説明します。

### 画面遷移




### 関連項目

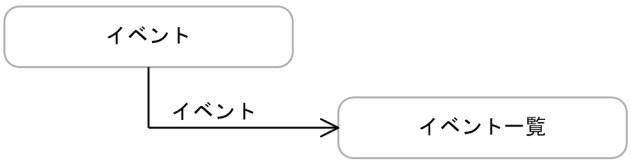
- 14.6 配布画面
- 14.6.1 ［配布アプリケーション一覧］画面
- 14.6.2 ［Android アプリケーション］画面

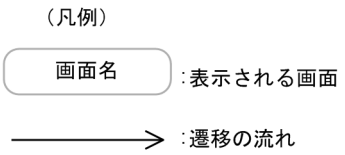
- 14.6.4 ［iOS アプリケーション］画面

## 14.1.5 イベント画面の画面遷移

JP1/ITDM2 - SDM の運用中に発生したイベントを確認するイベント画面の画面遷移を説明します。

**画面遷移**



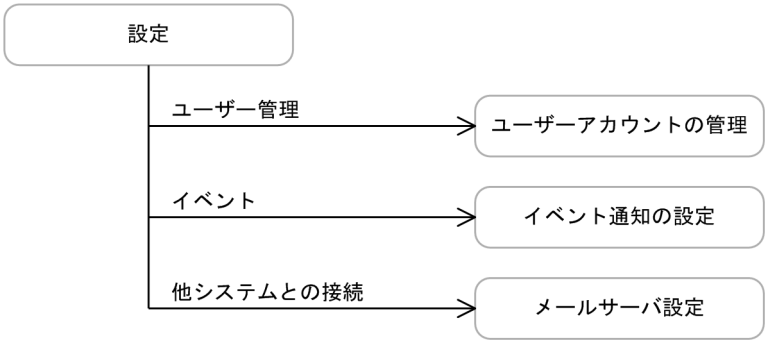

**関連項目**

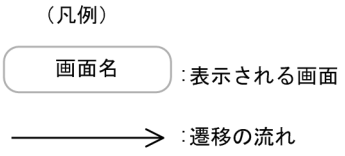
- 14.7 イベント画面
- 14.7.1 ［イベント一覧］画面

## 14.1.6 設定画面の画面遷移

JP1/ITDM2 - SDM の運用に必要な設定をする設定画面の画面遷移を説明します。

**画面遷移**



**関連項目**

- 14.8 設定画面
- 14.8.1 ［ユーザーアカウントの管理］画面
- 14.8.4 ［イベント通知の設定］画面
- 14.8.5 ［メールサーバ設定］画面

## 14.2　ログイン画面

ログイン画面ではユーザー認証をします。認証に成功すると JP1/ITDM2 - SDM にログインできます。ビルトインアカウント、または新規に作成したユーザーアカウントでログインした場合や、パスワードが期限切れとなった場合に、[パスワードの変更] ダイアログが表示されます。

### 画面

### 項目

表示される入力項目を次に示します。

[ユーザー ID]

JP1/ITDM2 - SDM（スマートデバイスマネージャー）にログインするためのユーザー ID を入力します。

[パスワード]

ユーザー名に対応するパスワードを入力します。

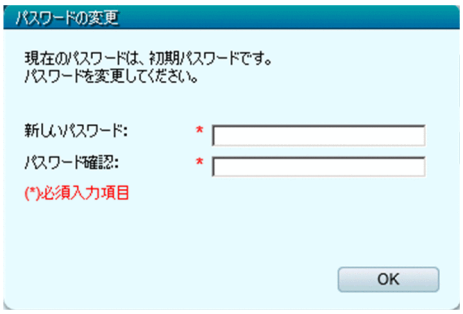
### 関連項目

- 14.2.1 [パスワードの変更] ダイアログ

## 14.2.1　[パスワードの変更] ダイアログ

[パスワードの変更] ダイアログでは、パスワードが変更できます。ビルトインアカウント、または新規に作成したユーザーアカウントでログインした場合や、パスワードが期限切れとなった場合に、[パスワードの変更] ダイアログが表示されます。

## 画面




## 項目

表示される入力項目を次に示します。

[新しいパスワード]

新しいパスワードを入力します。

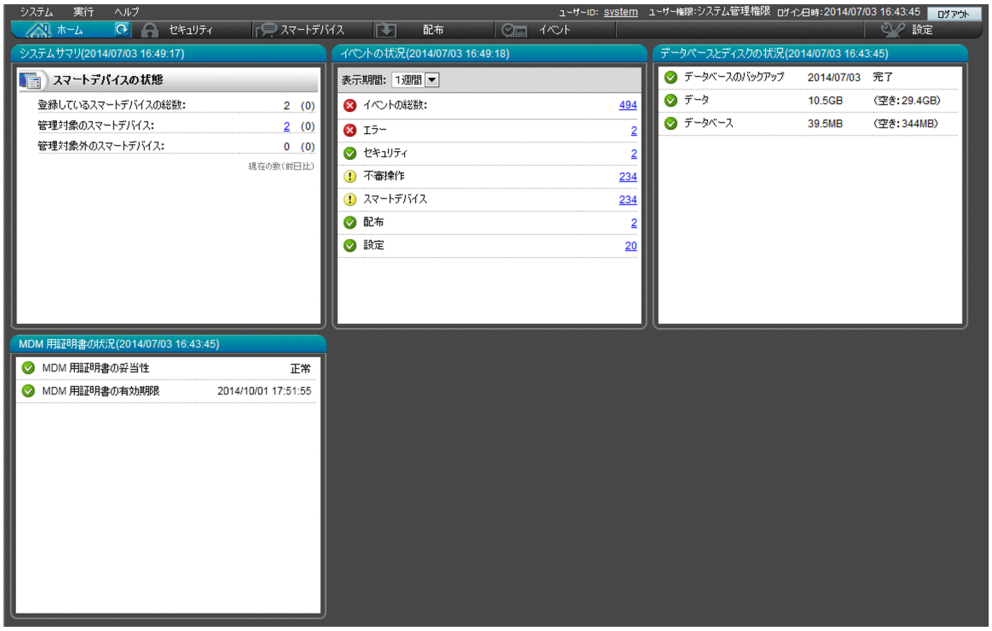
[パスワード確認]

確認のためにパスワードを再入力します。

# 14.3　ホーム画面

JP1/ITDM2 - SDM にログインすると、最初にホーム画面が表示されます。JP1/ITDM2 - SDM で管理している情報の概要を各パネルで確認できます。

### 画面



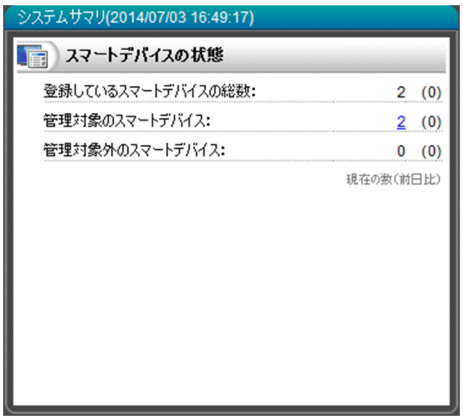

### 関連項目

- 14.3.1　[システムサマリ] パネル
- 14.3.2　[イベントの状況] パネル
- 14.3.3　[データベースとディスクの状況] パネル
- 14.3.4　[MDM 用証明書の状況] パネル

## 14.3.1　[システムサマリ] パネル

[システムサマリ] パネルでは、JP1/ITDM2 - SDM に登録されているスマートデバイスの概況が確認できます。

### 画面




### 項目

表示項目を次に示します。

登録しているスマートデバイスの総数

JP1/ITDM2 - SDM に登録しているスマートデバイスの総数および前日との差分台数が表示されます。

管理対象のスマートデバイス

管理対象のスマートデバイスの台数および前日との差分台数が表示されます。現在の台数が 1 台以上の場合は、スマートデバイスの台数のリンクをクリックするとスマートデバイス画面が表示され、管理対象のスマートデバイスの詳細情報を確認できます。

管理対象外のスマートデバイス

管理対象外のスマートデバイスの台数および前日との差分台数が表示されます。現在の台数が 1 台以上の場合は、スマートデバイスの台数のリンクをクリックするとスマートデバイス画面が表示され、管理対象外のスマートデバイスの詳細情報を確認できます。

### 関連項目

- 14.5 スマートデバイス画面

## 14.3.2 ［イベントの状況］パネル

［イベントの状況］パネルでは、表示対象期間内に発生したイベントの総件数およびイベントの種類別の発生件数が確認できます。

### 画面

発生件数のリンクをクリックするとイベント画面が表示され、イベントの内容を確認できます。

### 項目

表示項目を次に示します。

[表示期間]
　イベントの表示期間を変更します。

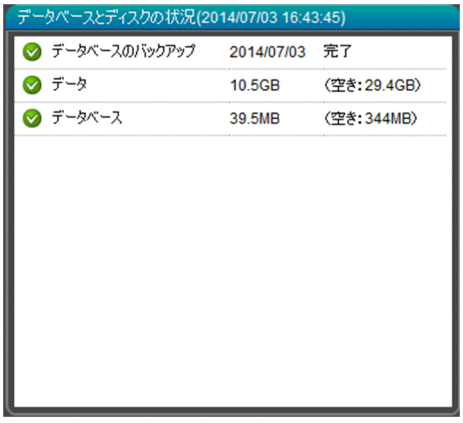
### 関連項目

- 14.7 イベント画面

## 14.3.3 ［データベースとディスクの状況］パネル

［データベースとディスクの状況］パネルでは、データベースのバックアップの実施状況やハードディスクの空き容量など、データベースに関する情報が確認できます。

### 画面



**項目**

表示項目を次に示します。

データベースのバックアップ
　データベースのバックアップを実施した日付および実施状態が表示されます。

データ
　データのハードディスクの使用量および空き容量が表示されます。

データベース
　データベースのハードディスクの使用量および空き容量が表示されます。

## 14.3.4 ［MDM 用証明書の状況］パネル

［MDM 用証明書の状況］パネルでは、証明書の有効期限、証明書の妥当性に関する情報が確認できます。

**画面**

**項目**

表示項目を次に示します。

MDM 用証明書の妥当性
　MDM 用証明書の妥当性が表示されます。
　表示される情報と内容を次に示します。

| 情報 | 内容 |
|---|---|
| 未使用 | 証明書の設定なし |
| 正常 | 証明書の設定あり（正常） |
| 不正 | 証明書の設定あり（不正） |

MDM 用証明書の有効期限
　MDM 用証明書の有効期限が表示されます。

表示される情報と内容を次に示します。

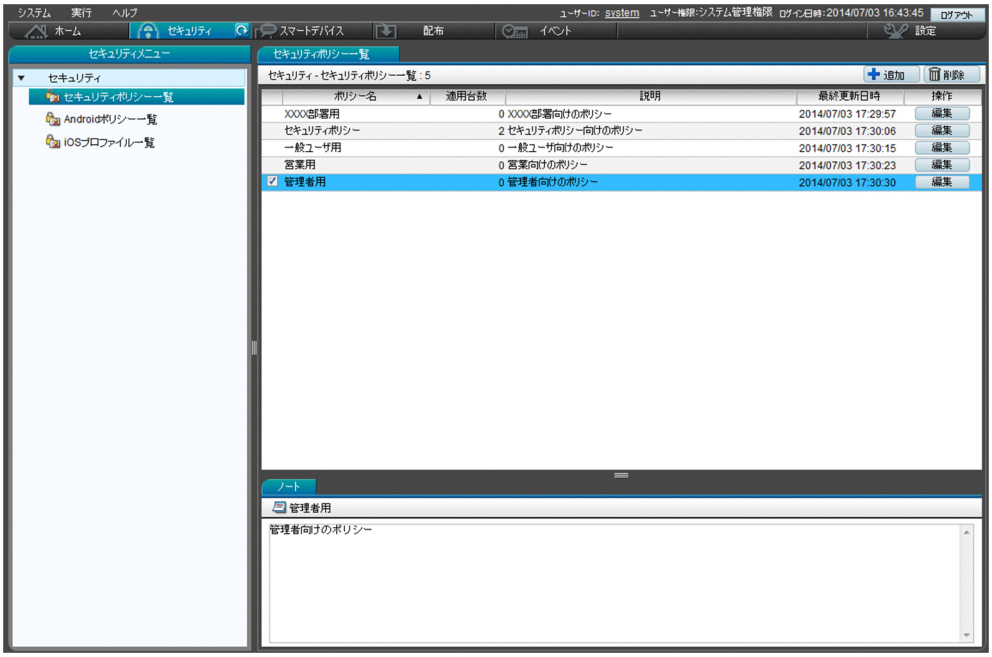
| 情報 | 内容 |
|---|---|
| -（ハイフン） | MDM 用証明書の設定なし |
| YYYY/MM/DD hh:mm:ss※（日時） | MDM 用証明書の設定あり |
| （緊急） | 期限切れ |
| （警戒） | 期限切れ 1 か月前 |
| （情報） | 期限内、または MDM 用証明書の設定なし |

注※　YYYY：年、MM：月、DD：日、hh：時、mm：分、ss：秒

# 14.4　セキュリティ画面

セキュリティ画面では、JP1/ITDM2 - SDM で提供するセキュリティのルールを管理できます。

### 画面



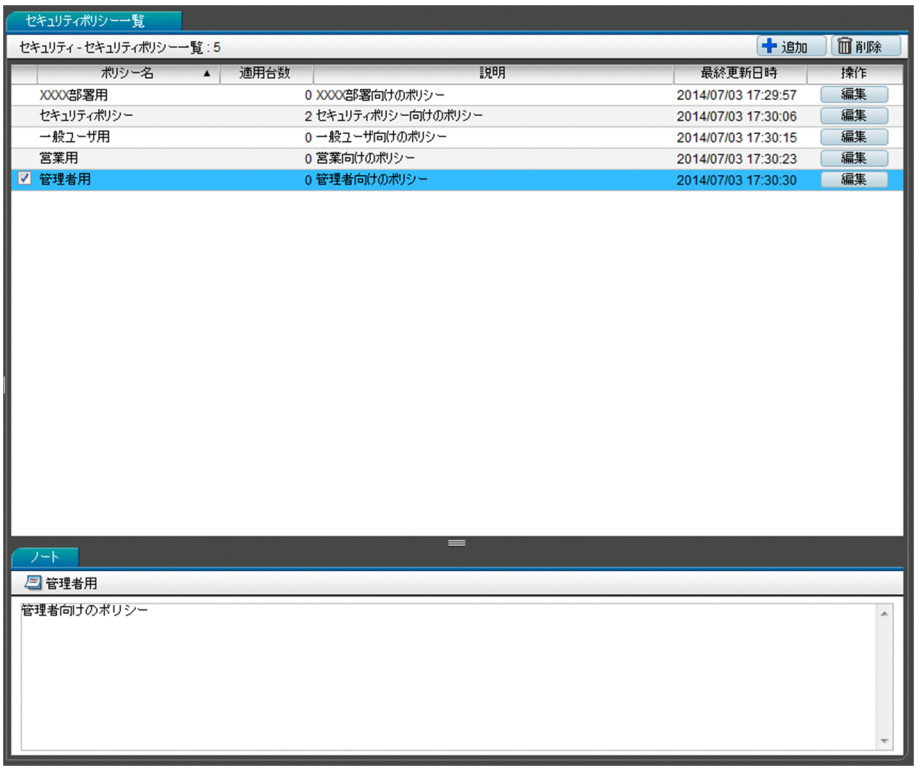

### 関連項目

- 14.4.1 ［セキュリティポリシー一覧］画面
- 14.4.11 ［Android ポリシー一覧］画面
- 14.4.15 ［iOS プロファイル一覧］画面

## 14.4.1　［セキュリティポリシー一覧］画面

［セキュリティポリシー一覧］画面では、作成したセキュリティポリシーの一覧が表示されます。また、セキュリティポリシーの追加、編集、および削除ができます。

## 画面




## 項目

表示されるボタンおよびタブを次に示します。

[追加] ボタン

新規にセキュリティポリシーを追加します。

[削除] ボタン

選択したセキュリティポリシーを削除します。

[編集] ボタン（[参照] ボタン）

選択したセキュリティポリシーを編集します。

参照権限のアカウントでログインしている場合は、[参照] ボタンが表示され、選択したセキュリティポリシーの内容を確認できます。

[ノート] タブ

インフォメーションエリア下部に、選択しているセキュリティポリシーの説明が表示されます。システム管理権限のアカウントでログインしている場合は、セキュリティポリシーの説明を編集できます。

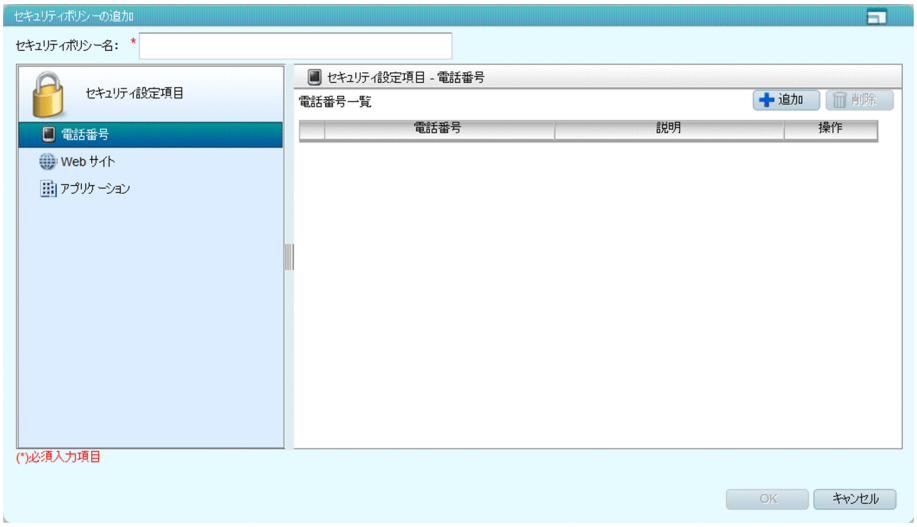
## 関連項目

- 14.4.2 [セキュリティポリシーの追加] ダイアログ
- 14.4.3 [セキュリティポリシーの編集] ダイアログ
- 14.4.4 [セキュリティポリシーの参照] ダイアログ

## 14.4.2 ［セキュリティポリシーの追加］ダイアログ

［セキュリティポリシーの追加］ダイアログでは、新規にセキュリティポリシーを追加できます。

### 画面




### 項目

セキュリティ設定項目を次に示します。

電話番号

利用を許可する電話番号を設定します。スマートデバイスで、電話番号一覧に登録されていない電話番号が利用された場合、イベントが発行され管理者に通知されます。

Web サイト

閲覧を許可または禁止する Web サイトを設定します。スマートデバイスで、閲覧を禁止している Web サイトが閲覧された場合、イベントが発行され管理者に通知されます。

アプリケーション

利用を許可または禁止するアプリケーションを設定します。スマートデバイスで、利用を禁止しているアプリケーションが利用された場合、イベントが発行され管理者に通知されます。

また、利用を許可するアプリケーションの場合、インストールが必須か任意かを設定できます。インストール必須のアプリケーションがインストールされていない場合、イベントが発行され管理者に通知されます。

表示される入力項目およびボタンを次に示します。

［セキュリティポリシー名］

セキュリティポリシー名を入力します。

［追加］ボタン

セキュリティ設定項目として、新規に電話番号などを追加します。

［削除］ボタン

選択した電話番号などを削除します。

［編集］ボタン

選択した電話番号などを編集します。

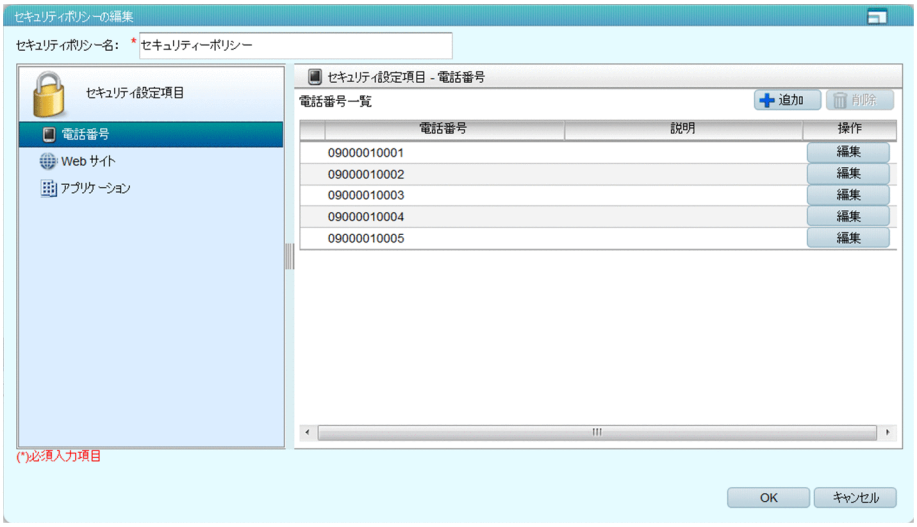
**関連項目**

- 14.4.5 ［電話番号の追加］ダイアログ
- 14.4.6 ［電話番号の編集］ダイアログ
- 14.4.7 ［Web サイトの追加］ダイアログ
- 14.4.8 ［Web サイトの編集］ダイアログ
- 14.4.9 ［アプリケーションの追加］ダイアログ
- 14.4.10 ［アプリケーションの編集］ダイアログ

## 14.4.3 ［セキュリティポリシーの編集］ダイアログ

［セキュリティポリシーの編集］ダイアログでは、作成されたセキュリティポリシーを編集できます。

**画面**




**項目**

セキュリティ設定項目を次に示します。

電話番号

利用を許可する電話番号を設定します。スマートデバイスで、電話番号一覧に登録されていない電話番号が利用された場合、イベントが発行され管理者に通知されます。

Web サイト

閲覧を許可または禁止する Web サイトを設定します。スマートデバイスで、閲覧を禁止している Web サイトが閲覧された場合、イベントが発行され管理者に通知されます。

アプリケーション

利用を許可または禁止するアプリケーションを設定します。スマートデバイスで、利用を禁止しているアプリケーションが利用された場合、イベントが発行され管理者に通知されます。

また、利用を許可するアプリケーションの場合、インストールが必須か任意かを設定できます。インストール必須のアプリケーションがインストールされていない場合、イベントが発行され管理者に通知されます。

表示される入力項目およびボタンを次に示します。

[セキュリティポリシー名]

セキュリティポリシー名を編集します。

[追加] ボタン

セキュリティ設定項目として、新規に電話番号などを追加します。

[削除] ボタン

選択した電話番号などを削除します。

[編集] ボタン

選択した電話番号などを編集します。

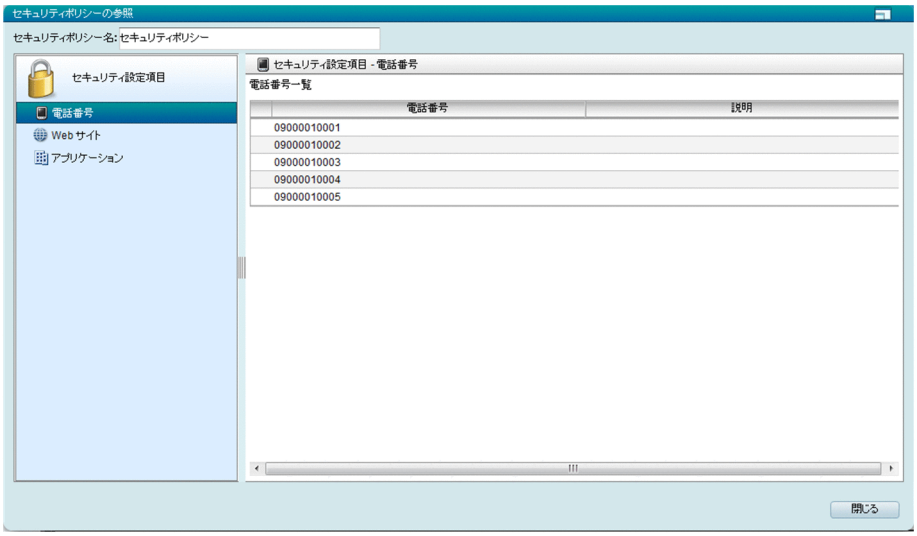
**関連項目**

- 14.4.5 [電話番号の追加] ダイアログ
- 14.4.6 [電話番号の編集] ダイアログ
- 14.4.7 [Web サイトの追加] ダイアログ
- 14.4.8 [Web サイトの編集] ダイアログ
- 14.4.9 [アプリケーションの追加] ダイアログ
- 14.4.10 [アプリケーションの編集] ダイアログ

## 14.4.4 [セキュリティポリシーの参照] ダイアログ

[セキュリティポリシーの参照] ダイアログでは、セキュリティポリシーの内容を確認できます。

### 画面




### 項目

セキュリティ設定項目を次に示します。

電話番号

利用を許可する電話番号の一覧が表示されます。スマートデバイスで、電話番号一覧に登録されていない電話番号が利用された場合、イベントが発行され管理者に通知されます。

Web サイト

閲覧を許可または禁止する Web サイトの一覧が表示されます。スマートデバイスで、閲覧を禁止している Web サイトが閲覧された場合、イベントが発行され管理者に通知されます。

アプリケーション

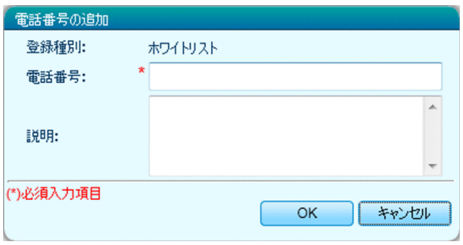
利用を許可または禁止するアプリケーションの一覧が表示されます。スマートデバイスで、利用を禁止しているアプリケーションが利用された場合、イベントが発行され管理者に通知されます。

また、利用を許可するアプリケーションの場合、インストールが必須か任意かを確認できます。インストール必須のアプリケーションがインストールされていない場合、イベントが発行され管理者に通知されます。

## 14.4.5 ［電話番号の追加］ダイアログ

［電話番号の追加］ダイアログでは、通話を許可する電話番号を追加できます。

### 画面




### 項目

表示される入力項目を次に示します。

[電話番号]

スマートデバイスに対して通話を許可する電話番号を入力します。

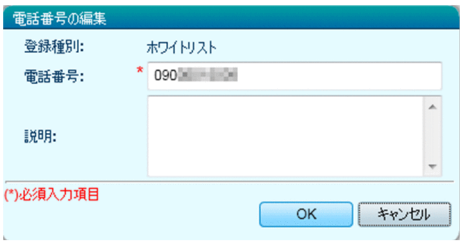
[説明]

電話番号についての説明を入力します。電話番号の利用者名や、電話番号の利用目的などを入力するとポリシーの管理が容易になります。

## 14.4.6 ［電話番号の編集］ダイアログ

［電話番号の編集］ダイアログでは、通話を許可する電話番号を編集できます。

### 画面




### 項目

表示される入力項目を次に示します。

[電話番号]

登録済みの電話番号を編集します。

[説明]

電話番号についての説明を編集します。電話番号の利用者名や、電話番号の利用目的などを入力するとポリシーの管理が容易になります。

## 14.4.7 ［Web サイトの追加］ダイアログ

［Web サイトの追加］ダイアログでは、閲覧を許可する Web サイトと禁止する Web サイトを追加できます。

### 画面

### 項目

表示される入力項目を次に示します。

［登録種別］

登録する Web サイトの閲覧を許可するか、または禁止するかを選択します。閲覧を許可する場合は［ホワイトリスト］を、禁止する場合は［ブラックリスト］を選択してください。

［URL］

閲覧を許可、または禁止する Web サイトの URL を入力します。

［説明］

登録する Web サイトについての説明を入力します。サイトの名称や、利用目的などを入力するとポリシーの管理が容易になります。

## 14.4.8 ［Web サイトの編集］ダイアログ

［Web サイトの編集］ダイアログでは、閲覧を許可する Web サイトと禁止する Web サイトを編集できます。

### 画面

### 項目

表示される入力項目を次に示します。

[登録種別]

登録する Web サイトの閲覧を許可するか、または禁止するかを選択します。閲覧を許可する場合は［ホワイトリスト］を、禁止する場合は［ブラックリスト］を選択してください。

[URL]

閲覧を許可、または禁止する Web サイトの URL を編集します。

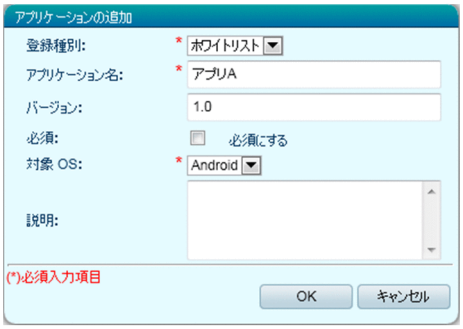
[説明]

Web サイトについての説明を編集します。サイトの名称や、利用目的などを入力するとポリシーの管理が容易になります。

## 14.4.9 ［アプリケーションの追加］ダイアログ

［アプリケーションの追加］ダイアログでは、利用を許可するアプリケーションと禁止するアプリケーションを追加できます。また、利用を許可するアプリケーションについては、インストールが必須かどうかも設定できます。

### 画面




### 項目

表示される入力項目を次に示します。

[登録種別]

登録するアプリケーションの利用を許可するか、または禁止するかを選択します。利用を許可する場合は［ホワイトリスト］を、禁止する場合は［ブラックリスト］を選択してください。

[アプリケーション名]

利用を許可、または禁止するアプリケーションの名称を入力します。

[バージョン]

利用を許可、または禁止するアプリケーションのバージョンを入力します。

すべてのバージョンを対象とする場合は「*」（アスタリスク）を入力します。

[必須]

利用を許可するアプリケーションのインストールを必須にするか、または任意にするかを設定します。インストールを必須にする場合、［必須にする］をチェックします。

[対象 OS]

利用を許可、または禁止するアプリケーションの対象とする OS を設定します。

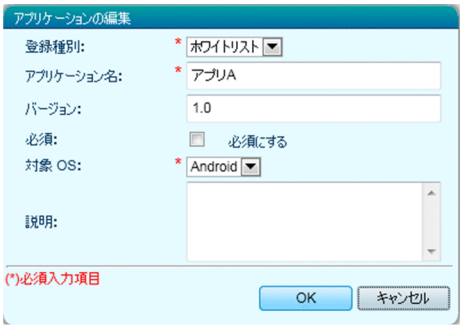
[説明]

登録するアプリケーションについての説明を入力します。アプリケーションの利用目的などを入力するとアプリケーションの管理が容易になります。

## 14.4.10 ［アプリケーションの編集］ダイアログ

［アプリケーションの編集］ダイアログでは、利用を許可するアプリケーションと禁止するアプリケーションを編集できます。また、利用を許可するアプリケーションについては、インストールが必須かどうかも編集できます。

### 画面




### 項目

表示される入力項目を次に示します。

[登録種別]

登録するアプリケーションの利用を許可するか、または禁止するかを選択します。利用を許可する場合は［ホワイトリスト］を、禁止する場合は［ブラックリスト］を選択してください。

[アプリケーション名]

利用を許可、または禁止するアプリケーションの名称を編集します。

[バージョン]

利用を許可、または禁止するアプリケーションのバージョンを編集します。

[必須]

利用を許可するアプリケーションのインストールを必須にするか、または任意にするかを設定します。インストールを必須にする場合、［必須にする］をチェックします。

[対象 OS]

利用を許可、または禁止するアプリケーションの対象とする OS を設定します。

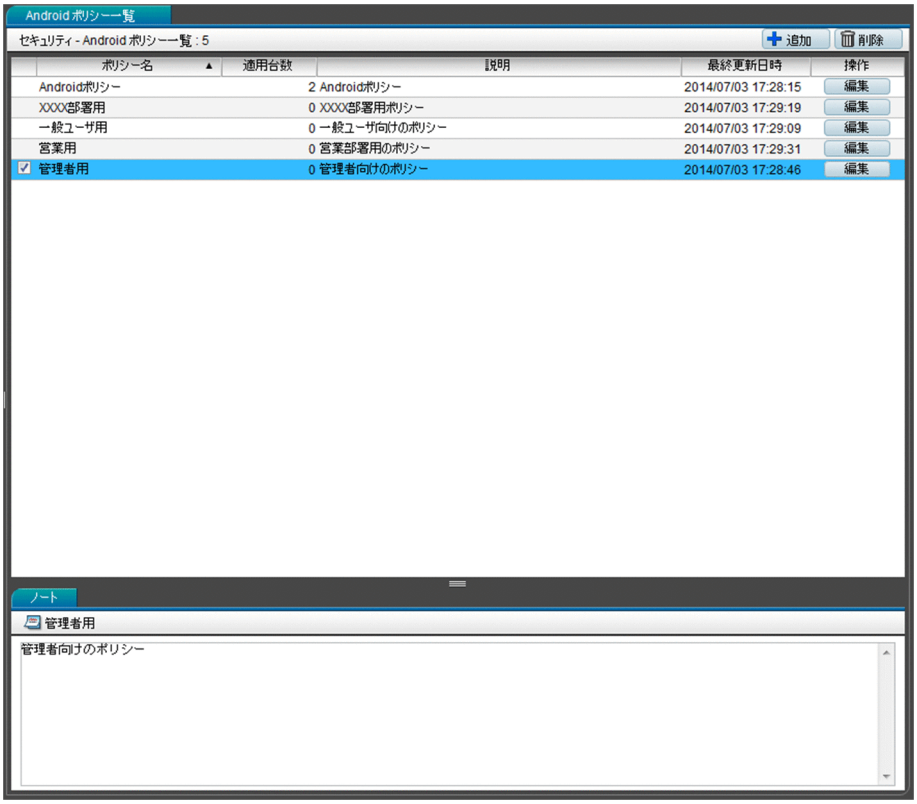
[説明]

アプリケーションについての説明を編集します。アプリケーションの利用目的などを入力するとアプリケーションの管理が容易になります。

## 14.4.11 [Android ポリシー一覧] 画面

[Android ポリシー一覧] 画面では、作成した Android ポリシーの一覧が表示されます。また、Android ポリシーの追加、編集、および削除ができます。

### 画面




### 項目

表示されるボタンおよびタブを次に示します。

[追加] ボタン

新規に Android ポリシーを追加します。

[削除] ボタン

選択した Android ポリシーを削除します。

[編集] ボタン（[参照] ボタン）

選択した Android ポリシーを編集します。

参照権限のアカウントでログインしている場合は、［参照］ボタンが表示され、選択した Android ポリシーの内容を確認できます。

［ノート］タブ

インフォメーションエリア下部に、選択している Android ポリシーの説明が表示されます。システム管理権限のアカウントでログインしている場合は、Android ポリシーの説明を編集できます。

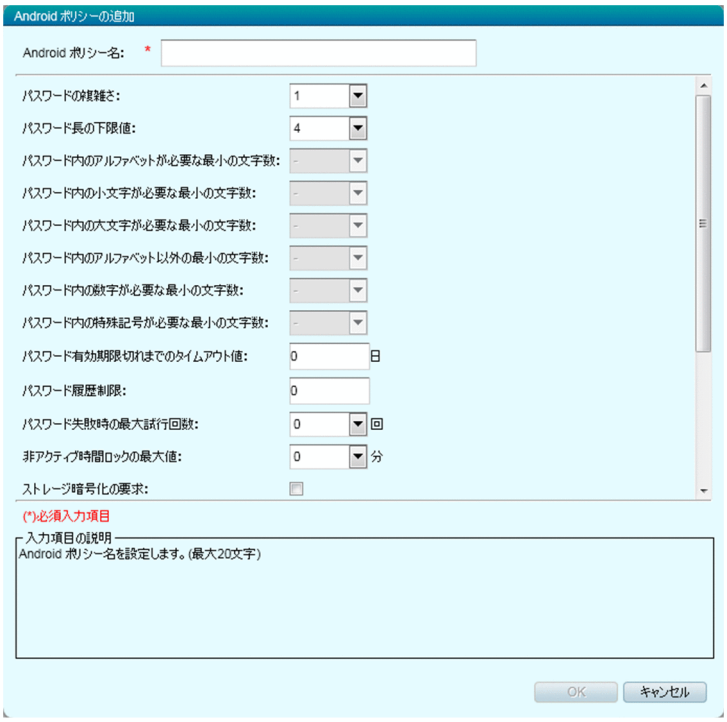
**関連項目**

- 14.4.12 ［Android ポリシーの追加］ダイアログ
- 14.4.13 ［Android ポリシーの編集］ダイアログ
- 14.4.14 ［Android ポリシーの参照］ダイアログ

## 14.4.12 ［Android ポリシーの追加］ダイアログ

［Android ポリシーの追加］ダイアログでは、新規に Android ポリシーを追加できます。

**画面**

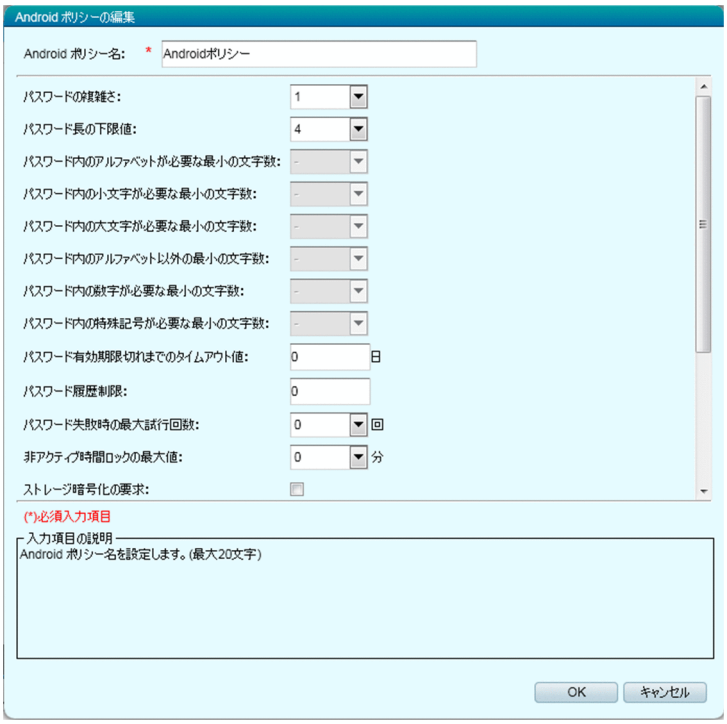


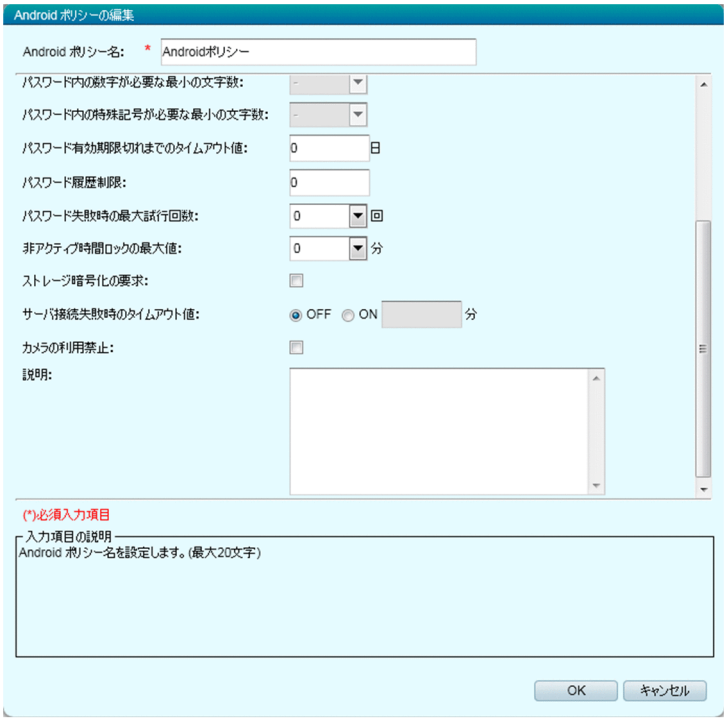
入力項目を選択すると、入力項目の説明に、選択した項目の説明が表示されます。

## 14.4.13 ［Android ポリシーの編集］ダイアログ

［Android ポリシーの編集］ダイアログでは、作成した Android ポリシーを変更できます。

### 画面



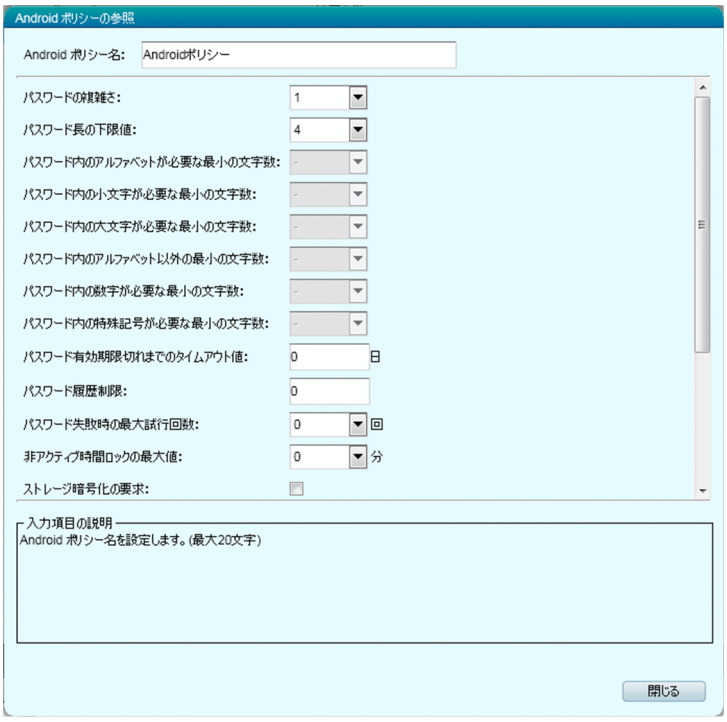


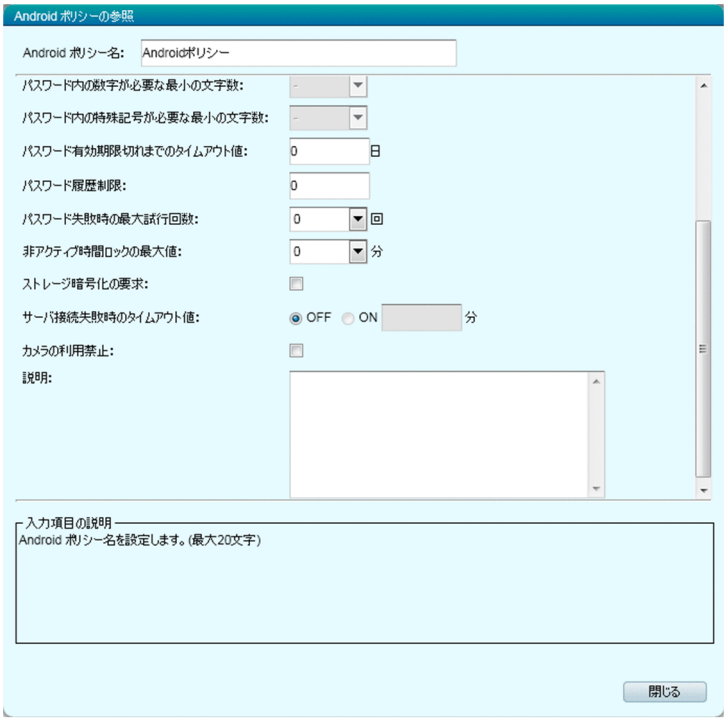

入力項目を選択すると、入力項目の説明に、選択した項目の説明が表示されます。

## 14.4.14 [Android ポリシーの参照] ダイアログ

[Android ポリシーの参照] ダイアログでは、Android ポリシーの内容を確認できます。

### 画面



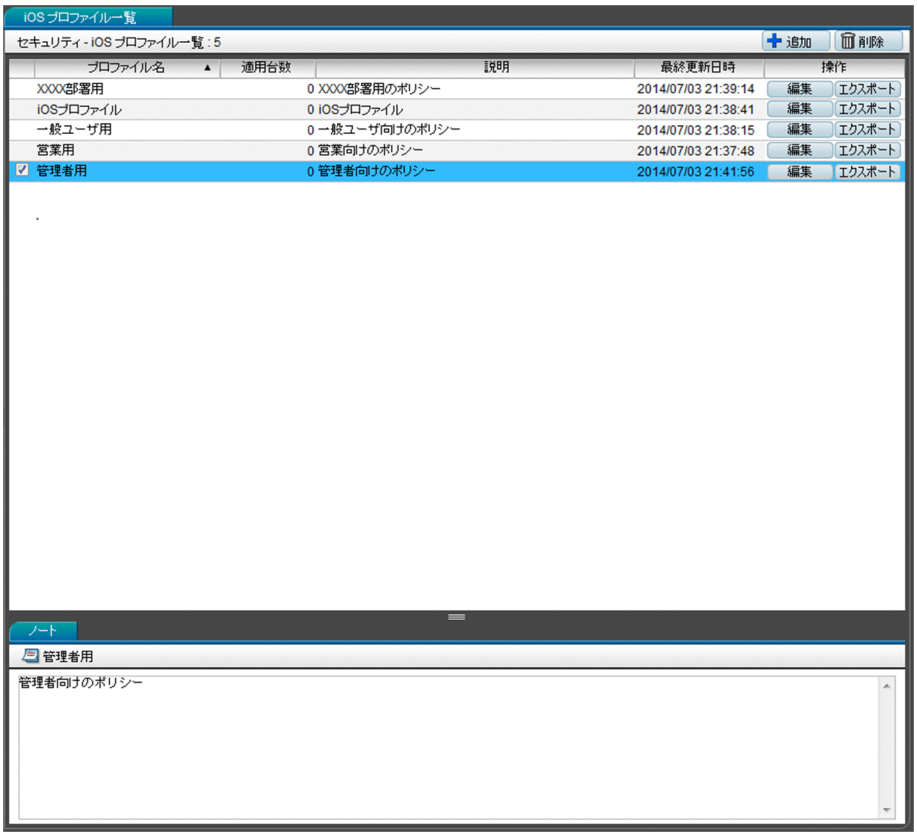



入力項目を選択すると、入力項目の説明に、選択した項目の説明が表示されます。

## 14.4.15 ［iOS プロファイル一覧］画面

［iOS プロファイル一覧］画面では、作成した iOS プロファイルの一覧が表示されます。また、iOS プロファイルの追加、編集、削除、およびエクスポートができます。

## 画面




## 項目

表示されるボタンおよびタブを次に示します。

[追加] ボタン

新規に iOS プロファイルを追加します。

[削除] ボタン

選択した iOS プロファイルを削除します。

[編集] ボタン

選択した iOS プロファイルの情報を編集します。

[エクスポート] ボタン

選択した iOS プロファイルの内容をエクスポートします。

[ノート] タブ

インフォメーションエリア下部に、選択している iOS プロファイルの説明が表示されます。システム管理権限のアカウントでログインしている場合は、iOS プロファイルの説明を編集できます。

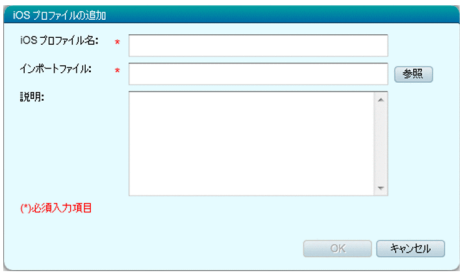
## 関連項目

- 14.4.16 [iOS プロファイルの追加] ダイアログ
- 14.4.17 [iOS プロファイル情報の編集] ダイアログ

## 14.4.16 ［iOS プロファイルの追加］ダイアログ

［iOS プロファイルの追加］ダイアログでは、iPhone 構成ユーティリティで作成した構成プロファイルを読み込み、iOS プロファイルとして追加します。

### 画面




### 項目

表示される入力項目を次に示します。

［iOS プロファイル名］

iOS プロファイル名を入力します。

［インポートファイル］

［参照］ボタンをクリックして、iPhone 構成ユーティリティで作成した構成プロファイルを指定します。

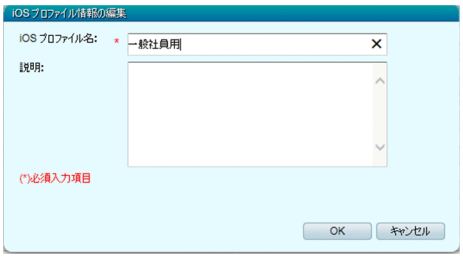
［説明］

追加する iOS プロファイルについての補足情報を入力します。iOS プロファイルの利用目的などを入力すると iOS プロファイルの管理が容易になります。

## 14.4.17 ［iOS プロファイル情報の編集］ダイアログ

［iOS プロファイル情報の編集］ダイアログでは、作成した iOS プロファイルの情報を編集できます。

### 画面




### 項目

表示される入力項目を次に示します。

[iOS プロファイル名]

iOS プロファイル名を編集します。

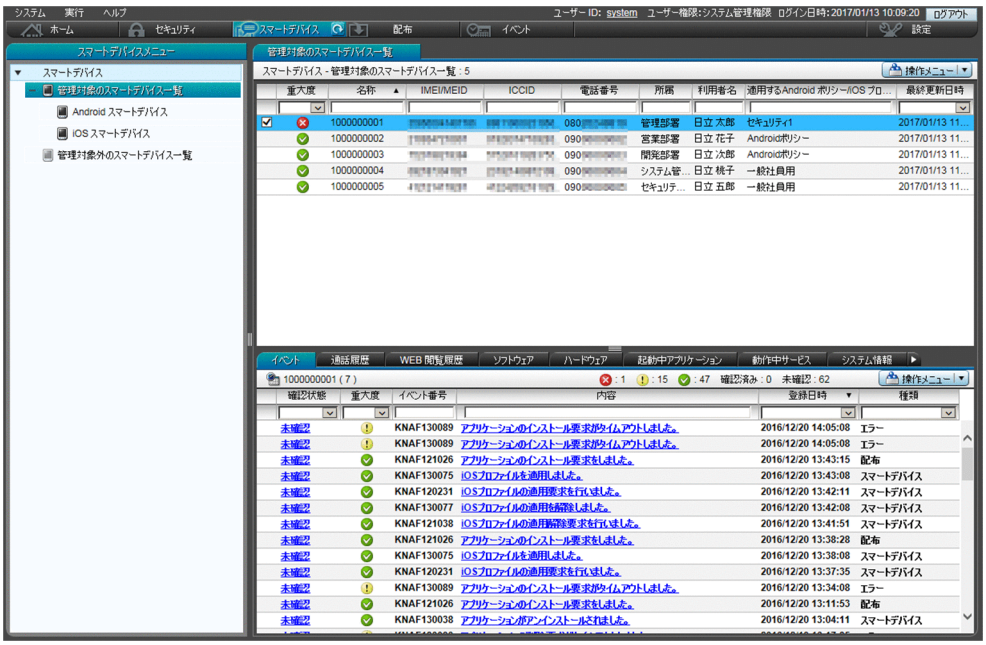
[説明]

iOS プロファイルについての補足情報を編集します。

# 14.5　スマートデバイス画面

スマートデバイス画面では、スマートデバイスの情報を管理できます。また、スマートデバイスへのセキュリティのルールの適用や、ロックや初期化などの操作ができます。

### 画面



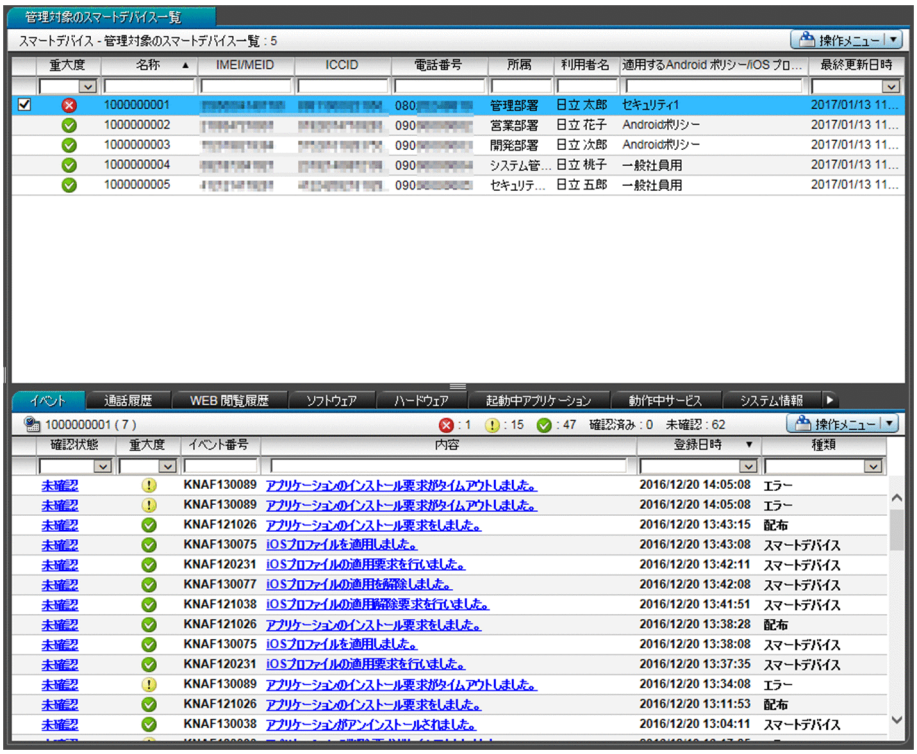

### 関連項目

- 14.5.1 ［管理対象のスマートデバイス一覧］画面
- 14.5.3 ［管理対象外のスマートデバイス一覧］画面

## 14.5.1　［管理対象のスマートデバイス一覧］画面

［管理対象のスマートデバイス一覧］画面では、管理対象のスマートデバイスが、一覧表示されます。スマートデバイスの登録、削除、セキュリティのルールの適用などができます。また、メニューエリアで［Android スマートデバイス］や［iOS スマートデバイス］を選択すると、OS ごとのスマートデバイスの一覧が確認できます。

## 画面




> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

## 項目

[操作メニュー] の項目を次に示します。

[最新の情報を取得する]

選択したスマートデバイスから最新のインベントリ情報を取得します。スマートデバイスは複数選択できます。

[初期化する]

選択したスマートデバイスを初期化します。スマートデバイスは複数選択できます。

[ロックする]

選択したスマートデバイスをロックします。スマートデバイスは複数選択できます。

[パスコードをリセットする]

選択した iOS 端末のパスコードをリセットします。iOS 端末は複数選択できます。

[メッセージを通知する]

選択した Android 端末にメッセージを通知します。Android 端末は複数選択できます。

[管理対象外にする]

選択したスマートデバイスを管理対象外にします。スマートデバイスは複数選択できます。

[セキュリティポリシーを適用する]

選択したスマートデバイスにセキュリティポリシーを適用します。スマートデバイスは複数選択できます。

[Android ポリシーを適用する]

選択した Android 端末に Android ポリシーを適用します。Android 端末は複数選択できます。

[iOS プロファイルを適用する]

選択した iOS 端末に iOS プロファイルを適用します。iOS 端末は複数選択できます。

[iOS プロファイルの適用を解除する]

選択した iOS 端末の iOS プロファイルの適用を解除します。iOS 端末は複数選択できます。

[スマートデバイスを追加する]

新規にスマートデバイスの情報を登録します。

[スマートデバイス一覧をインポートする]

スマートデバイスの情報を CSV ファイルからインポートします。

[スマートデバイス一覧をエクスポートする]

[管理対象のスマートデバイス一覧] 画面に表示されているスマートデバイスの一覧を CSV ファイルにエクスポートします。

**関連項目**

- 14.5.2 [管理対象のスマートデバイス一覧] 画面で表示されるタブ
- 14.5.5 [スマートデバイスの初期化] ダイアログ
- 14.5.6 [スマートデバイスのロック] ダイアログ
- 14.5.7 [スマートデバイスのパスコードのリセット] ダイアログ
- 14.5.8 [管理対象外にする] ダイアログ
- 14.5.9 [セキュリティポリシーを適用する] ダイアログ
- 14.5.10 [Android ポリシーを適用する] ダイアログ
- 14.5.11 [iOS プロファイルの適用] ダイアログ
- 14.5.12 [iOS プロファイルの適用解除] ダイアログ
- 14.5.13 [スマートデバイスの追加] ダイアログ
- 14.5.14 [スマートデバイス一覧のインポート] ダイアログ
- 14.5.15 [スマートデバイスへのメッセージ通知] ダイアログ
- 付録 H インベントリ情報一覧

## 14.5.2 ［管理対象のスマートデバイス一覧］画面で表示されるタブ

［管理対象のスマートデバイス一覧］画面で表示されるタブでは、インフォメーションエリアで選択したスマートデバイスのイベント一覧や通話履歴などが確認できます。

### ポイント

フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

表示されるタブを次に示します。

### ［イベント］タブ

選択したスマートデバイスで発生したイベントの一覧が表示されます。発生したイベントに対して、次の操作が実行できます。

- ［確認状態］欄に表示されているリンクをクリックして、イベントの確認状態を変更する。
- ［内容］欄に表示されているリンクをクリックして、イベントの詳細を確認する。

［操作メニュー］の項目を次に示します。

［確認済みに設定する］

選択したイベントの確認状態を「確認済み」にします。

［未確認に設定する］

選択したイベントの確認状態を「未確認」にします。

［イベント詳細を表示する］

選択したイベントの詳細を表示します。

### ［通話履歴］タブ

選択したスマートデバイスの通話履歴が表示されます。［確認状態］欄に表示されている状態のリンクをクリックすることで、履歴の確認状態を変更できます。また、通話履歴に表示されている電話番号を、通話を許可する電話番号としてスマートデバイスに適用されているセキュリティポリシーに登録することもできます。

[操作メニュー]の項目を次に示します。

[確認済みに設定する]

選択した通話履歴の確認状態を「確認済み」にします。

[未確認に設定する]

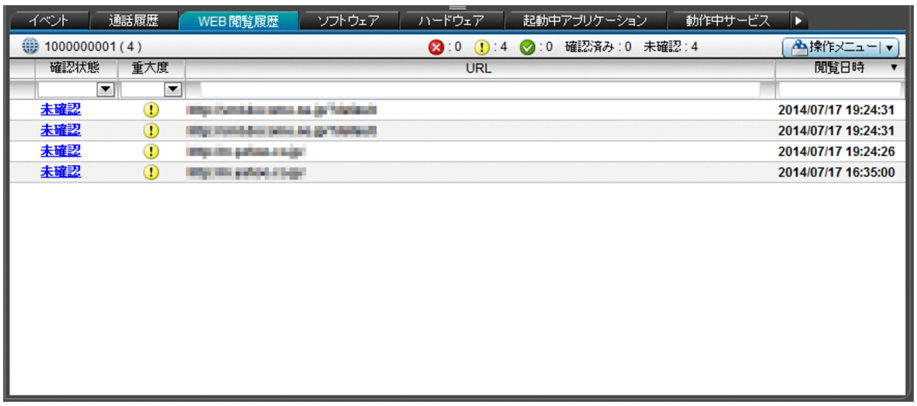
選択した通話履歴の確認状態を「未確認」にします。

[許可する]

選択した通話履歴の電話番号を、通話を許可する電話番号としてスマートデバイスに適用されているセキュリティポリシーに登録します。

### [WEB 閲覧履歴]タブ

選択したスマートデバイスの Web の閲覧履歴が表示されます。[確認状態]欄に表示されている状態のリンクをクリックすることで、履歴の確認状態を変更できます。また、Web の閲覧履歴に表示されている URL を、ホワイトリスト、またはブラックリストとしてスマートデバイスに適用されているセキュリティポリシーに登録することもできます。




[操作メニュー]の項目を次に示します。

[確認済みに設定する]

選択した Web の閲覧履歴の確認状態を「確認済み」にします。

[未確認に設定する]

選択した Web の閲覧履歴の確認状態を「未確認」にします。

[許可する]

選択した Web の閲覧履歴に表示されている URL を、ホワイトリストとしてスマートデバイスに適用されているセキュリティポリシーに登録します。

[禁止する]

選択した Web の閲覧履歴に表示されている URL を、ブラックリストとしてスマートデバイスに適用されているセキュリティポリシーに登録します。

### [ソフトウェア] タブ

選択したスマートデバイスに配布、またはインストールされているアプリケーションが表示されます。[確認状態] 欄に表示されている状態のリンクをクリックすることで、配布またはインストールされているアプリケーションの確認状態を変更できます。また、一覧に表示されているアプリケーションをホワイトリスト、またはブラックリストとしてスマートデバイスに適用されているセキュリティポリシーに登録することもできます。

[操作メニュー] の項目を次に示します。

[確認済みに設定する]

選択したアプリケーションの確認状態を「確認済み」にします。

[未確認に設定する]

選択したアプリケーションの確認状態を「未確認」にします。

[許可する]

選択したアプリケーションを、ホワイトリストとしてスマートデバイスに適用されているセキュリティポリシーに登録します。

[禁止する]

選択したアプリケーションを、ブラックリストとしてスマートデバイスに適用されているセキュリティポリシーに登録します。

### [ハードウェア] タブ

選択したスマートデバイスのシリアル番号や内部ストレージ容量など、ハードウェアに関する情報が表示されます。

### [起動中アプリケーション] タブ

選択したスマートデバイスで起動中のアプリケーションの一覧が表示されます。

### [動作中サービス] タブ

選択したスマートデバイスで動作中のサービスの一覧が表示されます。

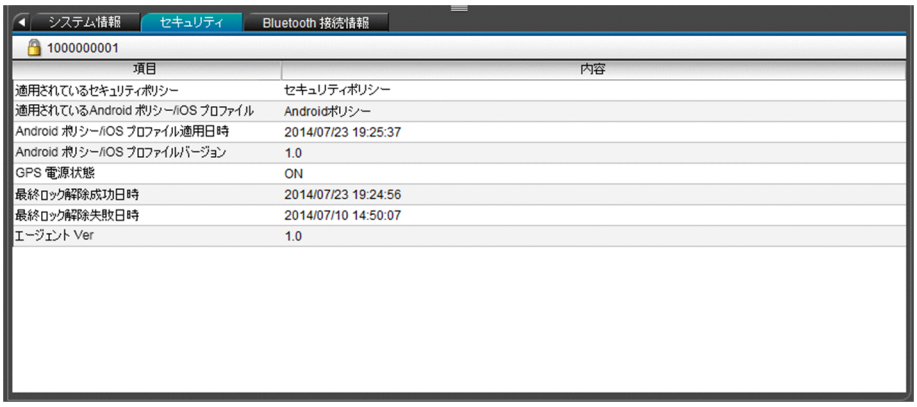
### [システム情報] タブ

選択したスマートデバイスの OS 情報や電話番号など、システムに関する情報が表示されます。

[GPS 情報] のリンクをクリックして地図表示サイトでスマートデバイスの位置を確認できます。

### [セキュリティ] タブ

選択したスマートデバイスに適用されているセキュリティのルール、GPS 電源状態、最後にスマートデバイスをロックした日時など、セキュリティに関する情報が表示されます。




### [Bluetooth 接続情報] タブ

選択したスマートデバイスの Bluetooth 通信を使用した接続履歴が表示されます。[確認状態] 欄に表示されている状態のリンクをクリックすることで、接続履歴の確認状態を変更できます。

［操作メニュー］の項目を次に示します。

［確認済みに設定する］

選択した Bluetooth 接続情報の確認状態を「確認済み」にします。

［未確認に設定する］

選択した Bluetooth 接続情報の確認状態を「未確認」にします。

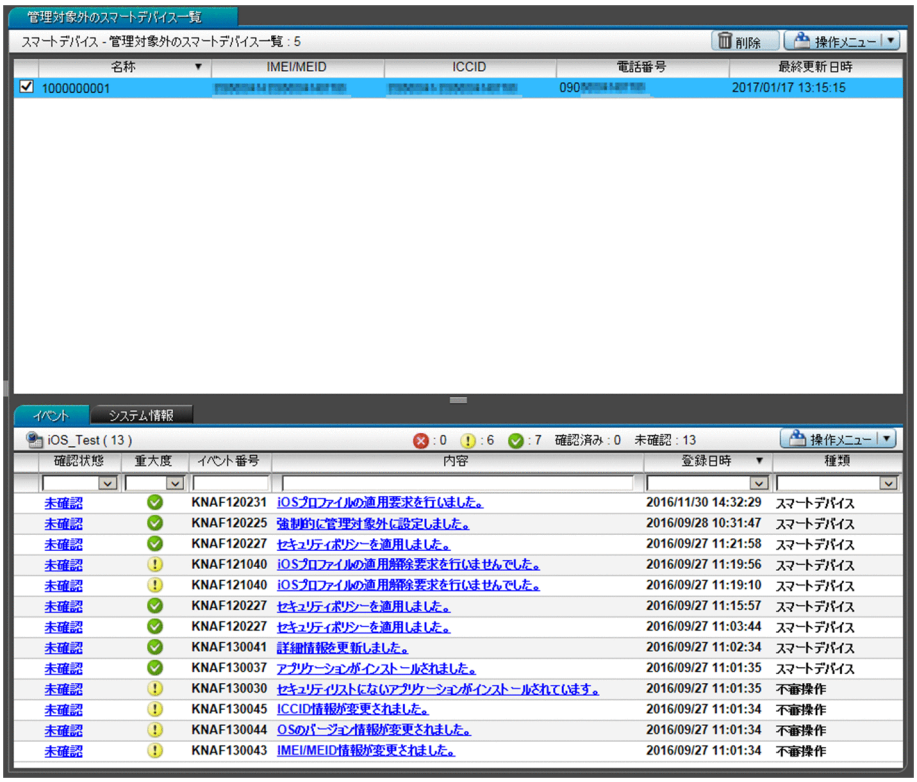
**関連項目**

- 付録 H インベントリ情報一覧

## 14.5.3 ［管理対象外のスマートデバイス一覧］画面

［管理対象外のスマートデバイス一覧］画面では、管理対象外のスマートデバイスの一覧が表示されます。スマートデバイスを削除したり、セキュリティのルールを適用して管理対象にしたりできます。

**画面**




**ヒント**

フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

### 項目

表示されるボタンを次に示します。

［削除］ボタン

選択したスマートデバイスを JP1/ITDM2 - SDM から削除します。

［操作メニュー］の項目を次に示します。

［セキュリティポリシーを適用する］

選択したスマートデバイスにセキュリティポリシーを適用します。スマートデバイスは複数選択できます。

［Android ポリシーを適用する］

選択した Android 端末に Android ポリシーを適用します。Android 端末は複数選択できます。

［iOS プロファイルを適用する］

選択した iOS 端末に iOS プロファイルを適用します。iOS 端末は複数選択できます。

### 関連項目

- 14.5.4 ［管理対象外のスマートデバイス一覧］画面で表示されるタブ
- 14.5.9 ［セキュリティポリシーを適用する］ダイアログ
- 14.5.10 ［Android ポリシーを適用する］ダイアログ
- 14.5.11 ［iOS プロファイルの適用］ダイアログ
- 付録 H インベントリ情報一覧

## 14.5.4 ［管理対象外のスマートデバイス一覧］画面で表示されるタブ

［管理対象外のスマートデバイス一覧］画面で表示されるタブでは、インフォメーションエリアで選択したスマートデバイスのイベント一覧やシステム情報が確認できます。

### ポイント

フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

表示されるタブを次に示します。

### ［イベント］タブ

選択したスマートデバイスで発生したイベントの一覧が表示されます。［確認状態］欄に表示されているリンクをクリックすることで、イベントの確認状態を変更できます。

[操作メニュー] の項目を次に示します。

[確認済みに設定する]

選択したイベントの確認状態を「確認済み」にします。

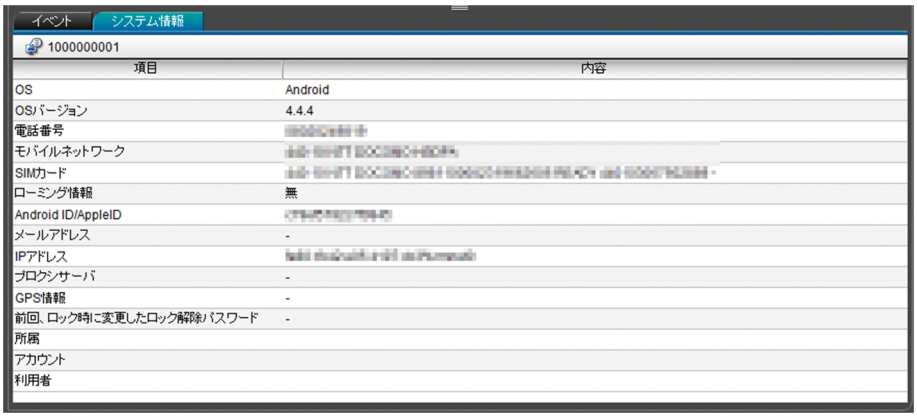
[未確認に設定する]

選択したイベントの確認状態を「未確認」にします。

### [システム情報] タブ

選択したスマートデバイスの OS 情報や電話番号など、システムに関する情報が表示されます。

[GPS 情報] のリンクをクリックして地図表示サイトでスマートデバイスの位置を確認できます。



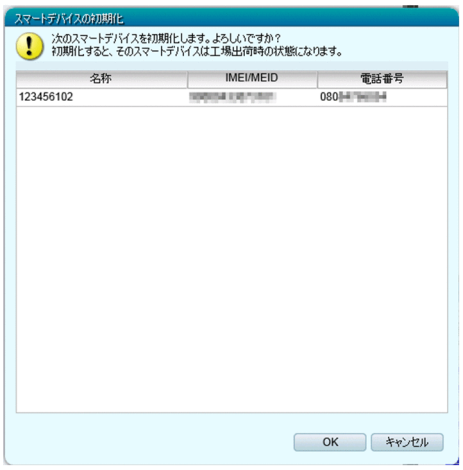

### 関連項目

- 付録 H インベントリ情報一覧

## 14.5.5 [スマートデバイスの初期化] ダイアログ

[スマートデバイスの初期化] ダイアログでは、表示されているスマートデバイスを初期化し、工場出荷時の状態にできます。

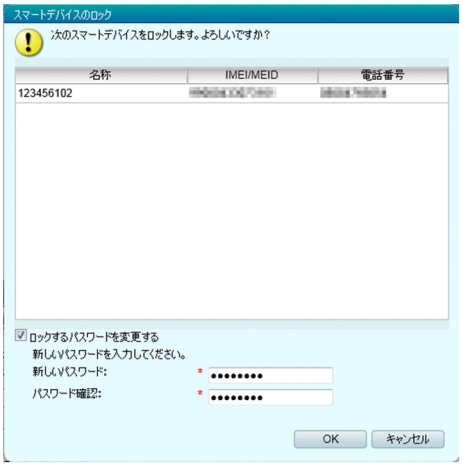
### 画面




## 14.5.6 ［スマートデバイスのロック］ダイアログ

［スマートデバイスのロック］ダイアログでは、表示されているスマートデバイスをロックできます。なお、Android 端末はパスワードの変更もできます。

### 画面




### 項目

表示される入力項目を次に示します。

［ロックするパスワードを変更する］

Android 端末のロック時にパスワードも変更する場合はチェックします。［ロックするパスワードを変更する］をチェックすると、［新しいパスワード］と［パスワード確認］が入力できるようになります。

> **重要**
>
> iOS 端末で［ロックするパスワードを変更する］をチェックしてパスワードを入力しても、パスワードは変更されません。

［新しいパスワード］

新しいパスワードを入力します。

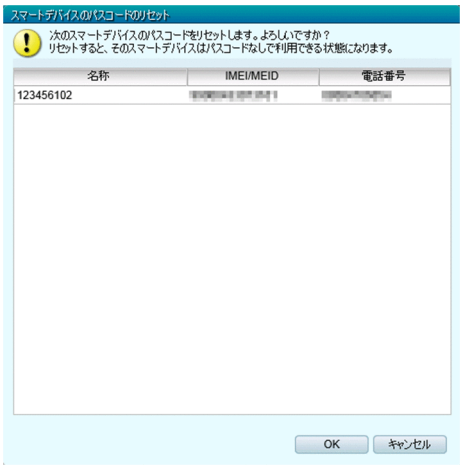
［パスワード確認］

確認のためにパスワードを再入力します。

## 14.5.7 ［スマートデバイスのパスコードのリセット］ダイアログ

［スマートデバイスのパスコードのリセット］ダイアログでは、表示されている iOS 端末のパスコードをリセットできます。

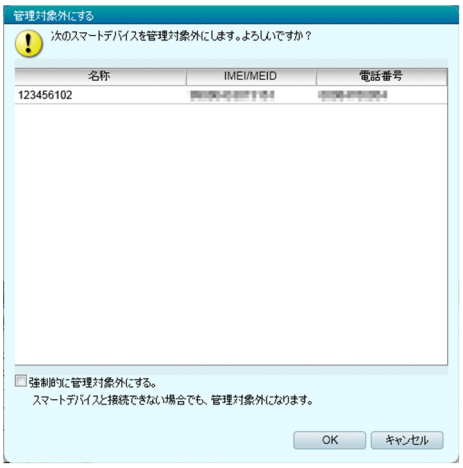
**画面**




## 14.5.8 ［管理対象外にする］ダイアログ

［管理対象外にする］ダイアログでは、表示されているスマートデバイスに適用されているセキュリティのルールを解除し管理対象外にできます。

### 画面




### 項目

表示される入力項目を次に示します。

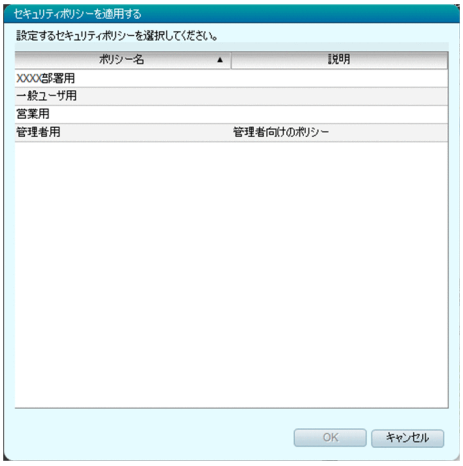
[強制的に管理対象外にする。]

スマートデバイスと接続できない場合でも強制的に管理対象外とするときにチェックします。

## 14.5.9 ［セキュリティポリシーを適用する］ダイアログ

［セキュリティポリシーを適用する］ダイアログでは、スマートデバイスにセキュリティポリシーを適用できます。

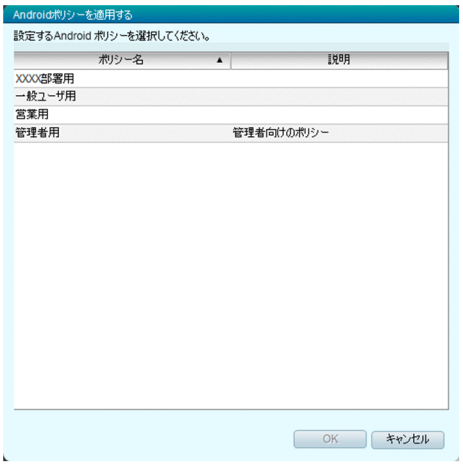
### 画面




## 14.5.10 ［Android ポリシーを適用する］ダイアログ

［Android ポリシーを適用する］ダイアログでは、Android 端末に Android ポリシーを適用できます。

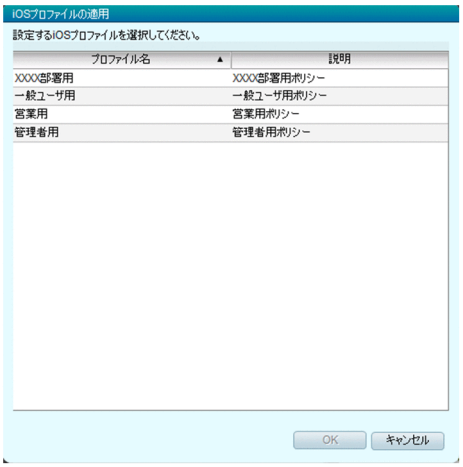
### 画面




## 14.5.11 ［iOS プロファイルの適用］ダイアログ

［iOS プロファイルの適用］ダイアログでは、iOS 端末に iOS プロファイルを適用できます。

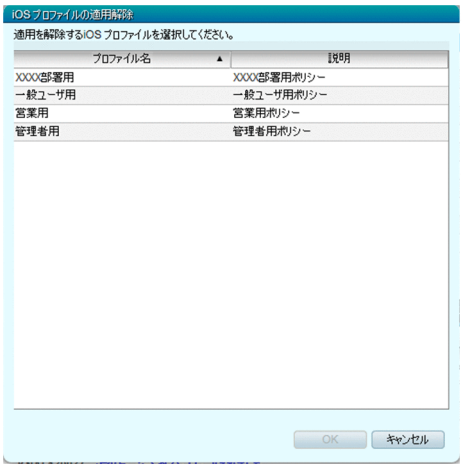
### 画面




## 14.5.12 ［iOS プロファイルの適用解除］ダイアログ

［iOS プロファイルの適用解除］ダイアログでは、iOS 端末の iOS プロファイルの適用を解除できます。

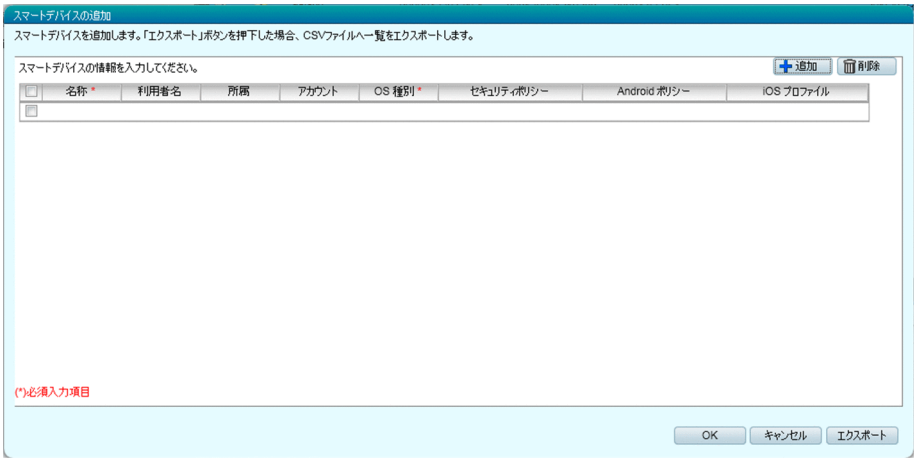
### 画面




## 14.5.13 ［スマートデバイスの追加］ダイアログ

［スマートデバイスの追加］ダイアログでは、管理するスマートデバイスを JP1/ITDM2 - SDM に登録できます。

### 画面




### 項目

表示されるボタンを次に示します。

［追加］ボタン

　スマートデバイスの情報を入力できる行を追加します。

［削除］ボタン

　選択した行を削除します。行は複数選択できます。

［エクスポート］ボタン

　入力した情報を CSV ファイルに出力します。

スマートデバイスの情報の入力項目を次に示します。

[名称]
　資産管理番号など、名称を入力します。

[利用者名]
　利用者名を入力します。

[所属]
　利用者の所属を入力します。

[アカウント]
　社員 ID やメールアドレスなどの情報を入力します。

[OS 種別]
　OS 種別を選択します。

[セキュリティポリシー]
　適用するセキュリティポリシーを選択します。

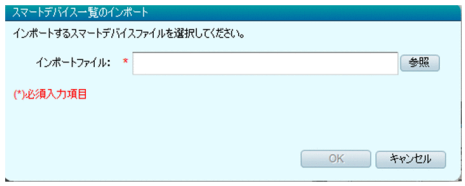
[Android ポリシー]
　適用する Android ポリシーを選択します。

[iOS プロファイル]
　適用する iOS プロファイルを選択します。

## 14.5.14 ［スマートデバイス一覧のインポート］ダイアログ

［スマートデバイス一覧のインポート］ダイアログでは、複数のスマートデバイスの情報を入力した CSV ファイルをインポートすることで、情報を JP1/ITDM2 - SDM に一括登録できます。

### 画面




### 項目

表示される入力項目を次に示します。

[インポートファイル]
　［参照］ボタンをクリックして、スマートデバイスの情報を入力した CSV ファイルを指定します。

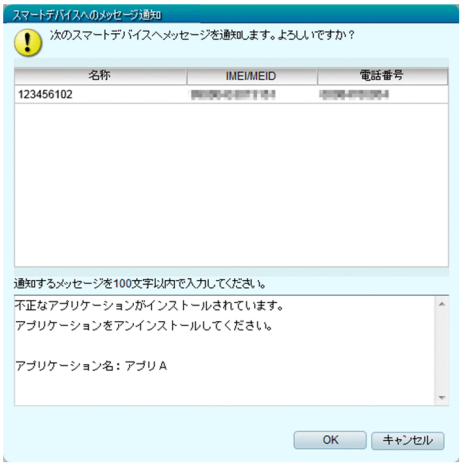
### 関連項目

- 付録 E インポート・エクスポートファイルの出力形式

## 14.5.15 ［スマートデバイスへのメッセージ通知］ダイアログ

［スマートデバイスへのメッセージ通知］ダイアログでは、表示されている Android 端末にメッセージを通知できます。

### 画面




### 項目

表示される入力項目を次に示します。

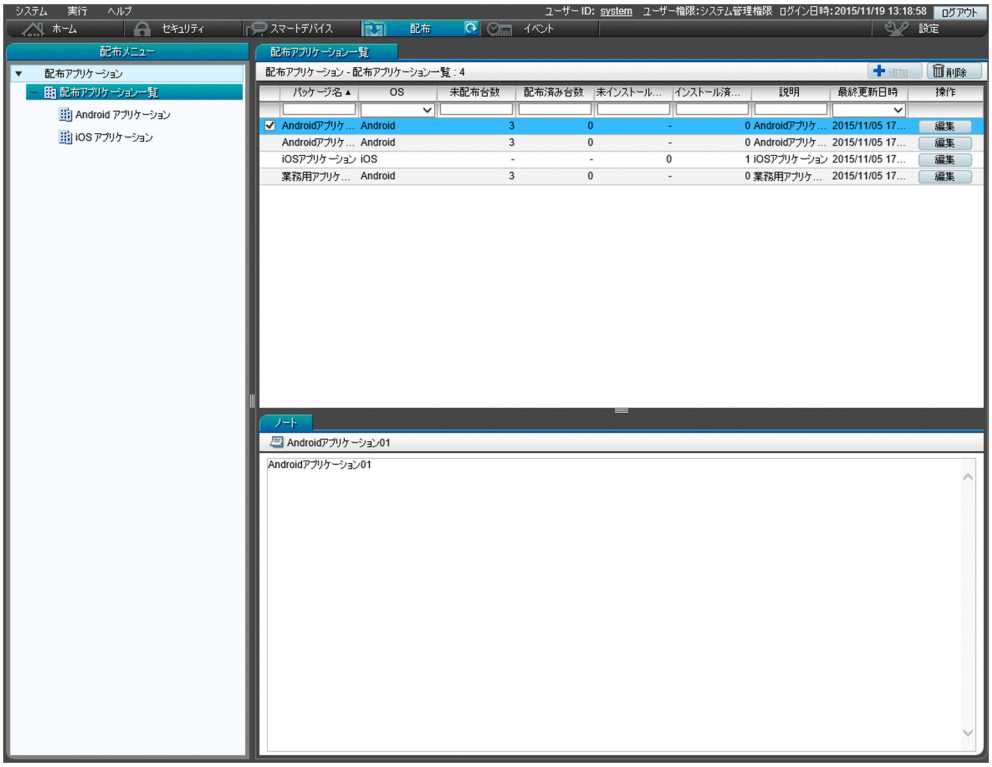
［通知するメッセージを 100 文字以内で入力してください。］

Android 端末に通知するメッセージを入力します。

# 14.6　配布画面

配布画面では、JP1/ITDM2 - SDM で配布するアプリケーションを管理できます。配布するアプリケーションを追加したり、インストールを指示したりできます。

### 画面



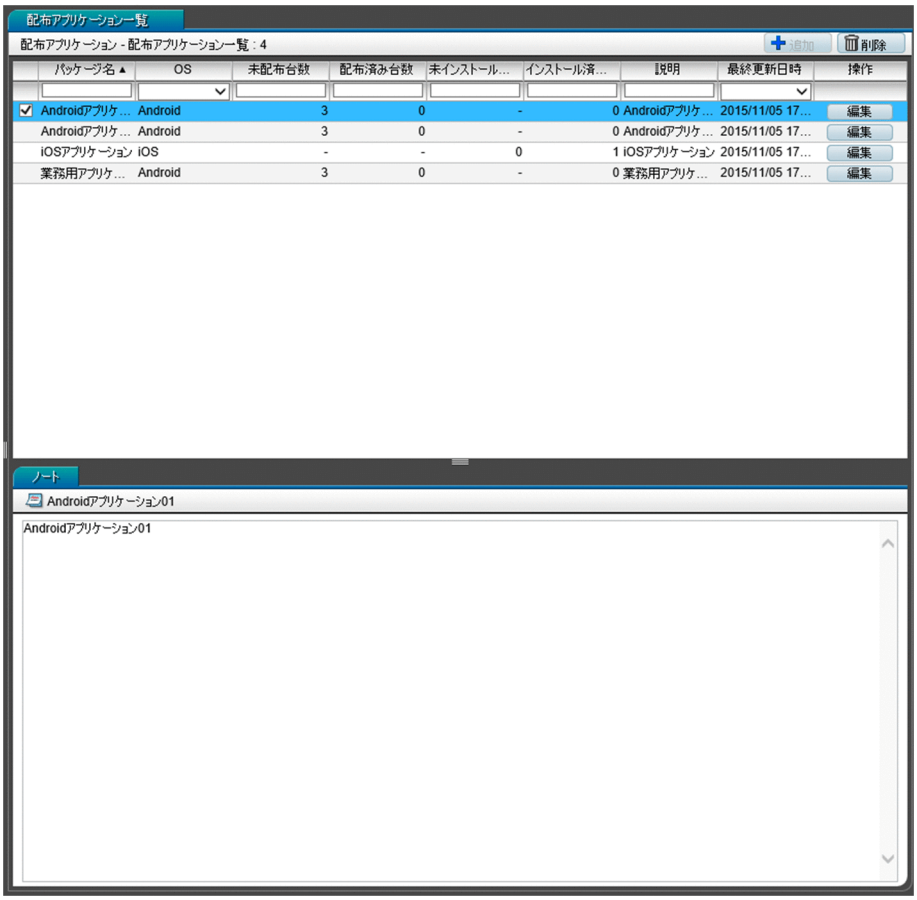

### 関連項目

- 14.6.1 ［配布アプリケーション一覧］画面
- 14.6.2 ［Android アプリケーション］画面
- 14.6.4 ［iOS アプリケーション］画面

## 14.6.1　［配布アプリケーション一覧］画面

［配布アプリケーション一覧］画面では、登録したアプリケーションの一覧が表示されます。また、アプリケーションの編集、および削除ができます。

## 画面




> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

## 項目

表示されるボタンおよびタブを次に示します。

[削除] ボタン

選択したアプリケーションを削除します。

[編集] ボタン（[参照] ボタン）

選択したアプリケーションを編集します。

参照権限のアカウントでログインしている場合は、[参照] ボタンが表示され、選択したアプリケーションの内容を確認できます。

[ノート] タブ

インフォメーションエリア下部に、選択しているアプリケーションの説明が表示されます。システム管理権限のアカウントでログインしている場合は、アプリケーションの説明を編集できます。

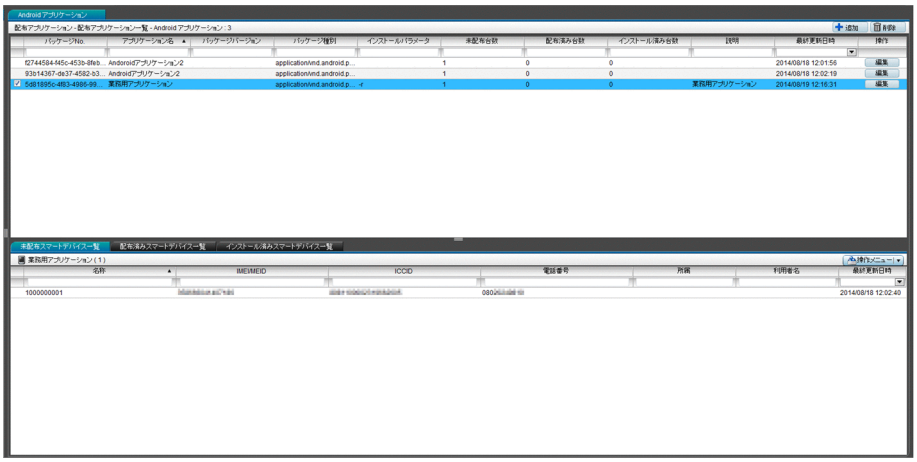
### 関連項目

- 14.6.7 ［Android アプリケーションの編集］ダイアログ
- 14.6.8 ［Android アプリケーションの参照］ダイアログ
- 14.6.10 ［iOS アプリケーションの編集］ダイアログ
- 14.6.11 ［iOS アプリケーションの参照］ダイアログ

## 14.6.2 ［Android アプリケーション］画面

［Android アプリケーション］画面では、登録した Android アプリケーションの一覧が表示されます。また、Android アプリケーションの追加、編集、および削除ができます。

### 画面



> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

### 項目

表示されるボタンを次に示します。

［追加］ボタン

新規に Android アプリケーションを追加します。

［削除］ボタン

選択した Android アプリケーションを削除します。

［編集］ボタン（［参照］ボタン）

選択した Android アプリケーションを編集します。

参照権限のアカウントでログインしている場合は、[参照] ボタンが表示され、選択した Android アプリケーションの内容を確認できます。

**関連項目**

- 14.6.3 [Android アプリケーション] 画面で表示されるタブ
- 14.6.6 [Android アプリケーションの追加] ダイアログ
- 14.6.7 [Android アプリケーションの編集] ダイアログ
- 14.6.8 [Android アプリケーションの参照] ダイアログ

## 14.6.3 [Android アプリケーション] 画面で表示されるタブ

[Android アプリケーション] 画面で表示されるタブでは、インフォメーションエリアで選択した Android アプリケーションの配布状況やインストール状況などが確認できます。

**ポイント**

フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

表示されるタブを次に示します。

**[未配布スマートデバイス一覧] タブ**

選択した Android アプリケーションを配布していないスマートデバイスの情報が表示されます。

[操作メニュー] の項目を次に示します。

[アプリケーション配布]

選択した Android 端末に Android アプリケーションを配布します。

[アプリケーションインストール]

選択した Android 端末に Android アプリケーションを配布し、インストールを指示します。

### [配布済みスマートデバイス一覧] タブ

選択した Android アプリケーションを配布したスマートデバイスの情報が表示されます。

[操作メニュー] の項目を次に示します。

[アプリケーションインストール]

選択したスマートデバイスに Android アプリケーションのインストールを指示します。

[アプリケーション削除]

選択したスマートデバイスに Android アプリケーションのアンインストールを指示し、配布した Android アプリケーションを削除します。

### [インストール済みスマートデバイス一覧] タブ

選択した Android アプリケーションをインストールしたスマートデバイスの情報が表示されます。

[操作メニュー] の項目を次に示します。

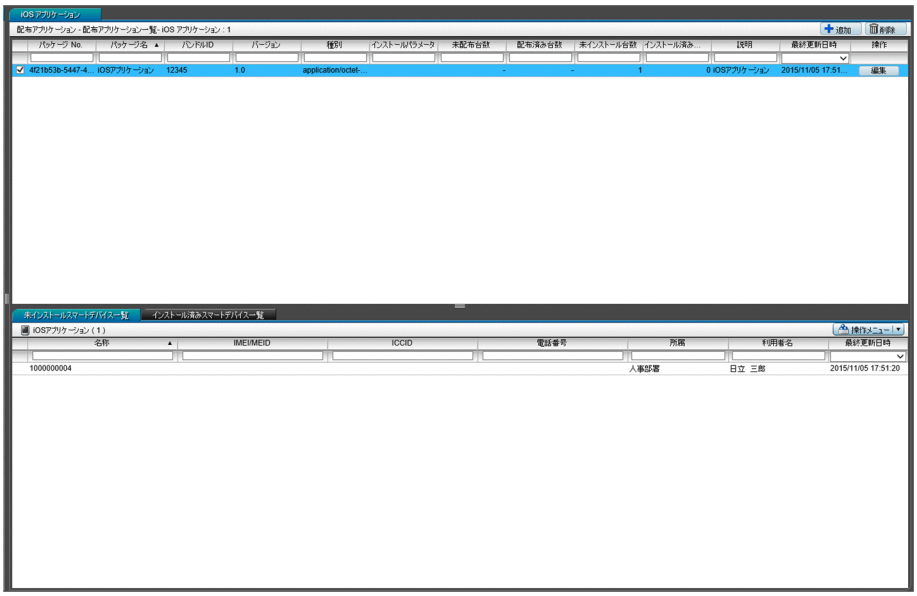
[アプリケーション削除]

選択したスマートデバイスに Android アプリケーションのアンインストールを指示し、配布した Android アプリケーションを削除します。

## 14.6.4 ［iOS アプリケーション］画面

［iOS アプリケーション］画面では、登録した iOS アプリケーションの一覧が表示されます。また、iOS アプリケーションの追加、編集、および削除ができます。

### 画面



> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

### 項目

表示されるボタンを次に示します。

［追加］ボタン

新規に iOS アプリケーションを追加します。

［削除］ボタン

選択した iOS アプリケーションを削除します。

［編集］ボタン（［参照］ボタン）

選択した iOS アプリケーションを編集します。

参照権限のアカウントでログインしている場合は、［参照］ボタンが表示され、選択した iOS アプリケーションの内容を確認できます。

### 関連項目

- 14.6.5 ［iOS アプリケーション］画面で表示されるタブ
- 14.6.9 ［iOS アプリケーションの追加］ダイアログ

- 14.6.10 ［iOS アプリケーションの編集］ダイアログ
- 14.6.11 ［iOS アプリケーションの参照］ダイアログ

## 14.6.5 ［iOS アプリケーション］画面で表示されるタブ

［iOS アプリケーション］画面で表示されるタブでは、インフォメーションエリアで選択した iOS アプリケーションのインストール状況が確認できます。

**ポイント**

フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

表示されるタブを次に示します。

### ［未インストールスマートデバイス一覧］タブ

選択した iOS アプリケーションをインストールしていないスマートデバイスの情報が表示されます。

［操作メニュー］の項目を次に示します。

［アプリケーションインストール］

選択したスマートデバイスに iOS アプリケーションを配布し、インストールを指示します。

### ［インストール済みスマートデバイス一覧］タブ

選択した iOS アプリケーションをインストールしたスマートデバイスの情報が表示されます。

[操作メニュー] の項目を次に示します。

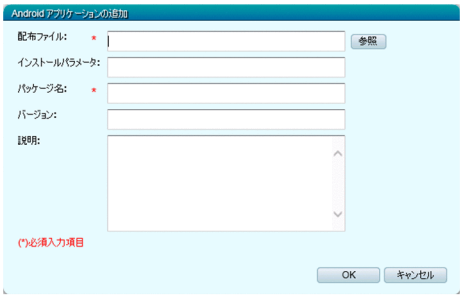
[アプリケーション削除]

選択したスマートデバイスに iOS アプリケーションのアンインストールを指示し、配布した iOS アプリケーションを削除します。

## 14.6.6 [Android アプリケーションの追加] ダイアログ

[Android アプリケーションの追加] ダイアログでは、配布する Android アプリケーションを JP1/ITDM2 - SDM に登録できます。

### 画面




### 項目

表示される入力項目を次に示します。

[配布ファイル]

[参照] ボタンをクリックし、登録する Android アプリケーションを指定します。

[インストールパラメータ]

インストール時のパラメーターを入力します。

[パッケージ名]

Android アプリケーション名を入力します。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

[バージョン]

Android アプリケーションのパッケージバージョンを入力します。

[説明]

登録する Android アプリケーションについての説明を入力します。Android アプリケーションの利用目的などを入力すると Android アプリケーションの管理が容易になります。

## 14.6.7 [Android アプリケーションの編集] ダイアログ

[Android アプリケーションの編集] ダイアログでは、登録済みの Android アプリケーションの情報を編集できます。

### 画面

### 項目

表示される入力項目を次に示します。

[インストールパラメータ]

インストール時のパラメーターを入力します。

[パッケージ名]

Android アプリケーション名を入力します。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

[説明]

Android アプリケーションについての説明を入力します。Android アプリケーションの利用目的などを入力すると Android アプリケーションの管理が容易になります。

## 14.6.8 [Android アプリケーションの参照] ダイアログ

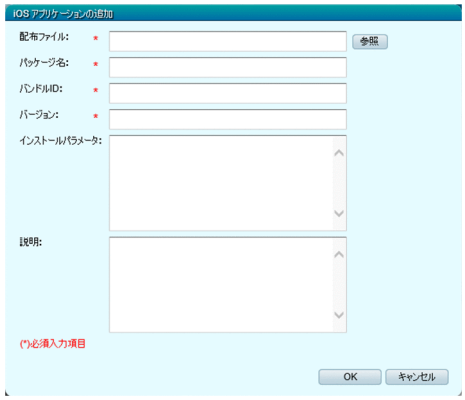
[Android アプリケーションの参照] ダイアログでは、登録済みの Android アプリケーションの内容を確認できます。

### 画面

## 14.6.9 ［iOS アプリケーションの追加］ダイアログ

［iOS アプリケーションの追加］ダイアログでは、配布する iOS アプリケーションを JP1/ITDM2 - SDM に登録できます。

### 画面




### 項目

表示される入力項目を次に示します。

［配布ファイル］

［参照］ボタンをクリックし、登録する iOS アプリケーションを指定します。

［パッケージ名］

iOS アプリケーション名を入力します。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

［バンドル ID］

iOS アプリケーションのバンドル ID を入力します。

［バージョン］

iOS アプリケーションのパッケージバージョンを入力します。

［インストールパラメータ］

iOS アプリケーションのインストールパラメーターを入力します。

指定可能なオプションを次に示します。詳細については、Apple 社のホームページなどで確認してください。

- マネージメントフラグオプション
- App Install オプション
- Managed App Configuration and Feedback オプション
- Managed Application Attributes Queries App Attribute オプション

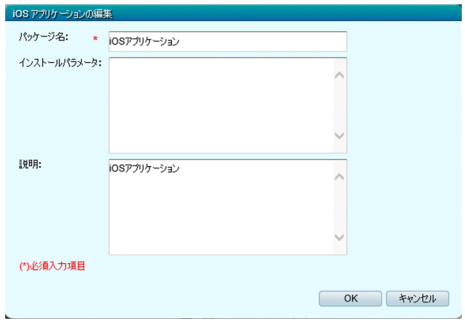
[説明]

登録する iOS アプリケーションについての説明を入力します。iOS アプリケーションの利用目的などを入力すると iOS アプリケーションの管理が容易になります。

## 14.6.10 ［iOS アプリケーションの編集］ダイアログ

［iOS アプリケーションの編集］ダイアログでは、登録済みの iOS アプリケーションの情報を編集できます。

### 画面




### 項目

表示される入力項目を次に示します。

[パッケージ名]

iOS アプリケーション名を入力します。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

[インストールパラメータ]

iOS アプリケーションのインストールパラメーターを入力します。

指定可能なオプションを次に示します。詳細については、Apple 社のホームページなどで確認してください。

- マネージメントフラグオプション
- App Install オプション
- Managed App Configuration and Feedback オプション
- Managed Application Attributes Queries App Attribute オプション

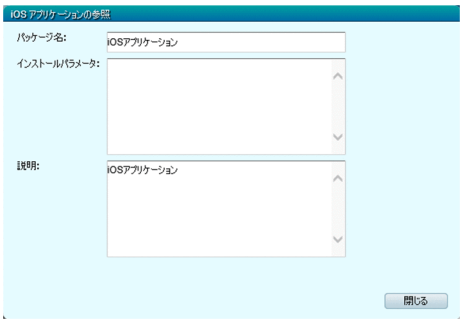
[説明]

iOS アプリケーションについての説明を入力します。iOS アプリケーションの利用目的などを入力すると iOS アプリケーションの管理が容易になります。

## 14.6.11 [iOS アプリケーションの参照] ダイアログ

[iOS アプリケーションの参照] ダイアログでは、登録済みの iOS アプリケーションの内容を確認できます。

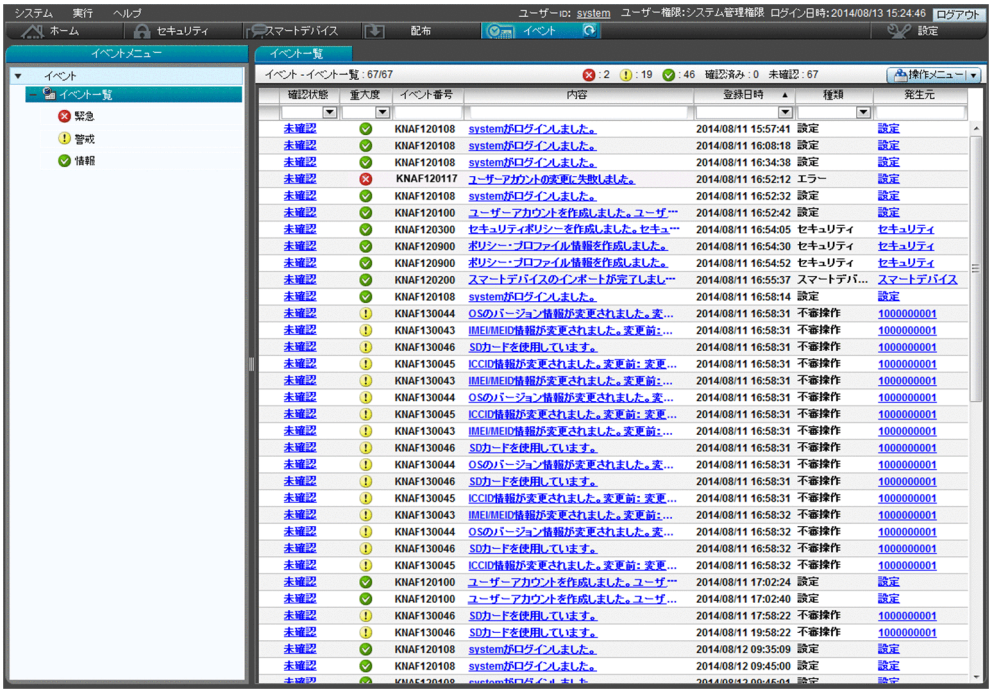
### 画面



# 14.7　イベント画面

イベント画面では、JP1/ITDM2 - SDM の運用中に発生したイベントを確認できます。また、イベントの詳細を確認したり、イベント一覧を CSV ファイルにエクスポートしたりできます。

## 画面



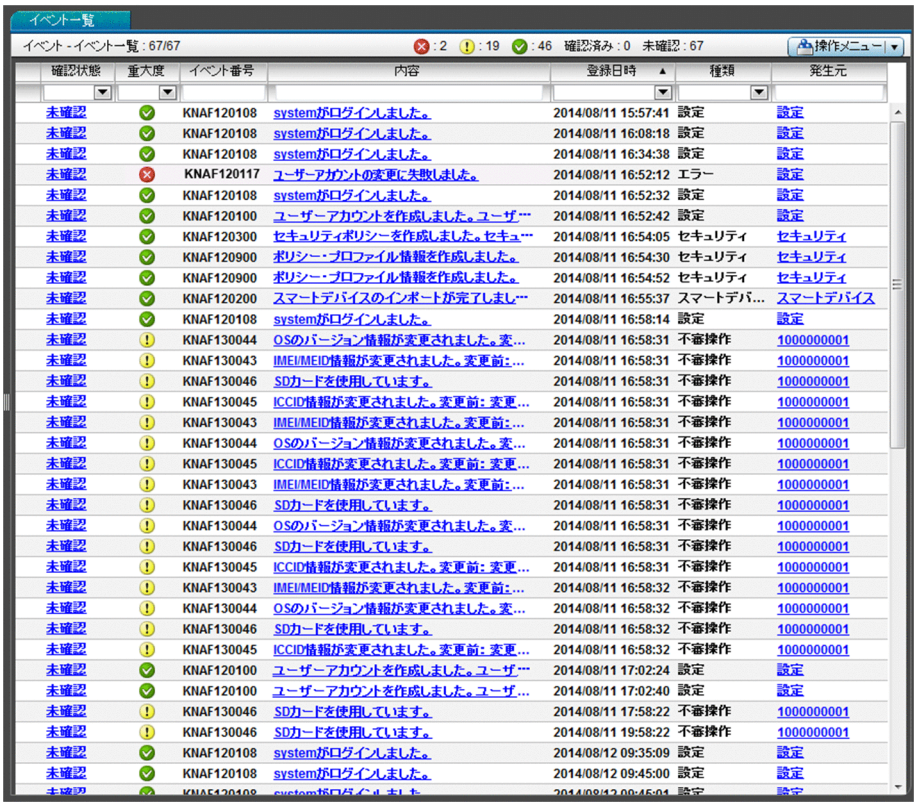

## 関連項目

- 14.7.1　［イベント一覧］画面

# 14.7.1　［イベント一覧］画面

［イベント一覧］画面では、JP1/ITDM2 - SDM の運用中に発生したイベントが表示されます。発生したイベントに対して、イベントの詳細を確認したり、イベント一覧を CSV ファイルにエクスポートしたりできます。

## 画面




> **ヒント**
>
> フィルタを利用すると表示する情報を絞り込めます。フィルタのテキストボックスに入力した内容で、前方一致のフィルタリングをします。

発生したイベントに対して、次に示す操作ができます。

- [確認状態] 欄に表示されているリンクをクリックして、イベントの確認状態を変更する。
- [内容] 欄に表示されているリンクをクリックして、イベントの詳細を確認する。
- [発生元] 欄に表示されているリンクをクリックして、イベントの発生元になった画面を表示する。
- イベント一覧を CSV ファイルにエクスポートする。

## 項目

[操作メニュー] の項目を次に示します。

[イベント詳細を表示する]

選択したイベントの詳細を表示します。

[発生元の情報を表示する]

スマートデバイス画面や設定画面など、選択したイベントの発生元の画面を表示します。

[確認済みに設定する]

選択したイベントの確認状態を「確認済み」にします。

[未確認に設定する]

選択したイベントの確認状態を「未確認」にします。

[イベント一覧をエクスポートする]

表示されているイベント一覧を CSV ファイルにエクスポートします。

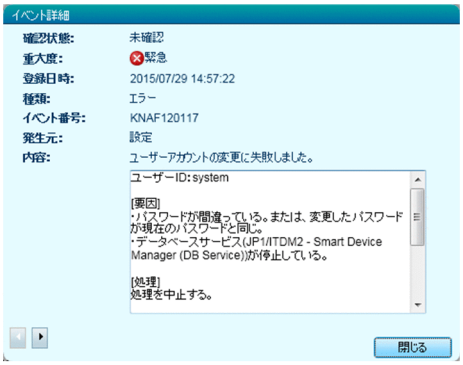
### 関連項目

- 14.7.2 ［イベント詳細］ダイアログ

## 14.7.2 ［イベント詳細］ダイアログ

［イベント詳細］ダイアログでは、イベントの詳細情報を確認できます。

### 画面



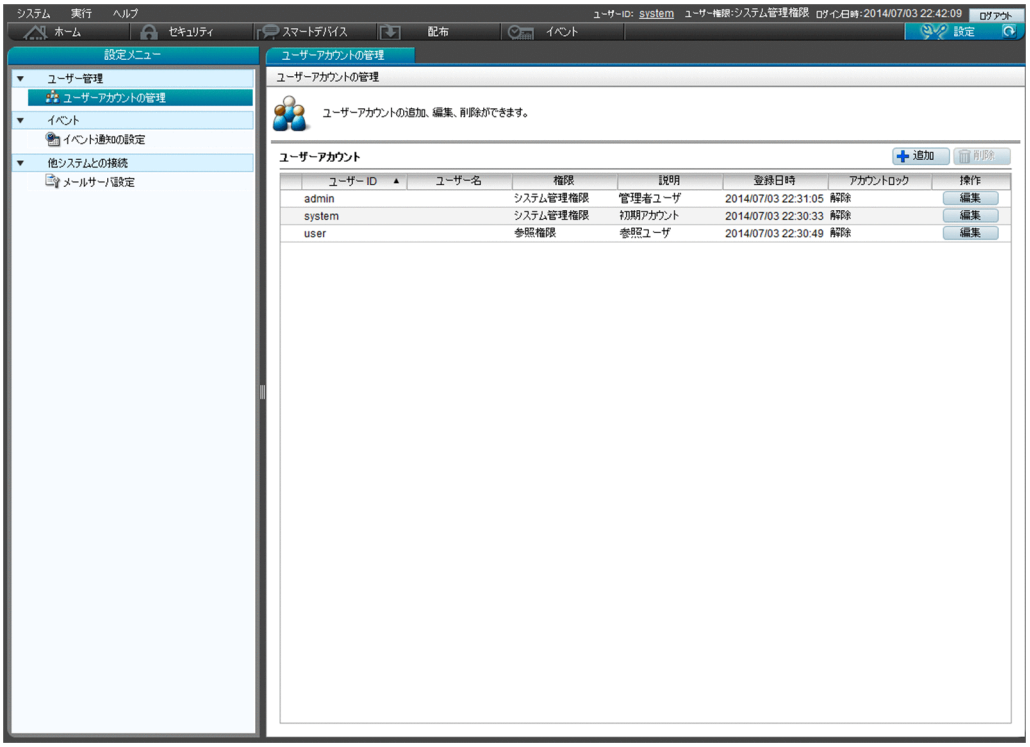

重大度の大きいイベントがあった場合は、このダイアログでイベントの詳細情報を確認し、適切な対策をしてください。

なお、 または をクリックすると、ダイアログを開いたまま前後のイベントの詳細を確認できます。

## 14.8　設定画面

設定画面では、ユーザーアカウントの管理やイベント通知の設定など、JP1/ITDM2 - SDM を運用するために必要な設定ができます。

### 画面



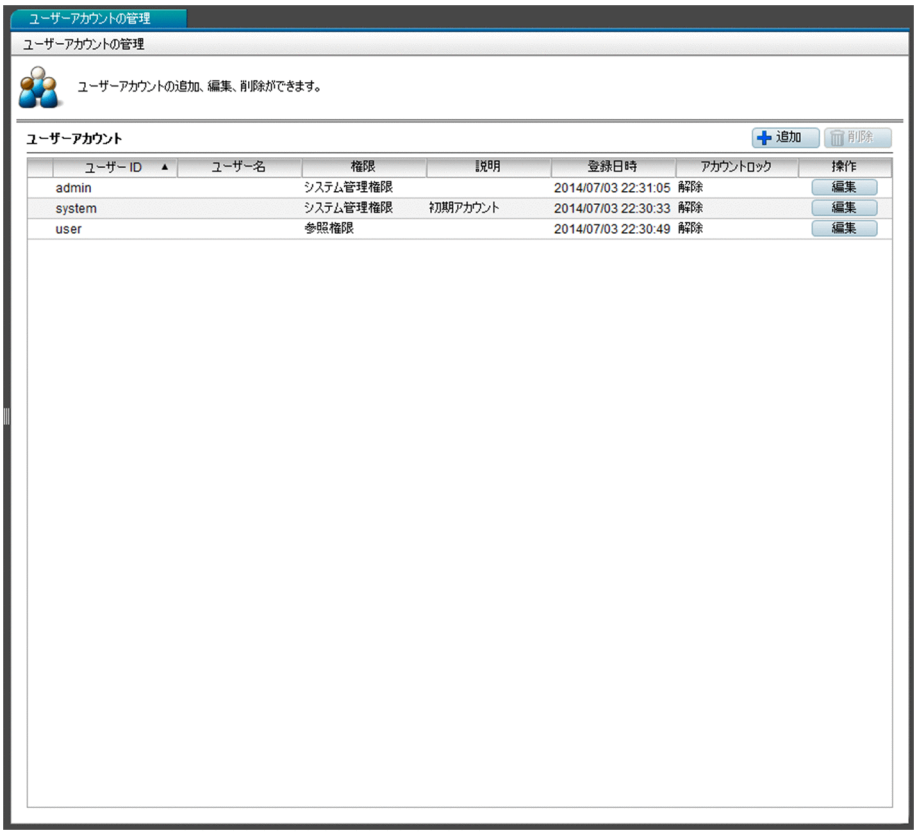

### 関連項目

- 14.8.1　［ユーザーアカウントの管理］画面
- 14.8.4　［イベント通知の設定］画面
- 14.8.5　［メールサーバ設定］画面

## 14.8.1　［ユーザーアカウントの管理］画面

［ユーザーアカウントの管理］画面では、登録されているユーザーアカウントの一覧が表示されます。また、ユーザーアカウントの追加、編集、および削除ができます。

### 画面




### 項目

表示されるボタンを次に示します。

［追加］ボタン

新規にユーザーアカウントを追加します。

［削除］ボタン

選択したユーザーアカウントを削除します。選択したユーザーアカウントがビルトインアカウントまたはログインユーザーの場合は削除できません。

［編集］ボタン

選択したユーザーアカウントを編集します。

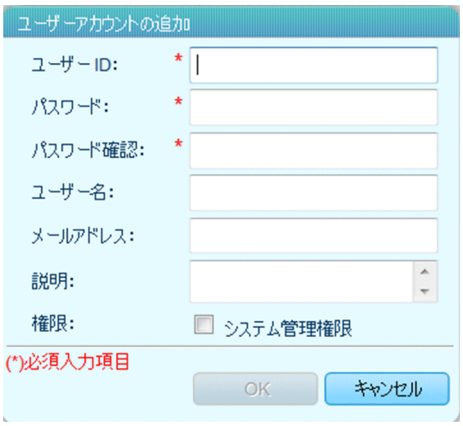
### 関連項目

- 14.8.2 ［ユーザーアカウントの追加］ダイアログ
- 14.8.3 ［ユーザーアカウントの編集］ダイアログ

## 14.8.2 ［ユーザーアカウントの追加］ダイアログ

［ユーザーアカウントの追加］ダイアログでは、ユーザーアカウントを JP1/ITDM2 - SDM に登録できます。

### 画面




### 項目

表示される入力項目を次に示します。

[ユーザー ID]

JP1/ITDM2 - SDM にログインするためのユーザー ID を入力します。

[パスワード]

追加するユーザー ID でログインするためのパスワードを入力します。

[パスワード確認]

確認のためにパスワードを再入力します。

[ユーザー名]

ユーザー名を入力します。

[メールアドレス]

追加するユーザーのメールアドレスを入力します。

イベントの通知は、ここで指定したメールアドレスに送信されます。

[説明]

追加するユーザーアカウントについての説明を入力します。ユーザーアカウントの利用目的などを入力するとアカウントの管理が容易になります。

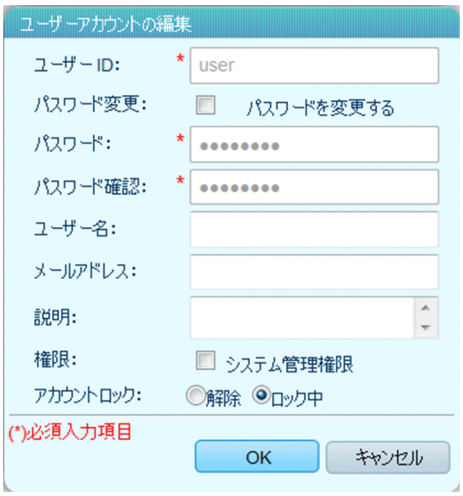
[権限]

ユーザーアカウントにシステム管理権限を付与する場合にチェックしてください。チェックしない場合は、参照権限が付与されます。

## 14.8.3 ［ユーザーアカウントの編集］ダイアログ

［ユーザーアカウントの編集］ダイアログでは、登録済みのユーザーアカウントの情報を編集できます。

## 画面




## 項目

表示される入力項目を次に示します。

[ユーザー ID]

JP1/ITDM2 - SDM にログインするためのユーザー ID が表示されます。この項目は編集できません。

[パスワード]

追加するユーザー ID でログインするためのパスワードを入力します。

[パスワード確認]

確認のためにパスワードを再入力します。

[ユーザー名]

ユーザー名を入力します。

[メールアドレス]

メールアドレスを入力します。

イベントの通知は、ここで指定したメールアドレスに送信されます。

[説明]

ユーザーアカウントについての説明を入力します。ユーザーアカウントの利用目的などを入力するとアカウントの管理が容易になります。

[権限]

ユーザーアカウントにシステム管理権限を付与する場合にチェックしてください。チェックしない場合は、参照権限が付与されます。

[アカウントロック]

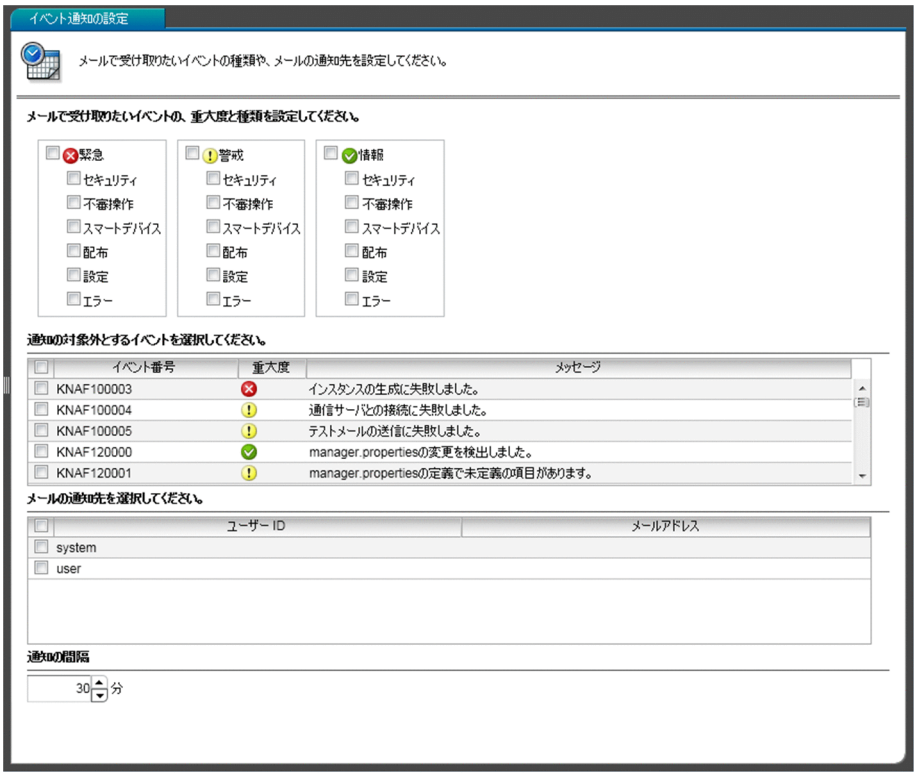
編集しているユーザーアカウントがロック状態の場合に表示されます。

システム管理権限のアカウントでログインしているときは、ユーザーアカウントのロックを解除できます。ロックを解除すると、そのユーザーアカウントでログインできるようになります。

## 14.8.4 ［イベント通知の設定］画面

［イベント通知の設定］画面では、イベントが発生したときに、自動的にメールで通知されるように設定できます。

### 画面




### 項目

表示される入力項目を次に示します。

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。

メールで受け取りたいイベントの重大度とイベントの種類をチェックします。

通知の対象外とするイベントを選択してください。

通知の対象外としたいイベントをチェックします。タイトル行の左端のチェックボックスをチェックすることで、すべてのイベントをチェックできます。

メールの通知先を選択してください。

イベントをメールで通知するユーザーアカウントをチェックします。タイトル行の左端のチェックボックスをチェックすることで、すべてのユーザーアカウントをチェックできます。

通知の間隔

イベントを通知する間隔を設定します。

### 関連項目

- 2.7.2 イベントの種類

## 14.8.5 ［メールサーバ設定］画面

［メールサーバ設定］画面では、イベントをメールで通知するときに利用するメールサーバ（SMTP サーバ）の設定ができます。また、テストメールの送信もできます。

### 画面

### 項目

表示される入力項目およびボタンを次に示します。

［ホスト名］

SMTP サーバのホスト名を入力します。

［セキュリティ保護の接続］

SMTP サーバと通信する際に使用するセキュリティ保護の方法を選択します。

> **重要**
>
> SSL/TLS を使用する場合、CA のルート証明書をスマートデバイスマネージャーが動作する環境にインポートする必要があります。

［ポート番号］

SMTP サーバのポート番号を入力します。

［送信元メールアドレス］

イベント通知をする送信元のメールアドレスを指定します。

[SMTP 認証を使用する]

SMTP 認証を使用する場合にチェックします。

[ユーザー ID]

SMTP 認証を使用する場合、ユーザー ID を入力します。

[パスワード]

SMTP 認証を使用する場合、ユーザー ID に対するパスワードを入力します。

[パスワード確認]

確認のためにパスワードを再入力します。

[テストメールを送信] ボタン

ログインユーザーのメールアドレスに対して、テストメールを送信します。

[適用] ボタン

指定した設定内容を適用します。

**関連項目**

- 3.12 スマートデバイスマネージャーでの SSL 通信用証明書の設定
- 14.8.4 [イベント通知の設定] 画面

# 15 コマンド

ここでは、JP1/ITDM2 - SDM のコマンドについて説明します。

# コマンドの説明形式

機能、形式、引数など、8 つの項目でコマンドを説明しています。コマンドの説明形式を表で示します。

## コマンドの説明形式

| 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 | 実行権限 | コマンドの実行に必要な権限について説明しています。 |
| 6 | 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。 |
| 7 | 戻り値 | コマンドの戻り値について説明しています。 |
| 8 | 使用例 | コマンドの使用例について説明しています。 |

# コマンドを実行する流れ

JP1/ITDM2 - SDM のコマンドは、Windows のコマンドプロンプトから実行できます。コマンドを実行する流れを次に示します。

## コマンドを実行する流れ

1. Windows のコマンドプロンプトを起動する
2. カレントディレクトリをコマンドの格納先に変更する
   コマンドの格納先を次の表に示します。

| サーバ種別 | 格納先 |
|---|---|
| スマートデバイスマネージャー | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin |
| 通信サーバ | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥bin |
| メッセージングサーバ | JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥bin |

3. 実行したいコマンドを入力する

# コマンド一覧

JP1/ITDM2 - SDM で使用できるコマンドを一覧で示します。

## コマンド一覧

| 項番 | コマンド名 | 機能 | 実行できるサーバ |
|---|---|---|---|
| 1 | sdmexportdb | スマートデバイスマネージャーが管理するデータのバックアップを取得します。 | スマートデバイスマネージャー |
| 2 | sdmimportdb | スマートデバイスマネージャー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。 | スマートデバイスマネージャー |
| 3 | sdmioutils exportdevice | スマートデバイスの情報をエクスポートします。 | スマートデバイスマネージャー |
| 4 | sdmioutils importdevice | スマートデバイスの情報をインポートします。 | スマートデバイスマネージャー |
| 5 | sdmioutils exportpolicy | セキュリティポリシーの設定情報をエクスポートします。 | スマートデバイスマネージャー |
| 6 | sdmioutils importpolicy | セキュリティポリシーの設定情報をインポートします。 | スマートデバイスマネージャー |
| 7 | sdmioutils exportsdpolicy | Android ポリシーまたは iOS プロファイルの情報をエクスポートします。 | スマートデバイスマネージャー |
| 8 | sdmioutils importsdpolicy | Android ポリシーまたは iOS プロファイルの情報をインポートします。 | スマートデバイスマネージャー |
| 9 | sdmioutils exportdeliveryapp | アプリケーション配布情報をエクスポートします。 | スマートデバイスマネージャー |
| 10 | sdmioutils importdeliveryapp | アプリケーション配布情報をインポートします。 | スマートデバイスマネージャー |
| 11 | sdmioutils exportdeliverypermit | 利用者の操作でインストールできるアプリケーションの設定情報をエクスポートします。 | スマートデバイスマネージャー |
| 12 | sdmioutils importdeliverypermit | 利用者の操作でインストールできるアプリケーションを設定します。 | スマートデバイスマネージャー |
| 13 | sdmioutils deletedeliverypermit | 利用者の操作でインストールできるアプリケーションの設定情報を削除します。 | スマートデバイスマネージャー |
| 14 | sdmdistributeapp | スマートデバイスにアプリケーションを配布し、インストールを指示します。 | スマートデバイスマネージャー |
| 15 | sdmapplyprofile | iOS 端末に対して、iOS プロファイルを適用または iOS プロファイルの適用を解除します。 | スマートデバイスマネージャー |
| 16 | sdmgetinventory | スマートデバイスから最新のインベントリ情報を取得します。 | スマートデバイスマネージャー |

| 項番 | コマンド名 | 機能 | 実行できるサーバ |
|---|---|---|---|
| 17 | sdmexportdistributestatus | アプリケーションの配布状況を出力します。 | スマートデバイスマネージャー |
| 18 | sdmexportinstallapp | 全スマートデバイスのインストールソフトウェア情報を出力します。 | スマートデバイスマネージャー |
| 19 | sdmnetchange | スマートデバイスマネージャーまたは通信サーバのネットワーク構成を変更します。 | • スマートデバイスマネージャー<br>• 通信サーバ |
| 20 | sdmcreatemdmcertreq | iOS 端末を管理する場合、MDM 用署名済み証明書要求ファイルを作成します。 | • スマートデバイスマネージャー<br>• 通信サーバ |
| 21 | sdmgetlogs | スマートデバイスマネージャー、通信サーバ、JP1/ITDM2 - SDM（スマートデバイスエージェント）、またはメッセージングサーバのログ情報を取得します。 | • スマートデバイスマネージャー<br>• 通信サーバ<br>• メッセージングサーバ |

**関連項目**

- 15. sdmexportdb（バックアップの取得）
- 15. sdmimportdb（バックアップデータのリストア）
- 15. sdmioutils exportdevice（スマートデバイス情報のエクスポート）
- 15. sdmioutils importdevice（スマートデバイス情報のインポート）
- 15. sdmioutils exportpolicy（セキュリティポリシー設定情報のエクスポート）
- 15. sdmioutils importpolicy（セキュリティポリシー設定情報のインポート）
- 15. sdmioutils exportsdpolicy（Android ポリシーまたは iOS プロファイルの情報のエクスポート）
- 15. sdmioutils importsdpolicy（Android ポリシーまたは iOS プロファイルの情報のインポート）
- 15. sdmioutils exportdeliveryapp（アプリケーション配布情報のエクスポート）
- 15. sdmioutils importdeliveryapp（アプリケーション配布情報のインポート）
- 15. sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
- 15. sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）
- 15. sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）
- 15. sdmdistributeapp（アプリケーションのインストール指示）
- 15. sdmapplyprofile（iOS プロファイルの適用または適用解除）
- 15. sdmgetinventory（インベントリ情報の取得）

- 15. sdmexportdistributestatus（アプリケーション配布状況の出力）
- 15. sdmexportinstallapp（インストールソフトウェア情報の出力）
- 15. sdmnetchange（スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更）
- 15. sdmcreatemdmcertreq（MDM 用署名済み証明書要求ファイルの作成）
- 15. sdmgetlogs（ログ情報の取得）

# sdmexportdb（バックアップの取得）

スマートデバイスマネージャーが管理するデータのバックアップを取得するコマンドです。

## 機能

スマートデバイスマネージャー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、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

## 形式

```
sdmexportdb[ -f バックアップ先フォルダ名]
```

## 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/ITDM2 - SDM 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には、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（"）で囲んでください。

バックアップ先フォルダパス長は、バックアップファイル名を含めて 165 文字（バイト）以内で指定してください。

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。

「#」、「(」、「)」、「-」（ハイフン）、「.」（ピリオド）、「@」、「_」（アンダーバー）、パス区切りの「¥」

この引数を指定した場合、バックアップ格納先フォルダは次のとおりです。

引数に指定したフォルダ¥yyyyMMddhhmmss

この引数を省略した場合は、次に示すデフォルトのバックアップ先フォルダに、バックアップファイルを格納します。

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥backup¥yyyyMMddhhmmss

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

### 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーおよび通信サーバが停止している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースのサービスが開始している必要があります。
- 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。
  - sdmimportdb
  - sdmioutils で始まるコマンド

## 戻り値

| 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。または、コマンドの引数に指定したフォルダ名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 16 | 指定されたフォルダが存在しません。 |
| 17 | 指定されたフォルダへのアクセスエラーが発生しました。 |
| 18 | ほかのコマンドを実行中です。 |
| 24 | バックアップファイルの作成に失敗しました。 |
| 30 | データベースにアクセスできません。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

バックアップを`C:¥tmp¥backup` に取得する場合の使用例を次に示します。

```
sdmexportdb -f C:¥tmp¥backup
```

### 関連項目

- 15. コマンドを実行する流れ

- 15. sdmimportdb（バックアップデータのリストア）

# sdmimportdb（バックアップデータのリストア）

スマートデバイスマネージャー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）するコマンドです。

## 機能

ディスク障害などが発生した場合に、スマートデバイスマネージャー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）します。データの復元にはsdmexportdb 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、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmimportdb[ -f バックアップ格納フォルダ名]
```

## 引数

-f バックアップ格納フォルダ名

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。フォルダにはsdmexportdb コマンドでバックアップ先フォルダに作成された yyyyMMddhhmmss のフォルダ名も指定してください。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。

バックアップ格納フォルダパス長は、バックアップファイル名を含めて 165 文字（バイト）以内で指定してください。

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。

「#」、「(」、「)」、「-」（ハイフン）、「.」（ピリオド）、「@」、「_」（アンダーバー）、パス区切りの「¥」

この引数を指定した場合、指定したフォルダをバックアップ格納フォルダとして使用します。

この引数を省略した場合は、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バックアップ格納フォルダを判断して使用します。

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥backup

（例）

フォルダ下に次のバックアップ格納フォルダが存在する場合、「¥20140101060000」フォルダを復元データに使用します。

¥20140101000000

¥20140101060000

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーおよび通信サーバが停止している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースのサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmioutils で始まるコマンド

## 戻り値

| 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。または、コマンドの引数に指定したフォルダ名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 16 | 指定されたフォルダが存在しません。 |
| 17 | 指定されたフォルダへのアクセスエラーが発生しました。 |
| 18 | ほかのコマンドを実行中です。 |
| 25 | データベースのリストアに失敗しました。 |
| 30 | データベースにアクセスできません。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

2014 年 1 月 1 日 2 時 30 分 00 秒にバックアップを取得したデータ（バックアップ格納先フォルダ：C:¥tmp¥backup¥20140101023000）を使用し、バックアップからのリストアを実行する場合の使用例を次に示します。

```
sdmimportdb -f C:¥tmp¥backup¥20140101023000
```

**関連項目**

- 15. コマンドを実行する流れ
- 15. sdmexportdb（バックアップの取得）

# sdmioutils exportdevice（スマートデバイス情報のエクスポート）

スマートデバイスの情報を CSV 形式でエクスポートするコマンドです。

## 機能

スマートデバイス情報を、指定したファイルに CSV 形式でエクスポートします。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils exportdevice -export エクスポートするファイル名[ -encoding 文字コード種別][ -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。

-encoding **文字コード種別**

エクスポートするファイルの文字コード種別を指定します。この引数を省略した場合、UTF-8 が指定されます。

指定できる文字コード種別は次のとおりです。

- ISO-8859-1
- UTF-8
- UTF-16

-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。この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/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。

- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

スマートデバイスの情報をC:¥temp¥smartdevice.csv にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportdevice -export C:¥temp¥smartdevice.csv -encoding UTF-8 -s
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils importdevice（スマートデバイス情報のインポート）
- 付録 E.1 スマートデバイス一覧エクスポート・インポート CSV ファイルの形式

# sdmioutils importdevice（スマートデバイス情報のインポート）

CSV ファイルを利用して、スマートデバイスの情報をインポートするコマンドです。

## 機能

CSV ファイルを利用してスマートデバイスの情報をインポートします。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils importdevice -import インポートするファイル名[ -encoding 文字コード種別]
```

## 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。

-encoding **文字コード種別**

インポートするファイルの文字コード種別を指定します。この引数を省略した場合、UTF-8 が指定されます。

指定できる文字コード種別は次のとおりです。

- ISO-8859-1
- UTF-8
- UTF-16

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb

- sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

CSV ファイル`C:¥temp¥smartdevice.csv` に定義したスマートデバイスの情報をインポートする場合の使用例を次に示します。

```
sdmioutils importdevice -import C:¥temp¥smartdevice.csv -encoding UTF-8
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportdevice（スマートデバイス情報のエクスポート）
- 付録 E.1 スマートデバイス一覧エクスポート・インポート CSV ファイルの形式

# sdmioutils exportpolicy（セキュリティポリシー設定情報のエクスポート）

セキュリティポリシーの設定情報を XML 形式でエクスポートするコマンドです。

## 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 XML 形式でエクスポートします。

複数の JP1/ITDM2 - SDM 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、あるスマートデバイスマネージャーで作成したセキュリティポリシーをほかのスマートデバイスマネージャーに流用できます。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils 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。この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/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。

- sdmexportdb
- sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 20 | 指定されたセキュリティポリシーが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 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使用例を次に示します。

```
sdmioutils exportpolicy -export C:¥temp¥exportpolicy.xml -name 開発部用ポリシー -s
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils importpolicy（セキュリティポリシー設定情報のインポート）
- 付録 E.3 セキュリティポリシー一覧エクスポート XML ファイルの形式

# sdmioutils importpolicy（セキュリティポリシー設定情報のインポート）

エクスポートしたセキュリティポリシーをインポートするコマンドです。

## 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。

複数の JP1/ITDM2 - SDM 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、ほかのスマートデバイスマネージャーで作成したセキュリティポリシー設定情報を流用できます。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils 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]
```

## 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名を指定します。この引数を省略した場合、XML 内に定義されているセキュリティポリシー名で登録します。すでに同じセキュリティポリシー名がある場合は登録に失敗します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 22 | 指定されたセキュリティポリシーがすでに存在します。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

C:¥temp¥にエクスポートしたセキュリティポリシーの設定情報exportpolicy.xml（セキュリティポリシー名：開発部用ポリシー）をインポートする場合の使用例を次に示します。

```
sdmioutils importpolicy -import C:¥temp¥exportpolicy.xml -name 開発部用ポリシー
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportpolicy（セキュリティポリシー設定情報のエクスポート）
- 付録 E.3 セキュリティポリシー一覧エクスポート XML ファイルの形式

# sdmioutils exportsdpolicy（Android ポリシーまたは iOS プロファイルの情報のエクスポート）

Android ポリシーまたは iOS プロファイルの情報を XML 形式でエクスポートするコマンドです。

## 機能

Android ポリシーまたは iOS プロファイルの情報を、指定したファイルに XML 形式でエクスポートします。

複数の JP1/ITDM2 - SDM 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、あるスマートデバイスマネージャーで作成した Android ポリシーまたは iOS プロファイルをほかのスマートデバイスマネージャーに流用できます。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils exportsdpolicy -export エクスポートするファイル名 -name Androidポリシー名または
iOSプロファイル名 -policytype ポリシー種別[ -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。

-name Android ポリシー名または iOS プロファイル名

エクスポートする Android ポリシーまたは iOS プロファイルの名称を指定します。

-policytype ポリシー種別

エクスポート対象のポリシー種別を指定します。

指定できるポリシー種別は次のとおりです。

0：iOS プロファイル

1：Android ポリシー

-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。この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/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 20 | 指定された Android ポリシー、または iOS プロファイルが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

「開発部用ポリシー」をC:¥temp¥exportsdpolicy.xml にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportsdpolicy -export C:¥temp¥exportsdpolicy.xml -name 開発部用ポリシー -
policytype 0 -s
```

**関連項目**

- 15. コマンドを実行する流れ
- 15. sdmioutils importsdpolicy（Android ポリシーまたは iOS プロファイルの情報のインポート）
- 付録 E.4 スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式

# sdmioutils importsdpolicy（Android ポリシーまたは iOS プロファイルの情報のインポート）

エクスポートした Android ポリシーまたは iOS プロファイルの情報をインポートするコマンドです。

## 機能

エクスポートした Android ポリシーまたは iOS プロファイルの情報をインポートします。

複数の JP1/ITDM2 - SDM 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、ほかのスマートデバイスマネージャーで作成した Android ポリシーまたは iOS プロファイルの情報を流用できます。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils importsdpolicy -import インポートするファイル名[ -name Androidポリシー名またはiOSプロファイル名]
```

## 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。

-name Android ポリシー名または iOS プロファイル名

インポートする Android ポリシーまたは iOS プロファイルの名称を指定します。この引数を省略した場合、XML 内に定義されている Android ポリシーまたは iOS プロファイルの名称で登録します。すでに同じ名称がある場合は登録に失敗します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb

- sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 22 | 指定された Android ポリシーまたは iOS プロファイルがすでに存在します。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

C:¥temp¥exportsdpolicy.xml にエクスポートした「開発部用ポリシー」をインポートする場合の使用例を次に示します。

```
sdmioutils importsdpolicy -import C:¥temp¥exportsdpolicy.xml -name 開発部用ポリシー
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportsdpolicy（Android ポリシーまたは iOS プロファイルの情報のエクスポート）
- 付録 E.4 スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式

# sdmioutils exportdeliveryapp（アプリケーション配布情報のエクスポート）

アプリケーション配布情報を XML 形式でエクスポートするコマンドです。

## 機能

アプリケーション配布情報を、指定したファイルに XML 形式でエクスポートします。

複数の JP1/ITDM2 - SDM 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、あるスマートデバイスマネージャーで作成したアプリケーション配布情報をほかのスマートデバイスマネージャーに流用できます。

> **重要**
>
> ほかのスマートデバイスマネージャーに流用する場合、通信サーバに配置してあるアプリケーションを手動でコピーする必要があります。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils exportdeliveryapp -export エクスポートするファイル名 -name アプリケーション名[ -version バージョン] -ostype OS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。

-name アプリケーション名

エクスポートするアプリケーション名を指定します。

-version バージョン

エクスポートするアプリケーションのバージョンを指定します。

iOS アプリケーションの場合は必ず指定してください。

-ostype OS 種別

エクスポートするアプリケーションの OS 種別を指定します。

指定できる OS 種別は次のとおりです。

0：iOS

1：Android

-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。この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/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 21 | 指定されたアプリケーションが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |

| 戻り値 | 説明 |
| --- | --- |
| 253 | サービスが起動されていません。 |

## 使用例

アプリケーション配布情報「セキュリティアプリ」をC:¥temp¥exportdeliveryapp.xml にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportdeliveryapp -export C:¥temp¥exportdeliveryapp.xml -name セキュリティアプリ
-ostype 0 -s
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils importdeliveryapp（アプリケーション配布情報のインポート）
- 付録 E.5 配布アプリケーションエクスポート XML ファイルの形式

# sdmioutils importdeliveryapp（アプリケーション配布情報のインポート）

エクスポートしたアプリケーション配布情報をインポートするコマンドです。

## 機能

エクスポートしたアプリケーション配布情報をインポートします。

複数の JP1/ITDM2 - SDM 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、ほかのスマートデバイスマネージャーで作成したアプリケーション配布情報を流用できます。

> **重要**
>
> ほかのスマートデバイスマネージャーに流用する場合、通信サーバに配置してあるアプリケーションを手動でコピーする必要があります。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式

```
sdmioutils importdeliveryapp -import インポートするファイル名[ -name アプリケーション名]
```

## 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。

-name **アプリケーション名**

インポートするアプリケーション名を指定します。この引数を省略した場合、XML 内に定義されているアプリケーション名で登録します。すでに同じアプリケーション名がある場合は登録に失敗します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 23 | 指定されたアプリケーションがすでに存在します。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

C:¥temp¥exportdeliveryapp.xml にエクスポートしたアプリケーション配布情報（アプリケーション名：セキュリティアプリ）をインポートする場合の使用例を次に示します。

```
sdmioutils importdeliveryapp -import C:¥temp¥exportdeliveryapp.xml -name セキュリティアプリ
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportdeliveryapp（アプリケーション配布情報のエクスポート）
- 付録 E.5 配布アプリケーションエクスポート XML ファイルの形式

# sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）

利用者の操作でインストールできるアプリケーションの設定情報を CSV 形式でエクスポートするコマンドです。

## 機能

利用者の操作でインストールできるアプリケーションの設定情報を、配布許可定義ファイルにエクスポートします。

このコマンドは、-mode の指定値によってエクスポートされる情報が異なります。-mode の指定値とエクスポートされる情報を次に示します。

| -mode の指定値 | エクスポートされる情報 |
|---|---|
| all | 利用者の操作でインストールできるアプリケーションの全情報をエクスポートします。 |
| app | 指定したアプリケーションの配布が許可されているスマートデバイスの情報をエクスポートします。 |
| device | 指定したスマートデバイスに配布が許可されているアプリケーションの情報をエクスポートします。 |

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式 1

```
sdmioutils exportdeliverypermit -export 配布許可定義ファイル名 -mode all[ -encoding 文字コード種別][ -s]
```

## 形式 2

```
sdmioutils exportdeliverypermit -export 配布許可定義ファイル名 -mode {app | device} -name 名称 -ostype OS種別[ -encoding 文字コード種別][ -s]
```

## 引数

-export 配布許可定義ファイル名

利用者の操作でインストールできるアプリケーションの設定情報をエクスポートする配布許可定義ファイル名を 259 バイト以内の絶対パスで指定します。

-mode {all | app | device}

エクスポートのモードを指定します。

all

利用者の操作でインストールできるアプリケーションの全情報をエクスポートします。

app

指定したアプリケーションの配布が許可されているスマートデバイスの情報をエクスポートします。

device

指定したスマートデバイスに配布が許可されているアプリケーションの情報をエクスポートします。

-name 名称

エクスポートするアプリケーションまたはスマートデバイスの名称を指定します。

-ostype OS 種別

OS 種別を指定します。

指定できる OS 種別は次のとおりです。

0：Android

1：iOS

-encoding 文字コード種別

エクスポートするファイルの文字コード種別を指定します。この引数を省略した場合、UTF-8 が指定されます。

指定できる文字コード種別は次のとおりです。

- ISO-8859-1
- UTF-8
- UTF-16

-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。この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/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb

- sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 21 | 指定されたアプリケーションが存在しません。 |
| 29 | 指定されたスマートデバイスが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例 1

利用者の操作でインストールできるアプリケーションの全情報をC:¥temp¥exportdeliverypermit.csv にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportdeliverypermit -export C:¥temp¥exportdeliverypermit.csv -mode all -s
```

## 使用例 2

iOS アプリケーション（名称：application01）の配布が許可されているスマートデバイスの情報をC:¥temp¥exportdeliverypermit.csv にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportdeliverypermit -export C:¥temp¥exportdeliverypermit.csv -mode app -name
application01 -ostype 1 -s
```

## 使用例 3

iOS 端末（名称：smartdevice01）に配布が許可されているアプリケーションの情報をC:¥temp¥exportdeliverypermit.csv にエクスポートする場合の使用例を次に示します。

```
sdmioutils exportdeliverypermit -export C:¥temp¥exportdeliverypermit.csv -mode device -name
smartdevice01 -ostype 1 -s
```

**関連項目**

- 15. コマンドを実行する流れ
- 15. sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）
- 15. sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）
- 付録 E.6 配布許可定義ファイルの形式

# sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）

利用者の操作でインストールできるアプリケーションを設定するコマンドです。

## 機能

利用者の操作でインストールできるアプリケーションの情報を記述した配布許可定義ファイルをインポートして、利用者の操作でインストールできるアプリケーションを設定します。

このコマンドは、-mode の指定値によって設定する内容が異なります。-mode の指定値と設定する内容を次に示します。

| -mode の指定値 | 設定内容 |
|---|---|
| all | 配布許可定義ファイルに記述した利用者の操作でインストールできるアプリケーションの全情報を設定します。 |
| app | 指定したアプリケーションの配布許可を、配布許可定義ファイルに記述したスマートデバイスに対して設定します。 |
| device | 指定したスマートデバイスに対して、配布許可定義ファイルに記述したアプリケーションの配布許可を設定します。 |

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式 1

```
sdmioutils importdeliverypermit -import 配布許可定義ファイル名 -mode all [ -encoding 文字コード種別]
```

## 形式 2

```
sdmioutils importdeliverypermit -import 配布許可定義ファイル名 -mode app -name 名称 -version バージョン -ostype OS種別[ -encoding 文字コード種別]
```

## 形式 3

```
sdmioutils importdeliverypermit -import 配布許可定義ファイル名 -mode device -name 名称 -ostype OS種別[ -encoding 文字コード種別]
```

## 引数

-inport 配布許可定義ファイル名

利用者の操作でインストールできるアプリケーションの情報を記述した配布許可定義ファイル名を 259 バイト以内の絶対パスで指定します。

-mode {all | app | device}

インポートのモードを指定します。

all

利用者の操作でインストールできるアプリケーションの全情報を設定します。

app

指定したアプリケーションの配布許可をスマートデバイスに設定します。

device

指定したスマートデバイスに対して、アプリケーションの配布許可を設定します。

-name 名称

アプリケーションまたはスマートデバイスの名称を指定します。

-version バージョン

アプリケーションのバージョンを指定します。この引数は、-mode にapp を指定した場合だけ指定できます。

-ostype OS 種別

OS 種別を指定します。

指定できる OS 種別は次のとおりです。

0：Android

1：iOS

-encoding 文字コード種別

インポートするファイルの文字コード種別を指定します。この引数を省略した場合、UTF-8 が指定されます。

指定できる文字コード種別は次のとおりです。

- ISO-8859-1
- UTF-8
- UTF-16

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。

- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 21 | 指定されたアプリケーションが存在しません。 |
| 27 | ファイルの書式が不正です。 |
| 28 | 指定したデータが見つかりません。 |
| 29 | 指定されたスマートデバイスが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例 1

利用者の操作でインストールできるアプリケーションの全情報を設定する場合の使用例を次に示します（配布許可定義ファイル：C:¥temp¥exportdeliverypermit.csv※）。

```
sdmioutils importdeliverypermit -import C:¥temp¥exportdeliverypermit.csv -mode all
```

注※　C:¥temp¥exportdeliverypermit.csv の記述内容を次に示します。

```
OS種別,アプリケーション名,バージョン,配布許可対象種別,配布許可対象名
Android,app2,v1,0,device4
Android,app2,v1,0,device5
Android,app3,v1,0,device5
iOS,app1,v1,0,device1
```

```
iOS,app1,v1,0,device2
iOS,app1,v1,0,device3
```

## 使用例 2

iOS アプリケーション（名称：application01、バージョン：1.00）の配布を許可する場合の使用例を次に示します（配布許可定義ファイル：C:¥temp¥exportdeliverypermit.csv※）。

```
sdmioutils importdeliverypermit -import C:¥temp¥exportdeliverypermit.csv -mode app -name
application01 -version 1.00 -ostype 1
```

注※　C:¥temp¥exportdeliverypermit.csv の記述内容を次に示します。

```
配布許可対象種別,配布許可対象名
0,device1
0,device2
0,device3
```

## 使用例 3

iOS 端末（名称：smartdevice01）に対してアプリケーションの配布を許可する場合の使用例を次に示します（配布許可定義ファイル：C:¥temp¥exportdeliverypermit.csv※）。

```
sdmioutils importdeliverypermit -import C:¥temp¥exportdeliverypermit.csv -mode device -name
smartdevice01 -ostype 1
```

注※　C:¥temp¥exportdeliverypermit.csv の記述内容を次に示します。

```
アプリケーション名,バージョン
app1,v1
app2,v1
app3,v1
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
- 15. sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）
- 付録 E.6 配布許可定義ファイルの形式

# sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）

利用者の操作でインストールできるアプリケーションの設定情報を削除するコマンドです。

## 機能

利用者の操作でインストールできるアプリケーションの設定情報を削除します。

なお、このコマンドはスマートデバイスマネージャー上で実行してください。

## 形式 1

```
sdmioutils deletedeliverypermit -mode all
```

## 形式 2

```
sdmioutils deletedeliverypermit -mode app -name 名称 -version バージョン -ostype OS種別
```

## 形式 3

```
sdmioutils deletedeliverypermit -mode device -name 名称 -ostype OS種別
```

## 引数

-mode {all | app | device}

削除のモードを指定します。

`all`

利用者の操作でインストールできるアプリケーションの設定情報をすべて削除します。

`app`

指定したアプリケーションの配布許可を削除します。

`device`

指定したスマートデバイスの配布許可を削除します。

-name 名称

削除するアプリケーションまたはスマートデバイスの名称を指定します。

-version バージョン

削除するアプリケーションのバージョンを指定します。この引数は、-mode にapp を指定した場合だけ指定できます。

-ostype OS 種別

OS 種別を指定します。

指定できる OS 種別は次のとおりです。

0：Android

1：iOS

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。
- 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。
  - sdmexportdb
  - sdmimportdb

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 21 | 指定されたアプリケーションが存在しません。 |
| 29 | 指定されたスマートデバイスが存在しません。 |
| 30 | データベースにアクセスできません。 |
| 40 | コマンドの実行を中断しました。 |
| 150 | そのほかのエラーが発生しました。 |

| 戻り値 | 説明 |
|---|---|
| 253 | サービスが起動されていません。 |

## 使用例 1

利用者の操作でインストールできるアプリケーションの全情報を削除する場合の使用例を次に示します。

```
sdmioutils deletedeliverypermit -mode all
```

## 使用例 2

iOS アプリケーション（名称：application01、バージョン：1.00）の配布許可を削除する場合の使用例を次に示します。

```
sdmioutils deletedeliverypermit -mode app -name application01 -version 1.00 -ostype 1
```

## 使用例 3

iOS 端末（名称：smartdevice01）の配布許可を削除する場合の使用例を次に示します。

```
sdmioutils deletedeliverypermit -mode device -name smartdevice01 -ostype 1
```

### 関連項目

- 15. コマンドを実行する流れ
- 15. sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
- 15. sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）

# sdmdistributeapp（アプリケーションのインストール指示）

スマートデバイスにアプリケーションを配布し、利用者にインストールを指示するコマンドです。

## 機能

アプリケーション配布情報ファイルに記述したスマートデバイスに対して、アプリケーションを配布し、インストールを指示します。

## 形式

```
sdmdistributeapp -file アプリケーション配布情報ファイル
```

## 引数

-file アプリケーション配布情報ファイル

配布するアプリケーションおよび配布対象のスマートデバイスを記述したアプリケーション配布情報ファイル名を 259 バイト以内の絶対パスで指定します。

アプリケーション配布情報ファイルの文字コードは、UTF-8 固定です。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーおよび通信サーバのサービスがすべて開始している必要があります。
- Android アプリケーションのとき、アプリケーション配布情報ファイルに、アプリケーションの配布とインストールの指示が定義されている場合、アプリケーションの配布が先に実施されます。また、同一アプリケーションの配布とインストールが定義されている場合、アプリケーションの配布は実施しないで、アプリケーションのインストールだけが実施されます。

  アプリケーションのインストールは、アプリケーションの配布状態が配布済みの場合、アプリケーションの配布は実施しないで、アプリケーションのインストールだけが実施されます。
- アプリケーション配布情報ファイルに、存在しないアプリケーションおよびスマートデバイスが記述されている場合、コマンドは異常終了します。
- アプリケーション配布情報ファイルに、同じ内容の行が複数行記述されても、アプリケーションの配布およびインストール指示は 1 度しか実行されません。

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 27 | ファイルの書式が不正です。 |
| 28 | 指定したアプリケーションまたはスマートデバイスが見つかりません。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

アプリケーション配布情報ファイルC:¥temp¥distributeapp.csv※に記述したアプリケーションおよびスマートデバイスに対して、アプリケーションを配布し、インストールを指示する場合の使用例を次に示します。

```
sdmdistributeapp -file C:¥temp¥distributeapp.csv
```

注※　C:¥temp¥distributeapp.csv の記述内容を次に示します。

```
操作,OS種別,配布アプリケーション,バージョン,スマートデバイス名
install,iOS,ApplicationA,1.0,Device1
install,iOS,ApplicationA,1.0,Device2
install,iOS,ApplicationA,1.0,Device3
install,iOS,ApplicationB,1.0,Device1
install,iOS,ApplicationB,1.0,Device2
```

### 関連項目

- 15. コマンドを実行する流れ
- 付録 E.7 アプリケーション配布情報ファイルの形式

# sdmapplyprofile（iOS プロファイルの適用または適用解除）

iOS 端末に対して、iOS プロファイルを適用または iOS プロファイルの適用を解除するコマンドです。

## 機能

iOS プロファイル情報ファイルに記述した iOS 端末に対して、iOS プロファイル適用要求または適用解除要求を発行します。

## 形式

```
sdmapplyprofile -file iOSプロファイル情報ファイル
```

## 引数

-file iOS プロファイル情報ファイル

iOS プロファイルの適用または適用解除対象の iOS 端末を記述した iOS プロファイル情報ファイル名を 259 バイト以内の絶対パスで指定します。

iOS プロファイル情報ファイルの文字コードは、UTF-8 固定です。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーおよび通信サーバのサービスがすべて開始している必要があります。
- iOS プロファイル情報ファイルに記述されている順に iOS プロファイルの適用または適用解除が実施されます。iOS プロファイルの適用または適用解除に失敗した場合でも、次の行の処理を実行しコマンドは正常終了します。
- iOS プロファイルの適用解除を実施したとき、iOS 端末に該当の iOS プロファイルしか適用されていない場合は、適用解除に失敗します。この場合でも、コマンドは正常終了します。

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |

| 戻り値 | 説明 |
|---|---|
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 27 | ファイルの書式が不正です。 |
| 28 | 指定したスマートデバイスが見つかりません。 |
| 30 | データベースにアクセスできません。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

iOS プロファイル情報ファイル`C:¥temp¥profile.csv`※に記述した iOS 端末に対して、iOS プロファイルを適用する場合の使用例を次に示します。

```
sdmapplyprofile -file C:¥temp¥profile.csv
```

注※　`C:¥temp¥profile.csv` の記述内容を次に示します。

```
操作,プロファイル名,名称,コメント
apply,profile_A,Device1,
apply,profile_A,Device2,
```

### 関連項目

- 15. コマンドを実行する流れ
- 付録 E.8 iOS プロファイル情報ファイルの形式

# sdmgetinventory（インベントリ情報の取得）

スマートデバイスから、最新のインベントリ情報を取得するコマンドです。

## 機能

デバイス情報ファイルに記述したインベントリ取得対象のスマートデバイスに対して、インベントリ取得要求を発行します。

## 形式

```
sdmgetinventory -file デバイス情報ファイル
```

## 引数

-file デバイス情報ファイル

インベントリ取得対象のデバイス情報を記述したデバイス情報ファイル名を 259 バイト以内の絶対パスで指定します。

デバイス情報ファイルの文字コードは、UTF-8 固定です。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーおよび通信サーバのサービスがすべて開始している必要があります。
- デバイス情報ファイルに記述されている順にインベントリ情報が取得されます。インベントリ情報の取得に失敗した場合でも、次の行の処理を実行しコマンドは正常終了します。

## 戻り値

| 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。または、コマンドの引数に指定したファイル名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |

| 戻り値 | 説明 |
|---|---|
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 27 | ファイルの書式が不正です。 |
| 28 | 指定したスマートデバイスが見つかりません。 |
| 30 | データベースにアクセスできません。 |
| 150 | そのほかのエラーが発生しました。 |
| 253 | サービスが起動されていません。 |

## 使用例

デバイス情報ファイルC:¥temp¥dev_info.csv※に記述したスマートデバイスに対して、インベントリ情報を取得する場合の使用例を次に示します。

```
sdmgetinventory -file C:¥temp¥dev_info.csv
```

注※　デバイス情報ファイルC:¥temp¥dev_info.csv の記述内容を次に示します。

```
インベントリ種別,名称,コメント
All,Device1,
All,Device2,
All,Device3,
```

### 関連項目

- 15. コマンドを実行する流れ
- 付録 E.9 デバイス情報ファイルの形式

# sdmexportdistributestatus（アプリケーション配布状況の出力）

アプリケーションの配布状況をファイル出力するコマンドです。

## 機能

アプリケーションの配布状況を配布状況出力ファイルに出力します。

出力される配布状況を次に示します。

### iOS の場合

| 配布状況 | 説明 | 備考 |
|---|---|---|
| 未インストール | アプリケーションのインストールを指示していない状態。または、アンインストールが完了した状態。 | － |
| インストール済み | インストール完了のインベントリ情報をスマートデバイスから取得した状態。 | － |
| インストール要求済み | インストール指示が成功し、配布待ちの状態。 | スマートデバイス側でエラーが発生した場合などはエラーを検知できないため、インストールが失敗しているおそれがあります。一定時間（24 時間）経ってもインストール済みの状態にならない場合は、再度インストール指示を実施してください。 |
| インストール中 | アプリケーション配布中の状態。 | |
| インストール要求失敗 | インストール指示が失敗した状態。 | インストールが失敗しています。再度インストール指示を実施してください。 |
| インストール失敗 | スマートデバイスでインストールが失敗した状態。 | |
| アンインストール要求済み | アンインストール指示が成功し、アンインストール待ちの状態。 | スマートデバイス側でエラーが発生した場合などはエラーを検知できないため、アンインストールが失敗しているおそれがあります。一定時間（24 時間）経っても未インストールの状態にならない場合は、再度アンインストール指示を実施してください。 |
| アンインストール要求失敗 | アンインストール指示が失敗した状態。 | アンインストールが失敗しています。再度アンインストール指示を実施してください。 |
| アンインストール失敗 | スマートデバイスでアンインストールが失敗した状態。 | |

### Android の場合

| 項目 | 配布状況 | 説明 | 備考 |
|---|---|---|---|
| 配布状況 | 未配布 | アプリケーションが配布されていない状態。 | － |
| | 配布済み | アプリケーションが配布されている状態。 | － |
| 最終配布制御状態 | 正常 | 配布または削除が正常終了している状態。 | － |

| 項目 | 配布状況 | 説明 | 備考 |
|---|---|---|---|
| 最終配布制御状態 | 削除失敗 | スマートデバイスで、配布したアプリケーションの削除に失敗した状態。 | 配布したアプリケーションの削除に失敗しています。再度アプリケーションの削除を実施してください。 |
| | 削除処理中 | 配布したアプリケーションの削除要求が成功した状態。 | 一定時間（24 時間）経っても未配布の状態にならない場合は、再度アプリケーションの削除を実施してください。 |
| | 配布処理中 | アプリケーションの配布要求が成功した状態。 | 一定時間（24 時間）経っても配布済みまたは配布失敗の状態にならない場合は、再度アプリケーションの配布を実施してください。 |
| | 配布失敗 | アプリケーションの配布が失敗した状態。 | アプリケーションの配布が失敗しています。再度アプリケーションの配布を実施してください。 |
| 最終インストール制御状態 | 未インストール | アプリケーションがインストールされていない状態。 | － |
| | インストール済み | アプリケーションがインストールされている状態。 | － |
| | インストール失敗 | スマートデバイスでインストールが失敗した状態。 | アプリケーションのインストールが失敗しています。再度アプリケーションのインストールを実施してください。 |
| | アンインストール失敗 | スマートデバイスでアンインストールが失敗した状態。 | アプリケーションのアンインストールが失敗しています。再度アプリケーションのアンインストールを実施してください。 |

## 形式

```
sdmexportdistributestatus -os OS種別 -package パッケージ名[ -version バージョン] -file 配布状況出力ファイル
```

## 引数

-os OS 種別

OS 種別を指定します。

指定できる OS 種別は次のとおりです。

0：Android

1：iOS

-package パッケージ名

出力対象アプリケーションのパッケージ名を指定します。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

-version バージョン

出力対象アプリケーションのバージョンを指定します。省略した場合は、すべてのバージョンの配布状況が出力されます。ただし、次の文字は指定できません。

「<」、「>」、「&」、「|」、「^」、「%」

-file 配布状況出力ファイル

アプリケーションの配布状況を出力する配布状況出力ファイル名を 259 バイト以内の絶対パスで指定します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。

## 使用例

- アプリケーション（パッケージ名：PackageA、バージョン：1.0）の配布状況を配布状況出力ファイル C:¥temp¥PacA_0100_DB.csv に出力する場合の使用例を次に示します。

```
sdmexportdistributestatus -package PackageA -version 1.0 -file C:¥temp¥PacA_0100_DB.csv
```

- アプリケーション（パッケージ名：PackageA、バージョン：すべてのバージョン）の配布状況を配布状況出力ファイルC:¥temp¥PacA_all_DB.csv に出力する場合の使用例を次に示します。

```
sdmexportdistributestatus -package PackageA -file C:¥temp¥PacA_all_DB.csv
```

### 関連項目

- 15. コマンドを実行する流れ
- 付録 E.10 配布状況出力ファイルの形式

# sdmexportinstallapp（インストールソフトウェア情報の出力）

全スマートデバイスのインストールソフトウェア情報をファイル出力するコマンドです。

## 機能

全スマートデバイスにインストールされているソフトウェア情報をインストールソフトウェア情報出力ファイルに出力します。

## 形式

```
sdmexportinstallapp -file インストールソフトウェア情報出力ファイル
```

## 引数

-file インストールソフトウェア情報出力ファイル

全スマートデバイスにインストールされているソフトウェア情報を出力するインストールソフトウェア情報出力ファイル名を 259 バイト以内の絶対パスで指定します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- このコマンドを実行するには、スマートデバイスマネージャーが開始している必要があります。
- このコマンドを実行するには、スマートデバイスマネージャーのデータベースサービスが開始している必要があります。

## 使用例

全スマートデバイスのインストールソフトウェア情報をインストールソフトウェア情報出力ファイルC:¥temp¥installsoft_inf.csv に出力する場合の使用例を次に示します。

```
sdmexportinstallapp -file C:¥temp¥installsoft_inf.csv
```

### 関連項目

- 15. コマンドを実行する流れ
- 付録 E.11 インストールソフトウェア情報出力ファイルの形式

# sdmnetchange（スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更）

スマートデバイスマネージャーまたは通信サーバに設定されている接続先アドレスおよびポート番号を変更するコマンドです。

## 機能

スマートデバイスマネージャーまたは通信サーバに設定されている接続先アドレスおよびポート番号を変更します。

なお、このコマンドは変更対象のスマートデバイスマネージャー上、または変更対象の通信サーバ上で実行してください。

## 形式 1

```
sdmnetchange -target Manager -port ポート番号
```

## 形式 2

```
sdmnetchange -target Comsrv {-db データベースアドレス | -port ポート番号 | -db データベースアドレス -port ポート番号}
```

## 引数

-target {Manager | Comsrv}

変更対象のサーバ名を指定します。

- スマートデバイスマネージャーの場合：Manager
- 通信サーバの場合：Comsrv

-db **データベースアドレス**

データベースアドレス（接続先 IP アドレス）を変更する場合に指定します。この引数は、変更対象のサーバが通信サーバの場合だけ指定できます。

-port **ポート番号**

データベースの接続先ポート番号を変更する場合に指定します。この引数は、変更対象のサーバがスマートデバイスマネージャーの場合は必須です。

スマートデバイスマネージャーと通信サーバでは指定するポートが異なります。変更対象のサーバがスマートデバイスマネージャーの場合は、スマートデバイスマネージャー接続用のポート番号を指定します。変更対象のサーバが通信サーバの場合は、通信サーバ接続用のポート番号を指定します。

## 格納先

スマートデバイスマネージャーの場合

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

通信サーバの場合

JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- コマンドを実行する前に、データベースサービス以外の次の Windows サービスを停止してください。

  スマートデバイスマネージャー

  - JP1/ITDM2 - Smart Device Manager Server Service
  - JP1/ITDM2 - Smart Device Manager Web Server

  通信サーバ

  - JP1/ITDM2 - Smart Device Manager (Communication Server Service)
  - JP1/ITDM2 - Smart Device Manager Web Server

  また、コマンド実行後、上記のサービスを再起動する必要があります。
- このコマンドは、同時に複数実行できません。

## 戻り値

| 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 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 18 | ほかのコマンドを実行中です。 |
| 64 | XML ファイルのオープンに失敗しました。 |
| 66 | JP1/ITDM2 - Smart Device Manager Server Service の停止に失敗しました。 |
| 67 | JP1/ITDM2 - Smart Device Manager Server Service の開始に失敗しました。 |
| 68 | JP1/ITDM2 - Smart Device Manager (Communication Server Service)の停止に失敗しました。 |

| 戻り値 | 説明 |
|---|---|
| 69 | JP1/ITDM2 - Smart Device Manager (Communication Server Service)の開始に失敗しました。 |
| 80 | JP1/ITDM2 - Smart Device Manager Server Service が起動中です。<br>Windows の［サービス］画面で、このサービスを停止してからコマンドを再度実行してください。 |
| 81 | JP1/ITDM2 - Smart Device Manager (Communication Server Service)が起動中です。<br>Windows の［サービス］画面で、このサービスを停止してからコマンドを再度実行してください。 |
| 150 | そのほかのエラーが発生しました。 |

## 使用例

- スマートデバイスマネージャーのデータベースの接続先ポート番号を変更する場合の使用例を次に示します。

```
sdmnetchange -target Manager -port 32000
```

- 通信サーバのデータベースの接続先アドレスおよびポート番号を変更する場合の使用例を次に示します。

```
sdmnetchange -target Comsrv -db 192.168.1.13 -port 32001
```

### 関連項目

- 12.3 データベースの接続先ポート番号を変更する手順
- 15. コマンドを実行する流れ

# sdmcreatemdmcertreq（MDM 用署名済み証明書要求ファイルの作成）

iOS 端末を管理する場合、MDM 用署名済み証明書要求ファイルを作成するためのコマンドです。

## 機能

MDM 用署名済み証明書要求ファイルを作成します。iOS 端末を管理する場合に使用します。このコマンドで作成したファイルのファイル名は、「plist_encoded（-x 指定時はplist.xml）」です。

なお、このコマンドはスマートデバイスマネージャー上または通信サーバ上で実行してください。

## 形式

```
sdmcreatemdmcertreq -a エイリアス名 -p パスワード -f 署名用ファイル格納フォルダ名[ -o ファイル出力先][ -x]
```

## 引数

-a エイリアス名

MDM 用証明書要求ファイル作成時に指定したエイリアス名を 260 バイト以内で指定します。

-p パスワード

MDM 用証明書要求ファイル作成時に指定したパスワードを 260 バイト以内で指定します。

-f 署名用ファイル格納フォルダ名

MDM 用証明書要求ファイルを署名するためのファイル格納場所を 260 バイト以内の絶対パスで指定します。

-o ファイル出力先

MDM 用署名済み証明書要求ファイルの出力先を 260 バイト以内の絶対パスで指定します。

-x

MDM 用署名済み証明書要求ファイルを XML 形式（未エンコード）で出力する場合に指定します。

## 格納先

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

このコマンドは、同時に複数実行できません。

## 戻り値

| 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。 |
| 14 | ファイルが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 70 | エイリアス名に誤りがあります。 |
| 71 | パスワードに誤りがあります。 |
| 150 | そのほかのエラーが発生しました。 |

## 使用例

- MDM 用署名済みファイル（plist_encoded）作成時の使用例を次に示します。

```
sdmcreatemdmcertreq -a mdmalias -p mdmpass -f C:¥work -o C:¥temp
```

- MDM 用署名済みファイル作成時、XML 形式（plist.xml）で出力する場合の使用例を次に示します。

```
sdmcreatemdmcertreq -a mdmalias -p mdmpass -f C:¥work -o C:¥temp -x
```

### 関連項目

- 3.11.4 APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ（iOS 端末を管理する場合）
- 3.11.5 MDM 用証明書要求ファイルをダウンロードする手順（iOS 端末を管理する場合）
- 3.11.6 MDM 用署名済み証明書要求ファイルを作成する手順（iOS 端末を管理する場合）
- 15. コマンドを実行する流れ

# sdmgetlogs（ログ情報の取得）

スマートデバイスマネージャー、通信サーバ、JP1/ITDM2 - SDM（スマートデバイスエージェント）、またはメッセージングサーバのログ情報を zip 形式に圧縮して取得するコマンドです。

## 機能

スマートデバイスマネージャー、通信サーバ、JP1/ITDM2 - SDM（スマートデバイスエージェント）、またはメッセージングサーバのログ情報を zip 形式に圧縮して取得します。

なお、このコマンドはログ収集対象のサーバで実行してください。収集対象が JP1/ITDM2 - SDM（スマートデバイスエージェント）の場合は、通信サーバで実行してください。

出力ファイル名は次のとおりです。

| 収集対象 | ファイル名 |
|---|---|
| スマートデバイスマネージャー | tsinfo_manager.zip |
| 通信サーバ | tsinfo_comsrv.zip |
| JP1/ITDM2 - SDM（スマートデバイスエージェント） | tsinfo_agent.zip |
| メッセージングサーバ | tsinfo_msgsrv.zip |

## 形式

```
sdmgetlogs -target ログ収集対象[ -f 出力先フォルダ名]
```

## 引数

-target **ログ収集対象**

ログ収集対象を次のとおりに指定します。

| 収集対象 | 指定する内容 |
|---|---|
| スマートデバイスマネージャー | Manager |
| 通信サーバ | Comsrv |
| JP1/ITDM2 - SDM（スマートデバイスエージェント） | Agent |
| メッセージングサーバ | Msgsrv |

-f **出力先フォルダ名**

ログ取得情報の出力先フォルダ名を 161 バイト以内の絶対パスで指定します。

省略した場合、次のフォルダを作成してログ取得情報を出力します。

| 収集対象 | 引数を省略した場合の出力先 |
|---|---|
| スマートデバイスマネージャー | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥troubleshoot |
| 通信サーバ | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥troubleshoot |
| JP1/ITDM2 - SDM（スマートデバイスエージェント） | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥troubleshoot |
| メッセージングサーバ | JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥troubleshoot |

## 格納先

コマンドの格納先は次のとおりです。

| 収集対象 | 格納先 |
|---|---|
| スマートデバイスマネージャー | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin |
| 通信サーバ | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥bin |
| JP1/ITDM2 - SDM（スマートデバイスエージェント） | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥bin |
| メッセージングサーバ | JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥bin |

## 実行権限

Administrator 権限（Windows の UAC 機能が有効な場合は管理者コンソールから実行）

## 注意事項

- JP1/ITDM2 - SDM（スマートデバイスエージェント）のログ情報を収集する場合は、コマンド実行前に JP1/ITDM2 - SDM（スマートデバイスエージェント）から通信サーバにログ情報を送信しておく必要があります。
- このコマンドは、同時に複数実行できません。

## 戻り値

| 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。または、コマンドの引数に指定したフォルダ名長が上限値を超えています。 |
| 12 | コマンドの実行権限がありません。 |
| 13 | 指定されたサーバに誤りがあります。または、JP1/ITDM2 - SDM（スマートデバイスマネージャー）の動作環境が不正です。 |

| 戻り値 | 説明 |
|---|---|
| 14 | フォルダが存在しないか、アクセス権がありません。 |
| 15 | 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。 |
| 18 | ほかのコマンドを実行中です。 |
| 150 | そのほかのエラーが発生しました。 |

## 使用例

- スマートデバイスマネージャーのログ情報をC:¥work フォルダに出力する場合の使用例を次に示します。

```
sdmgetlogs -target Manager -f C:¥work
```

- 通信サーバのログ情報をC:¥work フォルダに出力する場合の使用例を次に示します。

```
sdmgetlogs -target Comsrv -f C:¥work
```

- JP1/ITDM2 - SDM（スマートデバイスエージェント）のログ情報を通信サーバのC:¥work フォルダに出力する場合の使用例を次に示します。

```
sdmgetlogs -target Agent -f C:¥work
```

- メッセージングサーバのログ情報をC:¥work フォルダに出力する場合の使用例を次に示します。

```
sdmgetlogs -target Msgsrv -f C:¥work
```

### 関連項目

- 8.12 スマートデバイスのログを取得する手順
- 15. コマンドを実行する流れ

# 16 定義ファイル

ここでは、JP1/ITDM2 - SDM で使用する定義ファイルについて説明します。

# 16.1　定義ファイル一覧

JP1/ITDM2 - SDM で使用する定義ファイルを一覧で説明します。

### 定義ファイル一覧

| サーバ | 定義ファイル | ファイル名 | 内容 |
|---|---|---|---|
| スマートデバイスマネージャー | スマートデバイスマネージャー環境設定ファイル | manager.properties | スマートデバイスマネージャーの環境設定ファイルです。 |
| | Provisioning 情報設定ファイル | provisioning.properties | スマートデバイスのプロビジョニング情報設定ファイルです。 |
| | イベントメールフォーマット情報ファイル | eventmail.properties | イベントメールのフォーマット情報ファイルです。 |
| | テストメール送信フォーマット情報ファイル | testmail.properties | テストメールのフォーマット情報ファイルです。 |
| 通信サーバ | 通信サーバ環境設定ファイル | CommunicationServerEngine.properties | 通信サーバの環境設定ファイルです。 |
| メッセージングサーバ | メッセージングサーバ設定ファイル | SdMessagingServer.ini | メッセージングサーバの環境設定ファイルです。 |

**重要**

定義ファイルを変更して設定を反映するためには、定義ファイルを格納するサーバを再起動する必要があります。

### 関連項目

- 16.2　スマートデバイスマネージャー環境設定ファイル（manager.properties）
- 16.3　Provisioning 情報設定ファイル（provisioning.properties）
- 16.4　イベントメールフォーマット情報ファイル（eventmail.properties）
- 16.5　テストメール送信フォーマット情報ファイル（testmail.properties）
- 16.6　通信サーバ環境設定ファイル（CommunicationServerEngine.properties）
- 16.7　メッセージングサーバ設定ファイル（SdMessagingServer.ini）

# 16.2 スマートデバイスマネージャー環境設定ファイル (manager.properties)

スマートデバイスマネージャーの動作環境を設定します。

### 記述形式

```
callhistory=通話履歴の保存期間
webhistory=Web閲覧履歴の保存期間
apphistory=アプリケーション使用履歴の保存期間
gpsevent=GPS電源OFFでのイベント発行有無
gpsmapview=GPS情報表示時、地図表示サイトとの連携有無
sdcardevent=SDカードの使用でのイベント発行有無
bluetoothevent=Bluetooth接続でのイベント発行有無
bluetoothalertlevel=Bluetooth接続でイベント発行する場合の警告レベル
simevent=SIMカードの変更でのイベント発行有無
unlockevent=次回ロックの解除までのイベント発行有無、イベントを発行するまでの日数
unconectedevent=インベントリ収集未完了時のイベント発行期間
callhistory.securityinterval=通話履歴のセキュリティチェック間隔
webhistory.securityinterval=Web閲覧履歴のセキュリティチェック間隔
application.securityinterval=アプリケーションのセキュリティチェック間隔
bluetooth.securityinterval=Bluetooth履歴のセキュリティチェック間隔
baseinfo.securityinterval=基本情報のセキュリティチェック間隔
communicationserverurl=通信サーバのアドレス
detail.debug.log.mode=トレースログの詳細ログ出力モード
distribute.mode=アプリケーションの配布方式
distribute.auth=アクセス認証有無
```

### 記述項目

スマートデバイスマネージャー環境設定ファイルの記述項目と設定値を次に示します。

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| callhistory | 通話履歴の保存期間を設定します。 | 1～365（単位：日） | 120 |
| webhistory | Web 閲覧履歴の保存期間を設定します。 | 1～365（単位：日） | 120 |
| apphistory | アプリケーション使用履歴の保存期間を設定します。 | 1～365（単位：日） | 120 |
| gpsevent | GPS 電源 OFF でイベント発行するかどうかを設定します。 | true<br>イベントを発行する<br>false<br>イベントを発行しない | true |
| gpsmapview | GPS 情報表示時、地図表示サイトと連携するかどうかを設定します。 | true<br>地図表示サイトと連携する | true |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| gpsmapview | GPS 情報表示時、地図表示サイトと連携するかどうかを設定します。 | false<br>地図表示サイトと連携しない | true |
| sdcardevent | SD カードの使用でイベント発行するかどうかを設定します。 | true<br>イベントを発行する<br>false<br>イベントを発行しない | true |
| bluetoothevent | Bluetooth 接続でイベント発行するかどうかを設定します。 | true<br>イベントを発行する<br>false<br>イベントを発行しない | true |
| bluetoothalertlevel | Bluetooth 接続でイベント発行する場合の警告レベルを設定します。 | 0<br>緊急<br>1<br>警戒<br>2<br>情報 | 0 |
| simevent | SIM カードの変更でイベント発行するかどうかを設定します。 | true<br>イベントを発行する<br>false<br>イベントを発行しない | true |
| unlockevent | 次回ロックの解除までにイベントを発行するかどうか、またはイベントを発行する場合は、イベントを発行するまでの日数を設定します。 | 0<br>イベントを発行しない<br>1～7<br>イベントを発行するまでの日数（単位：日） | 1 |
| unconectedevent | インベントリ収集未完了時のイベント発行期間を設定します。 | 1～7（単位：日） | 1 |
| callhistory.securityinterval | 通話履歴のセキュリティチェック間隔を設定します。 | 1～86400（単位：分） | 1440 |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| webhistory.securityinterval | Web 閲覧履歴のセキュリティチェック間隔を設定します。 | 1～86400（単位：分） | 1440 |
| application.securityinterval | アプリケーションのセキュリティチェック間隔を設定します。 | 1～86400（単位：分） | 1440 |
| bluetooth.securityinterval | Bluetooth 履歴のセキュリティチェック間隔を設定します。 | 1～86400（単位：分） | 1440 |
| baseinfo.securityinterval | 基本情報のセキュリティチェック間隔を設定します。 | 1～86400（単位：分） | 1440 |
| communicationserverurl | スマートデバイスマネージャーの接続先通信サーバのアドレスを設定します。<br>この項目は必須です。 | **ホスト名:ポート番号**<br>**ホスト名**<br>通信サーバのホスト名（FQDN 形式）<br>**ポート番号**※1<br>通信サーバの SSL 通信用 https ポート番号（デフォルト：26055） | なし |
| detail.debug.log.mode | トレースログの詳細ログ出力モードを設定します。 | 0<br>無効<br>1<br>有効 | 0 |
| distribute.mode※2 | アプリケーションの配布方式を設定します。 | 0<br>簡易配布<br>1<br>標準配布 | 1 |
| distribute.auth※2 | 標準配布の場合にアクセス認証をするかどうかを設定します。※3 | 0<br>認証なし<br>1<br>認証あり | 1 |

注※1

通信サーバの httpsd.conf に指定したポート番号と同一である必要があります。

注※2

「0」または「1」以外の値が指定されている場合または項目がない場合、「0」が仮定されます。

注※3

アクセス認証をしない場合、JP1/ITDM2 - SDM（通信サーバ）の httpsd.conf ファイルの次の行をコメントアウトし、通信サーバのサービス「JP1/ITDM2 - Smart Device Manager Web Server」を再起動してください。

```
<Directory ”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/uC/httpsd/htdocs/download”>
    AuthType Basic
    AuthName ”realm”
    AuthUserFile ”JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ/cms/conf/htpasswd”
    Require valid-user
</Directory>
```

### 記述例

```
callhistory=120
webhistory=120
apphistory=120
gpsevent=true
gpsmapview=true
sdcardevent=true
bluetoothevent=true
bluetoothalertlevel=1
simevent=true
unlockevent=1
unconectedevent=1
callhistory.securityinterval=30
webhistory.securityinterval=30
application.securityinterval=30
bluetooth.securityinterval=30
baseinfo.securityinterval=30
communicationserverurl=xxxxxxx.xxxxxxx.co.jp:26055
detail.debug.log.mode=1
distribute.mode=1
distribute.auth=1
```

# 16.3 Provisioning 情報設定ファイル（provisioning.properties）

スマートデバイス上で稼働する JP1/ITDM2 - SDM（スマートデバイスエージェント）のプロビジョニングを設定します。

### 記述形式

```
communicationserveraddress=通信サーバ接続先アドレス
messagingseverurl=メッセージングサーバ接続先アドレス
inventoryinterval=インベントリ間隔
gpsinterval=GPS情報取得間隔
lowbattery=低電圧時にインベントリを送信するバッテリー容量
```

### 記述項目

Provisioning 情報設定ファイルの記述項目と設定値を次に示します。

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| communicationserveraddress | 通信サーバ接続先アドレスを設定します。<br>この項目は必須です。 | **ホスト名:ポート番号**<br>**ホスト名**<br>通信サーバのホスト名（FQDN 形式）<br>**ポート番号**※1<br>通信サーバの SSL 通信用 https ポート番号（デフォルト：26055） | なし |
| messagingseverurl | メッセージングサーバ接続先アドレスを設定します（Android 限定）。<br>この項目は必須です。 | **ホスト名:ポート番号**<br>**ホスト名**<br>メッセージングサーバのホスト名（FQDN 形式）<br>**ポート番号**※2<br>メッセージングサーバの通信用 http ポート番号（デフォルト：26079） | なし |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| inventoryinterval | インベントリ間隔を設定します。 | 0～24（単位：時間）※3 | 24 |
| gpsinterval | GPS 情報取得間隔を設定します。 | 1～24（単位：時間） | 24 |
| lowbattery | 低電圧時にインベントリを送信するバッテリー容量を設定します。<br>コンマ区切りで複数設定できます。<br>（例）15,10,5 | 1～100（単位：%） | 5 |

注※1

通信サーバの httpsd.conf に指定したポート番号と同一である必要があります。

注※2

メッセージングサーバ設定ファイル（SdMessagingServer.ini）の HttpPort に設定するポート番号と同一である必要があります。

注※3

0 を指定した場合、インベントリ情報は収集しません。

運用時の管理対象スマートデバイスの台数が多くなる（1,000 台以上）とインベントリの収集に 1 時間以上かかることがあるため、その場合は 2 以上の値を設定してください。

## 記述例

```
communicationserveraddress=xxxxxxx.xxxxxxx.co.jp:26055
messagingseverurl=xxxxxxx.xxxxxxx.co.jp:26079
inventoryinterval=24
gpsinterval=24
lowbattery=10,5
```

## 関連項目

- 16.7　メッセージングサーバ設定ファイル（SdMessagingServer.ini）

# 16.4　イベントメールフォーマット情報ファイル（eventmail.properties）

イベントメールの形式を設定します。

### 記述形式

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>イベントメールプロパティ</comment>

<!-- メールサブジェクト -->
<entry key="mail_subject">メールの件名</entry>

<!-- メールヘッダー -->
<!--
下記のパラメータ文字 {} を対応するデータに置き換えデータを作成する。

{EVENT_COUNT}            ：イベント件数
 -->
<entry key="mailheader">メールヘッダー</entry>


<!-- メールフッター -->
<entry key="mailfooter">メールフッター</entry>


<!-- メールフォーマット -->
<!--
下記のパラメータ文字{}を対応するデータに置き換えデータを作成する。

{STATUS}                 ：確認状態
{ALERT_LEVEL}            ：重大度
{MESSAGE_ID}             ：イベント番号
{MESSAGE_CONTENT}        ：イベントの内容
{NOTE}                   ：イベントの詳細情報
{EVENT_DATE}             ：イベントの登録日時
{MESSAGE_TYPE}           ：イベントの種類
{EVENT_ORIGIN}           ：イベントの発生元
 -->
<entry key="mailformat">メール本文</entry>
</properties>
```

### 記述項目

イベントメールフォーマット情報ファイルの記述項目を次に示します。

| 項目 | 説明 |
|---|---|
| mail_subject | メールの件名を設定します。 |
| mailheader | メールヘッダーを設定します。 |
| mailfooter | メールフッターを設定します。 |

| 項目 | 説明 |
|---|---|
| mailformat | メール本文を設定します。 |

イベントメールの記述時に使用できるパラメーター文字を次に示します。パラメーター文字を使用すると、パラメーター文字に対応した内容に置き換えてメールが送信されます。

| パラメーター文字 | 内容 |
|---|---|
| {EVENT_COUNT} | イベント件数 |
| {STATUS} | 確認状態 |
| {ALERT_LEVEL} | 重大度 |
| {MESSAGE_ID} | イベント番号 |
| {MESSAGE_CONTENT} | イベントの内容 |
| {NOTE} | イベントの詳細情報 |
| {EVENT_DATE} | イベントの登録日時 |
| {MESSAGE_TYPE} | イベントの種類 |
| {EVENT_ORIGIN} | イベントの発生元 |

**記述例**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>イベントメールプロパティ</comment>

<!-- メールサブジェクト -->
<entry key="mail_subject">Event Mail Information</entry>

<!-- メールヘッダー -->
<!--
下記のパラメータ文字{}を対応するデータに置き換えデータを作成する。

{EVENT_COUNT}            ：イベント件数
 -->
<entry key="mailheader"><![CDATA[イベント件数：{EVENT_COUNT}]]></entry>


<!-- メールフッター -->
<entry key="mailfooter"><![CDATA[
////////////////////////////////////
*  会社名：XXXXXXX
*  住所：XXXXXXXXX X-X-X
*  MAIL:XXXXXX@XXX.XX.XX
*  TEL:XXX-XXXX-XXXX
////////////////////////////////////
]]></entry>
```

```
<!-- メールフォーマット -->
<!--
下記のパラメータ文字{}を対応するデータに置き換えデータを作成する。

{STATUS}                  :確認状態
{ALERT_LEVEL}             :重大度
{MESSAGE_ID}              :イベント番号
{MESSAGE_CONTENT}         :イベントの内容
{NOTE}                    :イベントの詳細情報
{EVENT_DATE}              :イベントの登録日時
{MESSAGE_TYPE}            :イベントの種類
{EVENT_ORIGIN}            :イベントの発生元
 -->
<entry key="mailformat"><![CDATA[
確認状態                  :{STATUS}
重大度                    :{ALERT_LEVEL}
イベント番号              :{MESSAGE_ID}
イベントの内容            :{MESSAGE_CONTENT}
イベントの詳細情報        :{NOTE}
イベントの登録日時        :{EVENT_DATE}
イベントの種類            :{MESSAGE_TYPE}
イベントの発生元          :{EVENT_ORIGIN}
]]></entry>
</properties>
```

# 16.5　テストメール送信フォーマット情報ファイル（testmail.properties）

テストメールの形式を設定します。

### 記述形式

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>イベントメールプロパティ</comment>

<!-- メールサブジェクト -->
<entry key="mail_subject">メールの件名</entry>

<!-- メールヘッダー -->
<entry key="mailheader">メールヘッダー</entry>


<!-- メールフッター -->
<entry key="mailfooter">メールフッター</entry>

</properties>
```

### 記述項目

テストメール送信フォーマット情報ファイルの記述項目を次に示します。

| 項目 | 説明 |
|---|---|
| mail_subject | メールの件名を設定します。 |
| mailheader | メールヘッダーを設定します。 |
| mailfooter | メールフッターを設定します。 |

### 記述例

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>イベントメールプロパティ</comment>

<!-- メールサブジェクト -->
<entry key="mail_subject">JP1/ITDM2 - SDM Test mail</entry>

<!-- メールヘッダー -->
<entry key="mailheader"><![CDATA[メール送信確認]]></entry>


<!-- メールフッター -->
<entry key="mailfooter"><![CDATA[--message end--]]></entry>

</properties>
```

# 16.6 通信サーバ環境設定ファイル (CommunicationServerEngine.properties)

通信サーバの動作環境を設定します。

### 記述形式

```
messaging.server.address = メッセージングサーバの接続先アドレス
messaging.server.port = メッセージングサーバの接続先ポート番号
request.timeout.time = リクエストのタイムアウト時間
semaphore.wait.timeout.time = セマフォ確保のタイムアウト時間
ios.battery.inventory.timeout.time = iOS端末のバッテリー情報の取得間隔
detail.debug.log.mode = トレースログの詳細ログ出力モード
communication.server.address = 通信サーバのアドレス
ios.request.getinventory.timeout.time = iOS端末でのインベントリ収集処理のタイムアウト時間
ios.request.wipe.timeout.time = iOS端末での初期化処理のタイムアウト時間
ios.request.lock.timeout.time = iOS端末でのロック処理のタイムアウト時間
ios.request.clearpasscode.timeout.time = iOS端末でのパスコードリセットのタイムアウト時間
ios.request.installappli.timeout.time = iOS端末でのアプリケーションインストールのタイムアウト時間
ios.request.uninstallappli.timeout.time = iOS端末でのアプリケーション削除のタイムアウト時間
ios.request.unmanage.timeout.time = iOS端末での管理対象外処理のタイムアウト時間
ios.request.applyprofile.timeout.time = iOS端末でのプロファイル適用処理のタイムアウト時間
ios.request.removeprofile.timeout.time = iOS端末でのプロファイル適用解除処理のタイムアウト時間
ios.inventory.collect.run.mode = iOS端末へのインベントリ収集方式
ios.inventory.collect.run.time = iOS端末へのインベントリ収集時刻
```

### 記述項目

通信サーバ環境設定ファイルの記述項目と設定値を次に示します。

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| messaging.server.address | メッセージングサーバの接続先アドレスを設定します。<br>この項目は必須です。 | IPv4 アドレス | localhost |
| messaging.server.port | メッセージングサーバの接続先ポート番号を設定します。<br>この項目は必須です。 | 1～65535 | 26078 |
| request.timeout.time | リクエストのタイムアウト時間を設定します。 | 0～60（単位：分） | 5 |
| semaphore.wait.timeout.time | セマフォ確保のタイムアウト時間を設定します。 | 0～60（単位：分） | 5 |
| ios.battery.inventory.timeout.time | iOS 端末のバッテリー情報の取得間隔を設定します。 | 0、60～1440（単位：分）※1 | 0 |
| detail.debug.log.mode | トレースログの詳細ログ出力モードを設定します。 | 0<br>無効 | 0 |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| detail.debug.log.mode | トレースログの詳細ログ出力モードを設定します。 | 1<br>有効 | 0 |
| communication.server.address | 通信サーバのアドレスを設定します。iOS アプリケーションを配布する場合、この項目は必須です。 | **ホスト名:ポート番号**<br>**ホスト名**<br>通信サーバのホスト名（FQDN 形式）<br>**ポート番号**※2<br>通信サーバの SSL 通信用 https ポート番号（省略した場合は、443 ポートを使用します） | なし |
| ios.request.getinventory.timeout.time | iOS 端末にインベントリ収集要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.wipe.timeout.time | iOS 端末に初期化要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.lock.timeout.time | iOS 端末にロック要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.clearpasscode.timeout.time | iOS 端末にパスコードリセット要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.installappli.timeout.time | iOS 端末にアプリケーションインストール要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 4320 |
| ios.request.uninstallappli.timeout.time | iOS 端末にアプリケーション削除要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 4320 |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| ios.request.unmanage.timeout.time | iOS 端末を管理対象外にしてから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.applyprofile.timeout.time | iOS 端末にプロファイル適用要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.request.removeprofile.timeout.time | iOS 端末にプロファイル適用解除要求を行ってから要求をタイムアウトさせるまでの時間を設定します。 | 0～10080（単位：分）※3 | 1440 |
| ios.inventory.collect.run.mode | iOS 端末のインベントリ収集方式を設定します。 | time<br>時刻指定でインベントリを収集します。<br>interval<br>一定間隔でインベントリを収集します。<br>none<br>インベントリを収集しません。 | time |
| ios.inventory.collect.run.time | iOS 端末のインベントリ収集方式に time を設定した場合、収集する時刻を設定します。※4 | 時刻を hh:mm の形式で設定します。時刻を複数指定する場合は、コンマで区切って指定します。※5 | 04:00 |

注※1

0 を指定した場合、iOS 端末のバッテリー情報は取得しません。

注※2

httpsd.conf に指定したポート番号と同一である必要があります。

注※3

0 を指定した場合、該当の操作はタイムアウトされません。

注※4

インベントリ収集要求は 1 回／日程度実行することを推奨します。また、ほかの業務と実行時間帯が重ならないよう設定してください。

注※5

時刻を複数指定する場合は、それぞれの時刻の間隔を 1 時間以上空けて指定してください。それぞれの時刻の間隔が 1 時間より短い場合、1 時間より短い間隔で指定した時刻は無効となります。

## 記述例

```
messaging.server.address = localhost
messaging.server.port = 9000
request.timeout.time = 5
semaphore.wait.timeout.time = 5
ios.battery.inventory.timeout.time = 60
detail.debug.log.mode = 0
communication.server.address = xxxxxxx.xxxxxxx.co.jp:26055
ios.request.getinventory.timeout.time = 1440
ios.request.wipe.timeout.time = 1440
ios.request.lock.timeout.time = 1440
ios.request.clearpasscode.timeout.time = 1440
ios.request.installappli.timeout.time = 4320
ios.request.uninstallappli.timeout.time = 4320
ios.request.unmanage.timeout.time = 1440
ios.request.applyprofile.timeout.time = 1440
ios.request.removeprofile.timeout.time = 1440
ios.inventory.collect.run.mode = time
ios.inventory.collect.run.time = 04:00
```

# 16.7　メッセージングサーバ設定ファイル（SdMessagingServer.ini）

メッセージングサーバの動作環境を設定します。

### 記述形式

```
[MessagingServer]
HttpPort=Android端末との待ち受けポート番号
HttpAddress=Android端末の待ち受けをするIPアドレス
HttpKeepConnectTime=Android端末とのComet接続維持時間
HttpClosePendingTime=Android端末からの再接続のための待機時間
HttpMaxConnection=Android端末とのComet接続の最大同時接続数
ManagePort=通信サーバとの待ち受けポート番号
ManageAddress=通信サーバの待ち受けをするIPアドレス
```

### 記述項目

メッセージングサーバ設定ファイルの記述項目と設定値を次に示します。

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| HttpPort | Android 端末との TCP 接続のための待ち受けポート番号を設定します。<br>初期値を変更する場合、指定を省略したり、空文字を指定したりしたときは、ポート番号「80」で待ち受けが行われます。このため、この項目は必ず設定してください。 | 1～65535 | 26079 |
| HttpAddress | Android 端末との TCP 接続のための待ち受けをする IP アドレスを設定します。<br>指定を省略した場合、または空文字列を指定した場合は、ローカルコンピュータのすべての IP アドレスに対して待ち受けが行われます。 | IPv4 アドレス | なし |
| HttpKeepConnectTime | Android 端末との Comet 接続を維持する時間を秒単位で設定します。<br>設定された時間を超過した接続は、いったん切断され、JP1/ITDM2 - SDM（スマートデバイス Android エージェント）に対して再接続されます。 | 1 以上（上限値なし）（単位：秒） | 86400 |
| HttpClosePendingTime | Android 端末との Comet 接続が切断された際に、Android 端末からの再接続を待つための待機時間を設定します。 | 0～3600（単位：秒） | 60 |
| HttpMaxConnection | Android 端末との Comet 接続の最大同時接続数を設定します。 | 1～30000 | 10000 |

| 項目 | 説明 | 設定値 | 初期値 |
|---|---|---|---|
| HttpMaxConnection | 設定値を超過した接続要求は、接続後に直ちに切断されます。 | 1～30000 | 10000 |
| ManagePort | 通信サーバとの TCP 接続のための待ち受けポート番号を設定します。<br>初期値を変更する場合、指定を省略したり、空文字を指定したりしたときは、ポート番号「9000」で待ち受けが行われます。このため、この項目は必ず設定してください。 | 1～65535 | 26078 |
| ManageAddress | 通信サーバとの TCP 接続のために待ち受けをする IP アドレスを設定します。<br>指定を省略した場合、または空文字列を指定した場合は、ローカルコンピュータのすべての IP アドレスに対して待ち受けが行われます。 | IPv4 アドレス | なし |

## 記述例

```
[MessagingServer]
HttpPort=26079
HttpAddress=xxx.xxx.xxx.xxx
HttpKeepConnectTime=86400
HttpClosePendingTime=60
HttpMaxConnection=10000
ManagePort=26078
ManageAddress=xxx.xxx.xxx.xxx
```

# 17 メッセージ

ここでは、JP1/ITDM2 - SDM のメッセージを一覧で説明します。

# 17.1 メッセージの形式

JP1/ITDM2 - SDM が出力するメッセージは、メッセージ ID、メッセージ種別、およびメッセージテキストから構成されます。

メッセージ ID およびメッセージ種別と、構成する項目の意味を説明します。

形式：KNAFpnnnnn-m

KNAF

JP1/ITDM2 - SDM から出力されたメッセージであることを示します。

p

メッセージを出力したコンポーネントコードを示します。番号とコンポーネントの対応を次の表に示します。

| 番号 | コンポーネント |
|---|---|
| 0 | インストーラ |
| 1 | スマートデバイスマネージャー |
| 2 | 通信サーバ |
| 3 | メッセージングサーバ |
| 4 | JP1/ITDM2 - SDM（スマートデバイス Android エージェント） |
| 5 | JP1/ITDM2 - SDM（スマートデバイス iOS エージェント） |
| 6 | コマンド |

nnnnn

メッセージの番号を示します。

m

メッセージの種別を示します。出力されるメッセージ種別を次の表に示します。

| メッセージ種別 | 種類 | 説明 |
|---|---|---|
| E | エラー | エラーが発生しているため、処理を続行できません。 |
| W | 警告 | 警告が通知されましたが、処理を続行します。警告メッセージの内容を参照して、問題がないかどうかを確認してください。 |
| I | 情報 | 正常に処理されました。 |

## 17.2 イベントとして出力される JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージには、イベントとして出力されるものと、出力されないものがあります。

### JP1/ITDM2 - SDM（スマートデバイスマネージャー）の各メッセージのイベント出力の有無

| メッセージ ID | イベント出力 |
|---|---|
| KNAF100003-E | ○ |
| KNAF100004-W | ○ |
| KNAF100005-W | ○ |
| KNAF120000-I | ○ |
| KNAF120001-W | ○ |
| KNAF120002-W | ○ |
| KNAF120100-I | ○ |
| KNAF120101-E | ○ |
| KNAF120102-I | ○ |
| KNAF120103-E | ○ |
| KNAF120105-E | ○ |
| KNAF120107-E | ○ |
| KNAF120108-I | ○ |
| KNAF120109-W | ○ |
| KNAF120111-E | ○ |
| KNAF120113-E | ○ |
| KNAF120114-W | ○ |
| KNAF120115-W | ○ |
| KNAF120116-I | ○ |
| KNAF120117-E | ○ |
| KNAF120118-I | ○ |
| KNAF120119-I | ○ |
| KNAF120200-I | ○ |
| KNAF120201-E | ○ |
| KNAF120203-E | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF120204-I | ○ |
| KNAF120205-E | ○ |
| KNAF120207-E | ○ |
| KNAF120209-E | ○ |
| KNAF120211-E | ○ |
| KNAF120212-I | ○ |
| KNAF120213-W | ○ |
| KNAF120214-I | ○ |
| KNAF120215-W | ○ |
| KNAF120216-I | ○ |
| KNAF120217-W | ○ |
| KNAF120218-I | ○ |
| KNAF120219-W | ○ |
| KNAF120220-I | ○ |
| KNAF120221-W | ○ |
| KNAF120222-I | ○ |
| KNAF120223-W | ○ |
| KNAF120224-I | ○ |
| KNAF120225-I | ○ |
| KNAF120226-W | ○ |
| KNAF120227-I | ○ |
| KNAF120228-W | ○ |
| KNAF120229-I | ○ |
| KNAF120230-W | ○ |
| KNAF120231-I | ○ |
| KNAF120232-W | ○ |
| KNAF120233-I | ○ |
| KNAF120234-W | ○ |
| KNAF120300-I | ○ |
| KNAF120301-E | ○ |
| KNAF120302-I | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF120303-E | ○ |
| KNAF120305-E | ○ |
| KNAF120307-E | ○ |
| KNAF120309-E | ○ |
| KNAF120310-I | ○ |
| KNAF120311-E | ○ |
| KNAF120312-I | ○ |
| KNAF120313-E | ○ |
| KNAF120315-E | ○ |
| KNAF120317-E | ○ |
| KNAF120318-I | ○ |
| KNAF120319-E | ○ |
| KNAF120320-I | ○ |
| KNAF120321-E | ○ |
| KNAF120323-E | ○ |
| KNAF120325-E | ○ |
| KNAF120326-I | ○ |
| KNAF120327-E | ○ |
| KNAF120328-I | ○ |
| KNAF120329-E | ○ |
| KNAF120331-E | ○ |
| KNAF120332-I | ○ |
| KNAF120333-E | ○ |
| KNAF120401-E | ○ |
| KNAF120403-E | ○ |
| KNAF120405-E | ○ |
| KNAF120407-E | ○ |
| KNAF120409-E | ○ |
| KNAF120411-E | ○ |
| KNAF120501-E | ○ |
| KNAF120503-E | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF120505-E | ○ |
| KNAF120507-E | ○ |
| KNAF120509-E | ○ |
| KNAF120511-E | ○ |
| KNAF120513-E | ○ |
| KNAF120515-E | ○ |
| KNAF120517-E | ○ |
| KNAF120519-E | ○ |
| KNAF120521-E | ○ |
| KNAF120523-E | ○ |
| KNAF120524-E | ○ |
| KNAF120526-E | ○ |
| KNAF120528-E | ○ |
| KNAF120530-E | ○ |
| KNAF120531-E | ○ |
| KNAF120533-E | ○ |
| KNAF120535-E | ○ |
| KNAF120537-E | ○ |
| KNAF120539-E | ○ |
| KNAF120541-E | ○ |
| KNAF120543-E | ○ |
| KNAF120545-E | ○ |
| KNAF120547-E | ○ |
| KNAF120600-I | ○ |
| KNAF120601-E | ○ |
| KNAF120602-I | ○ |
| KNAF120603-E | ○ |
| KNAF120607-E | ○ |
| KNAF120700-I | ○ |
| KNAF120701-E | ○ |
| KNAF120702-I | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF120703-E | ○ |
| KNAF120707-E | ○ |
| KNAF120900-I | ○ |
| KNAF120901-E | ○ |
| KNAF120902-I | ○ |
| KNAF120903-E | ○ |
| KNAF120907-E | ○ |
| KNAF120908-I | ○ |
| KNAF120909-E | ○ |
| KNAF121000-I | ○ |
| KNAF121001-E | ○ |
| KNAF121003-E | ○ |
| KNAF121005-E | ○ |
| KNAF121006-I | ○ |
| KNAF121007-E | ○ |
| KNAF121009-E | ○ |
| KNAF121011-E | ○ |
| KNAF121013-E | ○ |
| KNAF121015-E | ○ |
| KNAF121017-E | ○ |
| KNAF121019-E | ○ |
| KNAF121021-E | ○ |
| KNAF121023-E | ○ |
| KNAF121024-I | ○ |
| KNAF121025-E | ○ |
| KNAF121026-I | ○ |
| KNAF121027-E | ○ |
| KNAF121028-I | ○ |
| KNAF121029-E | ○ |
| KNAF121030-I | ○ |
| KNAF121031-E | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF121033-E | ○ |
| KNAF121034-W | ○ |
| KNAF121035-W | ○ |
| KNAF121038-I | ○ |
| KNAF121039-W | ○ |
| KNAF121040-W | ○ |
| KNAF121045-I | ○ |
| KNAF121046-E | ○ |
| KNAF121047-E | ○ |
| KNAF121048-E | ○ |
| KNAF121049-I | ○ |
| KNAF121050-E | ○ |
| KNAF121051-E | ○ |
| KNAF121052-I | ○ |
| KNAF121053-E | ○ |
| KNAF121054-E | ○ |
| KNAF130000-I | ○ |
| KNAF130001-E | ○ |
| KNAF130002-I | ○ |
| KNAF130003-E | ○ |
| KNAF130004-I | ○ |
| KNAF130005-E | ○ |
| KNAF130008-I | ○ |
| KNAF130009-E | ○ |
| KNAF130012-I | ○ |
| KNAF130013-E | ○ |
| KNAF130016-I | ○ |
| KNAF130017-E | ○ |
| KNAF130018-I | ○ |
| KNAF130019-W | ○ |
| KNAF130024-I | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF130025-E | ○ |
| KNAF130026-I | ○ |
| KNAF130027-W | ○ |
| KNAF130028-I | ○ |
| KNAF130029-W | ○ |
| KNAF130030-W | ○ |
| KNAF130031-I | ○ |
| KNAF130032-W | ○ |
| KNAF130033-W | ○ |
| KNAF130037-I | ○ |
| KNAF130038-I | ○ |
| KNAF130039-W | ○ |
| KNAF130040-I | ○ |
| KNAF130041-I | ○ |
| KNAF130043-W | ○ |
| KNAF130044-W | ○ |
| KNAF130045-W | ○ |
| KNAF130046-W | ○ |
| KNAF130047-W | ○ |
| KNAF130048-W | ○ |
| KNAF130051-W | ○ |
| KNAF130056-I | ○ |
| KNAF130057-E | ○ |
| KNAF130060-I | ○ |
| KNAF130061-W | ○ |
| KNAF130062-I | ○ |
| KNAF130063-W | ○ |
| KNAF130064-W | ○ |
| KNAF130065-I | ○ |
| KNAF130066-W | ○ |
| KNAF130067-I | ○ |

| メッセージ ID | イベント出力 |
|---|---|
| KNAF130068-W | ○ |
| KNAF130069-I | ○ |
| KNAF130070-W | ○ |
| KNAF130071-I | ○ |
| KNAF130072-W | ○ |
| KNAF130073-I | ○ |
| KNAF130074-W | ○ |
| KNAF130075-I | ○ |
| KNAF130076-W | ○ |
| KNAF130077-I | ○ |
| KNAF130078-W | ○ |
| KNAF130079-W | ○ |
| KNAF130080-W | ○ |
| KNAF130081-W | ○ |
| KNAF130082-W | ○ |
| KNAF130083-W | ○ |
| KNAF130084-W | ○ |
| KNAF130086-W | ○ |
| KNAF130087-W | ○ |
| KNAF130088-W | ○ |
| KNAF130089-W | ○ |
| KNAF130090-W | ○ |
| KNAF130091-W | ○ |
| KNAF190001-I | × |
| KNAF190002-I | × |
| KNAF190003-I | × |
| KNAF190004-E | × |
| KNAF190005-E | × |
| KNAF190006-I | × |
| KNAF190007-I | × |
| KNAF190008-E | × |

| メッセージ ID | イベント出力 |
| --- | --- |
| KNAF190009-E | × |

（凡例）

○：出力する

×：出力しない

## 17.3 JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ一覧

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージについて説明します。

### KNAF100003-E

インスタンスの生成に失敗しました。**エラーの説明**(**インスタンス名**)
[要因] インスタンスの生成に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF100004-W

通信サーバとの接続に失敗しました。
[要因] 通信サーバとの接続に失敗した。
[処理] 接続を中止する。
[対処] 通信サーバが起動していることを確認する。
manager.properties の communicationserverurl が正しく設定されていることを確認する。
接続に必要なルート証明書が設定されているか確認する。

### KNAF100005-W

テストメールの送信に失敗しました。
[要因] テストメールの送信に失敗した。
[処理] メール通知を中止する。
[対処] testmail.properties の記述内容に誤りがないか見直す。または、メールサーバの接続設定を確認する。

### KNAF120000-I

manager.properties の変更を検出しました。**変更を検出したキー**:[**変更前の値**]->[**変更後の値**]

### KNAF120001-W

manager.properties の定義で未定義の項目があります。
**項目名**
[要因] manager.properties の必須定義項目に未定義の項目がある。
[処理] 処理を中止する。
[対処] 定義を追加し、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

### KNAF120002-W

定義ファイルの設定値が不正です。ファイル名：項目名

[要因] 定義ファイルの項目に不正な値が設定されている。

[処理] 定義ファイルの設定値を破棄して、処理を続行する。

[対処] 定義ファイルの設定値を見直し、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

### KNAF120100-I

ユーザーアカウントを作成しました。ユーザー ID：**ユーザー ID**

### KNAF120101-E

ユーザーアカウントの作成に失敗しました。ユーザー ID：**ユーザー ID**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120102-I

ユーザーアカウントを削除しました。ユーザー ID：**ユーザー ID**

### KNAF120103-E

ユーザーアカウントの削除に失敗しました。ユーザー ID：**ユーザー ID**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120105-E

ユーザーアカウント数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120107-E

ユーザーアカウント情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120108-I

ログインしました。

## KNAF120109-W

ログインに失敗しました。ユーザー ID：**ユーザー ID**

[要因]

・ユーザー ID、またはパスワードが異なっている。

・データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処]

・正しいユーザー ID とパスワードを設定し、再度ログインを行う。

・データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120111-E

ロール情報の取得に失敗しました。ユーザー ID：**ユーザー ID**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120113-E

ユーザーアカウントリストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120114-W

連続でログインに失敗しました。

[要因] 規定回数以上、連続でログイン失敗した。

[処理] 処理を中止する。

[対処] 正しい、ユーザー ID、パスワードを使用するか、管理者にユーザーの作成を依頼する。

## KNAF120115-W

ユーザーアカウントがロックされました。ユーザー ID：**ユーザー ID**

[要因] ユーザーアカウントがロックした。

[処理] 処理を中止する。

[対処] 管理者権限を持つユーザー ID にロック状態の解除を依頼する。

すべての管理者権限のユーザーがロックした場合、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動すると、ロックが解除される。

## KNAF120116-I

ユーザーアカウントを変更しました。

## KNAF120117-E

ユーザーアカウントの変更に失敗しました。

[要因]

・パスワードが間違っている。または、変更したパスワードが現在のパスワードと同じ。

・データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処]

・正しいパスワードを設定する。または、変更するパスワードは現在のパスワードと異なる値を設定する。

・データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120118-I

ユーザーアカウントのロックを解除しました。

### KNAF120119-I

ログアウトしました。ユーザー ID：**ユーザー ID**

### KNAF120200-I

スマートデバイスのインポートが完了しました。

### KNAF120201-E

スマートデバイスのインポートに失敗しました。エラー行番号：**行番号**
[要因] スマートデバイス情報のインポートに失敗した。
[処理] 処理を中止する。
[対処] 指定したファイルの行番号で発生したエラーを取り除き、再度インポートする。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120203-E

スマートデバイス情報のエクスポートに失敗しました。**エラーの説明**
[要因] スマートデバイス情報のエクスポートに失敗した。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120204-I

スマートデバイスを削除しました。**名称**

### KNAF120205-E

スマートデバイスの削除に失敗しました。**名称**
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120207-E

スマートデバイス数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120209-E

前日比情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120211-E

スマートデバイス情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120212-I

最新情報の取得要求を行いました。

## KNAF120213-W

最新情報の取得要求に失敗しました。

[要因] 最新情報の取得に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120214-I

初期化要求を行いました。

## KNAF120215-W

初期化要求に失敗しました。

[要因] 初期化要求に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120216-I

ロックを指示しました。

## KNAF120217-W

ロックの指示に失敗しました。

[要因] ロックの指示に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120218-I

パスワード更新を含む、ロックを指示しました。

## KNAF120219-W

パスワード更新を含む、ロックの指示に失敗しました。

[要因] パスワード更新を含む、ロックの指示に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120220-I

パスコードのリセットを指示しました。

## KNAF120221-W

パスコードのリセットの指示に失敗しました。

[要因] パスコードのリセットの指示に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120222-I

ログの取得要求を行いました。

## KNAF120223-W

ログの取得要求に失敗しました。

[要因] ログの取得要求に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する

## KNAF120224-I

管理対象外に設定しました。

## KNAF120225-I

強制的に管理対象外に設定しました。

## KNAF120226-W

管理対象外の設定に失敗しました。

[要因] 管理対象外の設定に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。スマートデバイスが故障、紛失などで接続できない場合は、「強制的に管理対象外にする」にチェックする。

## KNAF120227-I

セキュリティポリシーを適用しました。ポリシー名：**ポリシー名**

## KNAF120228-W

セキュリティポリシーの適用に失敗しました。ポリシー名：**ポリシー名**

[要因] セキュリティポリシーの適用に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

### KNAF120229-I

Android ポリシーの適用要求を行いました。ポリシー名：**ポリシー名**

### KNAF120230-W

Android ポリシーの適用要求に失敗しました。ポリシー名：**ポリシー名**

[要因] Android ポリシーの適用要求に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

### KNAF120231-I

iOS プロファイルの適用要求を行いました。プロファイル名：**プロファイル名**

### KNAF120232-W

iOS プロファイルの適用要求に失敗しました。プロファイル名：**プロファイル名**

[要因] iOS プロファイルの適用要求に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

### KNAF120233-I

メッセージ送信しました。

### KNAF120234-W

メッセージ送信に失敗しました。

[要因] メッセージ送信に失敗した。

[処理] 処理を中止する。

[対処] 圏外、もしくは WiFi 未接続の場合、操作できないため、取得対象のスマートデバイスがネットワークに接続しているか確認する。

## KNAF120300-I

セキュリティポリシーを作成しました。**ポリシー名**

## KNAF120301-E

セキュリティポリシーの作成に失敗しました。**ポリシー名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120302-I

セキュリティポリシーを削除しました。**ポリシー名**

## KNAF120303-E

セキュリティポリシーの削除に失敗しました。**ポリシー名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120305-E

セキュリティポリシー情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120307-E

セキュリティポリシー数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120309-E

セキュリティポリシー**ポリシー名**の電話番号リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120310-I

セキュリティポリシー**ポリシー名**の電話番号を追加、変更しました。

### KNAF120311-E

セキュリティポリシー**ポリシー名**の電話番号の追加、変更に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120312-I

セキュリティポリシー**ポリシー名**の電話番号を削除しました。

### KNAF120313-E

セキュリティポリシー**ポリシー名**の電話番号の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120315-E

セキュリティポリシー**ポリシー名**の電話番号の登録数の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120317-E

セキュリティポリシー**ポリシー名**の URL リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120318-I

セキュリティポリシー**ポリシー名**の URL を追加、変更しました。

### KNAF120319-E

セキュリティポリシー**ポリシー名**の URL の追加、変更に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120320-I

セキュリティポリシー**ポリシー名**の URL を削除しました。

### KNAF120321-E

セキュリティポリシー**ポリシー名**の URL の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120323-E

セキュリティポリシー**ポリシー名**の URL の登録数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120325-E

セキュリティポリシー**ポリシー名**のアプリケーションリストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120326-I

セキュリティポリシー**ポリシー名**のアプリケーションを追加、変更しました。

## KNAF120327-E

セキュリティポリシー**ポリシー名**のアプリケーションの追加、変更に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120328-I

セキュリティポリシー**ポリシー名**のアプリケーションを削除しました。

## KNAF120329-E

セキュリティポリシー**ポリシー名**のアプリケーションの削除に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120331-E

セキュリティポリシー**ポリシー名**のアプリケーションの登録数の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120332-I

セキュリティポリシーを変更しました。

### KNAF120333-E

セキュリティポリシーの変更に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120401-E

イベントの削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120403-E

イベントリストのエクスポートに失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120405-E

イベント数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120407-E

イベント情報リストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120409-E

イベント情報の追加、変更に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120411-E

アラートレベルの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120501-E

インベントリ情報の更新に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120503-E

インベントリ情報の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120505-E

通話履歴情報の更新に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120507-E

通話履歴情報の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120509-E

通話履歴情報数の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120511-E

URL 閲覧履歴情報の更新に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120513-E

URL 閲覧履歴情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120515-E

URL 閲覧履歴情報数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120517-E

インストールされているアプリケーション情報の作成に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120519-E

インストールされているアプリケーション情報数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120521-E

インストールされているアプリケーション情報リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120523-E

起動中アプリケーション情報の作成に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120524-E

起動中アプリケーション情報の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120526-E

起動中アプリケーション情報数の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120528-E

起動中アプリケーション情報リストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120530-E

動作中サービス情報の作成に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120531-E

動作中サービス情報の削除に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120533-E

動作中サービス情報数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120535-E

動作中サービス情報リストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120537-E

GPS 履歴情報の作成に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120539-E

GPS 履歴情報数の取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120541-E

GPS 履歴情報リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120543-E

Bluetooth 履歴情報の作成に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120545-E

Bluetooth 履歴情報数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120547-E

Bluetooth 履歴情報リストの取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120600-I

Android プロビジョニング情報を作成しました。

## KNAF120601-E

Android プロビジョニング情報の作成に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120602-I

Android プロビジョニング情報を削除しました。

## KNAF120603-E

Android プロビジョニング情報の削除に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120607-E

Android プロビジョニング情報リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120700-I

iOS プロビジョニング情報を作成しました。

### KNAF120701-E

iOS プロビジョニング情報の作成に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120702-I

iOS プロビジョニング情報を削除しました。

### KNAF120703-E

iOS プロビジョニング情報の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120707-E

iOS プロビジョニング情報リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120900-I

ポリシー・プロファイル情報を作成しました。

### KNAF120901-E

ポリシー・プロファイル情報の作成に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120902-I

ポリシー・プロファイル情報を削除しました。

### KNAF120903-E

ポリシー・プロファイル情報の削除に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF120907-E

ポリシー・プロファイル情報リストの取得に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF120908-I

ポリシー・プロファイル情報を変更しました。

## KNAF120909-E

ポリシー・プロファイル情報の変更に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121000-I

配布アプリケーションを削除しました。アプリケーション名：**アプリケーション名**

## KNAF121001-E

配布アプリケーションの削除に失敗しました。アプリケーション名：**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121003-E

配布アプリケーション数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121005-E

配布アプリケーション情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121006-I

配布アプリケーションを登録しました。アプリケーション名：**アプリケーション名**

### KNAF121007-E

配布アプリケーションの登録に失敗しました。アプリケーション名：**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121009-E

配布アプリケーション状態の削除に失敗しました。**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121011-E

配布アプリケーション状態数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121013-E

配布アプリケーション状態情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121015-E

配布アプリケーション状態情報の登録に失敗しました。**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121017-E

アプリケーションデータの削除に失敗しました。アプリケーション名：**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121019-E

アプリケーションデータ数の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121021-E

アプリケーションデータ情報の取得に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121023-E

アプリケーションデータ情報の登録に失敗しました。アプリケーション名：**アプリケーション名**

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121024-I

アプリケーションを配布しました。

### KNAF121025-E

アプリケーションの配布に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121026-I

アプリケーションのインストール要求をしました。

### KNAF121027-E

アプリケーションのインストール要求に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121028-I

アプリケーションの削除要求をしました。

### KNAF121029-E

アプリケーションの削除要求に失敗しました。
[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。
[処理] 処理を中止する。
[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121030-I

配布アプリケーションを変更しました。

## KNAF121031-E

配布アプリケーションの登録に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121033-E

配布アプリケーション状態情報の変更に失敗しました。

[要因] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))が停止している。

[処理] 処理を中止する。

[対処] データベースサービス(JP1/ITDM2 - Smart Device Manager (DB Service))を起動後、サービス(JP1/ITDM2 - Smart Device Manager Server Service)を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121034-W

アプリケーションのインストールに失敗しました。

[要因] 端末からエラーが通知された。

[処理] 処理を中止する。

[対処] 端末から通知されたエラーの内容を確認する。

## KNAF121035-W

アプリケーションの削除に失敗しました。

[要因] 端末からエラーが通知された。

[処理] 処理を中止する。

[対処] 端末から通知されたエラーの内容を確認する。

## KNAF121038-I

iOS プロファイルの適用解除要求を行いました。プロファイル名：**プロファイル名**

## KNAF121039-W

iOS プロファイルの適用解除要求に失敗しました。プロファイル名：**プロファイル名**

[要因] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）が停止している。

[処理] 処理を中止する。

[対処] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）を起動後、サービス（JP1/ITDM2 - Smart Device Manager Server Service）を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121040-W

iOS プロファイルの適用解除要求を行いませんでした。プロファイル名：**プロファイル名**

[要因] 端末に 1 個の iOS プロファイルしか適用されていない。

[処理] 処理を中止する。

[対処] 端末に 2 個以上の iOS プロファイルを適用後に再実行する。

## KNAF121045-I

sdmioutils imortdeliverypermit コマンドが完了しました。 **配布許可定義ファイルパス 行数**

## KNAF121046-E

sdmioutils importdeliverypermit コマンドでエラーが発生しました。 **配布許可定義ファイルパス エラー行番号**

[要因] 配布許可定義ファイルの書式が不正です。

[処理] 処理を中止する。

[対処] 指定したファイルの行番号で発生したエラーを取り除き sdmioutils importdeliverypermit コマンドを再実行する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121047-E

sdmioutils importdeliverypermit コマンドでエラーが発生しました。 **配布許可定義ファイルパス エラー行番号 配布アプリケーション名(バージョン)または配布許可対象名**

[要因] 配布許可定義ファイルまたはコマンド引数に指定した配布アプリケーションまた配布許可対象が見つかりません。

[処理] 処理を中止する。

[対処] エラーを取り除き、sdmioutils importdeliverypermit コマンドを再実行する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121048-E

sdmioutils importdeliverypermit コマンドでエラーが発生しました。 **配布許可定義ファイルパス**

[要因] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）が停止している。

[処理] 処理を中止する。

[対処] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）を起動後、サービス（JP1/ITDM2 - Smart Device Manager Server Service）を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121049-I

sdmioutils exportdeliverypermit コマンドが完了しました。 **配布許可定義ファイルパス 行数**

## KNAF121050-E

sdmioutils exportdeliverypermit コマンドでエラーが発生しました。 **配布許可定義ファイルパス**

[要因] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）が停止している。

[処理] 処理を中止する。

[対処] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）を起動後、サービス（JP1/ITDM2 - Smart Device Manager Server Service）を再起動する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121051-E

sdmioutils exportdeliverypermit コマンドでエラーが発生しました。 **配布許可定義ファイルパス 配布アプリケーション名(バージョン)または配布許可対象名**

[要因] コマンド引数に指定した配布アプリケーションまた配布許可対象が見つかりません。

[処理] 処理を中止する。

[対処] エラーを取り除き、sdmioutils exportdeliverypermit コマンドを再実行する。

解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF121052-I

sdmioutils deletedeliverypermit コマンドが完了しました。 **行数**

## KNAF121053-E

sdmioutils deletedeliverypermit コマンドでエラーが発生しました。 **配布アプリケーション名(バージョン)または配布許可対象名**

[要因] コマンド引数に指定した配布アプリケーションまたは配布許可対象が見つかりません。

[処理] 処理を中止する。
[対処] エラーを取り除き、sdmioutils deletedeliverypermit コマンドを再実行する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF121054-E

sdmioutils deletedeliverypermit コマンドでエラーが発生しました。
[要因] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）が停止している。
[処理] 処理を中止する。
[対処] データベースサービス（JP1/ITDM2 - Smart Device Manager (DB Service)）を起動後、サービス（JP1/ITDM2 - Smart Device Manager Server Service）を再起動する。
解決しない場合、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130000-I

詳細情報の更新が完了しました。

### KNAF130001-E

詳細情報の更新に失敗しました。
[要因] 詳細情報の更新に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130002-I

Bluetooth 接続情報を更新しました。

### KNAF130003-E

Bluetooth 接続情報の更新に失敗しました。
[要因] Bluetooth 接続情報の更新に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130004-I

通話履歴のセキュリティ検証を完了しました。

## KNAF130005-E

通話履歴のセキュリティ検証に失敗しました。
[要因] 通話履歴のセキュリティ検証に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF130008-I

アプリケーション情報のセキュリティ検証を完了しました。

## KNAF130009-E

アプリケーション情報のセキュリティ検証に失敗しました。
[要因] アプリケーション情報のセキュリティ検証に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF130012-I

WEB 閲覧履歴のセキュリティ検証を完了しました。

## KNAF130013-E

WEB 閲覧履歴のセキュリティ検証に失敗しました。
[要因] WEB 閲覧履歴のセキュリティ検証に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF130016-I

保持期間が過ぎた情報を削除しました。

## KNAF130017-E

保持期間が過ぎた情報の削除に失敗しました。
[要因] 保持期間が過ぎた情報の削除に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130018-I

重大度管理テーブルを更新しました。

### KNAF130019-W

重大度管理テーブルの更新に失敗しました。
[要因] 重大度管理テーブルの更新に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130024-I

詳細情報のセキュリティポリシーの検証を完了しました。

### KNAF130025-E

詳細情報のセキュリティポリシーの検証に失敗しました。
[要因] 詳細情報のセキュリティポリシーの検証に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130026-I

許可されている電話番号と通話しました。電話番号：**電話番号**

### KNAF130027-W

許可されていない電話番号と通話しました。電話番号：**電話番号**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130028-I

インストールが許可されています。アプリケーション名：**アプリケーション名**

### KNAF130029-W

インストールが禁止されています。アプリケーション名：**アプリケーション名**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。

[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130030-W

セキュリティリストにないアプリケーションがインストールされています。アプリケーション名：**アプリケーション名**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130031-I

閲覧は許可されています。URL：**URL**

### KNAF130032-W

閲覧は禁止されています。URL：**URL**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130033-W

セキュリティリストにないサイトを閲覧しています。
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130037-I

アプリケーションがインストールされました。

### KNAF130038-I

アプリケーションがアンインストールされました。

### KNAF130039-W

新たな Bluetooth 機器と接続しました。機器名：**機器名**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

## KNAF130040-I

Bluetooth 機器の接続を削除しました。機器名：**機器名**

## KNAF130041-I

詳細情報を更新しました。

## KNAF130043-W

IMEI/MEID 情報が変更されました。変更前：**変更前** 変更後：**変更後**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

## KNAF130044-W

OS のバージョン情報が変更されました。変更前：**変更前** 変更後：**変更後**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

## KNAF130045-W

ICCID 情報が変更されました。変更前：**変更前** 変更後：**変更後**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

## KNAF130046-W

SD カードを使用しています。
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

## KNAF130047-W

GPS の電源が OFF になっています。
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130048-W

一定期間ロック解除されていません。
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130051-W

必要なアプリケーションがインストールされていません。アプリケーション名：**アプリケーション名**
[要因] セキュリティポリシーの検証で違反を発見した。
[処理] 処理を続行する。
[対処] 規定しているセキュリティポリシーに則り、対処する。

### KNAF130056-I

スマートデバイスの管理台数を更新しました。

### KNAF130057-E

スマートデバイスの管理台数の更新に失敗しました。
[要因] スマートデバイスの管理台数の更新に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130060-I

イベント情報のメール通知を行いました。

### KNAF130061-W

イベント情報のメール送信に失敗しました。
[要因] イベント情報のメール送信に失敗した。
[処理] 処理を続行する。
[対処] トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF130062-I

最新情報を取得しました。

### KNAF130063-W

最新情報の取得に失敗しました。

[要因] 最新情報の取得に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130064-W

初期化に失敗しました。

[要因] 初期化に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130065-I

ロックしました。

## KNAF130066-W

ロックに失敗しました。

[要因] ロックに失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130067-I

パスコードリセットをしました。

## KNAF130068-W

パスコードリセットに失敗しました。

[要因] パスコードリセットに失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130069-I

ログの取得が完了しました。

## KNAF130070-W

ログの取得に失敗しました。

[要因] ログの取得に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130071-I

管理対象外に設定しました。

## KNAF130072-W

管理対象外の設定に失敗しました。

[要因] 管理対象外の設定に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130073-I

Android ポリシーを適用しました。

## KNAF130074-W

Android ポリシーの適用に失敗しました。

[要因] Android ポリシーの適用に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130075-I

iOS プロファイルを適用しました。

## KNAF130076-W

iOS プロファイルの適用に失敗しました。

[要因] iOS プロファイルの適用に失敗した。

[処理] 処理を続行する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130077-I

iOS プロファイルの適用を解除しました。

## KNAF130078-W

iOS プロファイルの適用解除に失敗しました。

[要因] iOS プロファイルの適用解除に失敗した。以下の要因が考えられる。

(1) スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した。

[処理] 処理を続行する。

[対処] しばらくしてから再度実行する。

## KNAF130079-W

アプリケーションのインストールに失敗しました。

[要因] アプリケーションのインストールに失敗した。

[処理] 処理を中止する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130080-W

アプリケーションの削除に失敗しました。

[要因] アプリケーションの削除に失敗した。

[処理] 処理を中止する。

[対処] スマートデバイスが圏外、または WiFi 接続断により、要求が失敗した可能性がある。しばらくしてから再度実行する。

## KNAF130081-W

最新情報の取得要求がタイムアウトしました。

[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。

[処理] 処理を続行する。

[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130082-W

初期化要求がタイムアウトしました。

[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130083-W

ロック要求がタイムアウトしました。
[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130084-W

パスコードリセット要求がタイムアウトしました。
[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130086-W

管理対象外の設定要求がタイムアウトしました。
[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130087-W

iOS プロファイルの適用要求がタイムアウトしました。
[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130088-W

iOS プロファイルの適用解除要求がタイムアウトしました。
[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。
[処理] 処理を続行する。
[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130089-W

アプリケーションのインストール要求がタイムアウトしました。

[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。

[処理] 処理を続行する。

[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130090-W

アプリケーションの削除要求がタイムアウトしました。

[要因] スマートデバイスが圏外、または WiFi 接続断により、要求がタイムアウトした。

[処理] 処理を続行する。

[対処] スマートデバイスの電源状態、またはネットワークの接続状態を確認して再度実行する。

## KNAF130091-W

指定した iOS プロファイルがスマートデバイスに存在しないため、iOS プロファイルの適用解除に失敗しました。プロファイル名:**プロファイル名称**

[要因] iOS プロファイルの適用解除に失敗した。以下の要因が考えられる。

(1) iOS プロファイル名がインポートしたプロファイルの表示名と一致していない。

(2) 指定した iOS プロファイルがスマートデバイスに適用されていない。

[処理] 処理を続行する。

[対処] iOS プロファイル名がインポートしたプロファイルの表示名と一致しているかを確認し、不一致の場合は iOS プロファイル名を正しい名称に修正する。

指定した iOS プロファイルがスマートデバイスから削除されている場合は、適用する Android ポリシー/iOS プロファイルから該当するプロファイルの情報を削除する。

## KNAF190001-I

JP1/ITDM2 - Smart Device Manager Server Service を起動します。

## KNAF190002-I

JP1/ITDM2 - Smart Device Manager Server Service を終了します。

## KNAF190003-I

システムが終了します。

## KNAF190004-E

システムエラーが発生しました。**エラーの説明**

[要因]システムエラーが発生した。
[処理]サービスを停止する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF190005-E

JP1/ITDM2 - Smart Device Manager Server Service の起動に失敗しました。
[要因]サービスの起動に失敗した。
[処理]サービスを停止する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF190006-I

JP1/ITDM2 - Smart Device Manager Server Service を登録しました。

### KNAF190007-I

JP1/ITDM2 - Smart Device Manager Server Service を削除しました。

### KNAF190008-E

JP1/ITDM2 - Smart Device Manager Server Service の登録に失敗しました。
[要因]Windows サービスへの登録に失敗した。
[処理]インストールを終了する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF190009-E

JP1/ITDM2 - Smart Device Manager Server Service の削除に失敗しました。
[要因]Windows サービスからの削除に失敗した。
[処理]アンインストールを終了する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

## 17.4 JP1/ITDM2 - SDM（メッセージングサーバ）のメッセージ一覧

JP1/ITDM2 - SDM（メッセージングサーバ）のメッセージについて説明します。

### KNAF300001-I

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)を起動します。

### KNAF300002-I

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)を終了します。

### KNAF300003-I

システムが終了します。

### KNAF300004-E

システムエラーが発生しました。**エラーの説明**
[要因]システムエラーが発生した。
[処理]サービスを停止する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300005-E

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)の起動に失敗しました。
[要因]サービスの起動に失敗した。
[処理]サービスを停止する。
[対処]本メッセージの前に出力されているメッセージの内容に従って対処する。対処できない場合は、トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300006-I

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)を登録しました。

### KNAF300007-I

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)を削除しました。

### KNAF300008-E

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)の登録に失敗しました。
[要因]Windows サービスへの登録に失敗した。

[処理]インストールを終了する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300009-E

JP1/ITDM2 - Smart Device Manager (Messaging Server Service)の削除に失敗しました。
[要因]Windows サービスからの削除に失敗した。
[処理]アンインストールを終了する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300201-E

サーバアドレスが無効です。
[要因]環境設定ファイルに定義した通信サーバもしくはエージェントからの接続待ち受けアドレスが不正。
[処理]サービスを停止する。
[対処]環境設定ファイルの定義値を確認する。問題が解決しない場合トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300202-E

スマートデバイスエージェントとの通信でエラーが発生しました。(Winsock エラーコード)
[要因]スマートデバイスエージェントとの通信でエラーが発生した。
[処理]処理を続行する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

### KNAF300203-I

サーバポートの待ち受けを開始しました。(IP アドレス:ポート番号)

### KNAF300204-I

サーバポートの待ち受けを終了しました。(IP アドレス:ポート番号)

### KNAF300205-I

スマートデバイスエージェントとの接続処理を開始します。(IP アドレス:ポート番号)

### KNAF300206-I

スマートデバイスエージェント(デバイス ID)との接続を解放しました。

## KNAF300207-E

受信データ長が最大サイズを超過しました。(**ソケット識別子**)
[要因]受信データ長が最大サイズを超過した。
[処理]処理を続行する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF300208-E

最大同時接続数を超過しました。
[要因]スマートデバイスエージェントとの同時接続数が超過した。
[処理]処理を続行する。
[対処]環境設定ファイルの定義値を確認する。問題が解決しない場合トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF300209-E

通信サーバとの通信でエラーが発生しました。(**WinSock エラーコード**)
[要因]通信サーバとの通信でエラーが発生した。
[処理]処理を続行する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF300210-E

サーバソケットでエラーが発生しました。(**WinSock エラーコード**)
[要因]通信エラーが発生した。
[処理]サービス起動時に発生した場合は、サービスを停止する。それ以外の場合は、処理を続行する。
[対処]環境設定ファイルの定義値を確認する。問題が解決しない場合トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF300211-W

データを送信しようとしたスマートデバイスエージェント(**デバイス ID**)は既に切断されています。
[要因]スマートデバイスエージェントと接続していない。
[処理]処理を続行する。
[対処]スマートデバイスエージェントの起動状態および通信状況を確認する。

## KNAF300212-I

スマートデバイスエージェント(**デバイス ID**)と接続しました。

## KNAF300213-E

環境設定ファイル(**ファイル名**)の読み込みに失敗しました。
[要因]環境設定ファイルのパスの取得に失敗した。
[処理]処理を続行する。
[対処]トラブルシュート情報取得後、サポートサービスへ連絡する。

## KNAF300214-W

処理を要求されたスマートデバイスエージェント(**デバイス ID**)は接続していません。
[要因]スマートデバイスエージェントと接続していない。
[処理]処理を続行する。
[対処]スマートデバイスエージェントの起動状態および通信状況を確認する。

## KNAF300215-I

スマートデバイスエージェント(**デバイス ID**)に接続要求を行います。

## KNAF300216-I

スマートデバイスエージェント(**デバイス ID**)にログ送信要求を行います。

## KNAF300217-E

スマートデバイスエージェントへの処理要求に失敗しました。
[要因]スマートデバイスエージェントとの通信でエラーが発生した。
[処理]処理を続行する。
[対処]スマートデバイスエージェントの起動状態および通信状況を確認する。

## KNAF300218-I

スマートデバイスエージェント(**デバイス ID**)にメッセージ通知を行います。

## 17.5　コマンドのメッセージ一覧

コマンドのメッセージについて説明します。

### KNAF600001-I

コマンドが正常終了しました。コマンド名：**コマンド名**

### KNAF600002-E

コマンドが異常終了しました。コマンド名：**コマンド名**，戻り値：**戻り値**
[要因]コマンドが異常終了した。
[処理]処理を中止する。
[対処]コマンドの戻り値を確認して対処を行った後、コマンドを再実行する。

# 付録

# 付録 A　フォルダー一覧

コンポーネントのインストール時に作成されるフォルダについて説明します。

## 付録 A.1　スマートデバイスマネージャーに作成されるフォルダ

JP1/ITDM2 - SDM（スマートデバイスマネージャー）インストール時にスマートデバイスマネージャーに作成されるフォルダについて説明します。

### JP1/ITDM2 - SDM（スマートデバイスマネージャー）インストール時に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のデータの格納フォルダです。<br>デフォルトパス：%Program Files%¥Hitachi¥jp1itdm2sdm |
| %WINDIR%¥Temp¥SDMINST | インストールで出力されるログファイルの格納フォルダです。 |

### インストール先フォルダの配下に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| log¥ | インストールで出力されるログファイルの格納フォルダです。 |
| mgr¥ | スマートデバイスマネージャーのルートフォルダです。 |
| mgr¥bin | 実行ファイルの格納フォルダです。 |
| mgr¥backup | デフォルトのバックアップ先フォルダです。 |
| mgr¥conf¥ | 環境定義ファイル格納フォルダです。 |
| mgr¥Database¥※ | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のデータの格納フォルダです。 |
| mgr¥db¥ | データベースのインストール先フォルダです。 |
| mgr¥log¥ | トレースログの格納フォルダです。 |
| mgr¥temp | temp フォルダです。 |
| mgr¥troubleshoot¥ | デフォルトのトラブルシュート情報格納フォルダです。 |
| mgr¥uC¥ | アプリケーションサーバのインストール先フォルダです。 |

注※　11-00 以降で新規インストールした場合に作成されるフォルダです。10-50 からバージョンアップした場合には作成されません。

### JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール時に作成されるフォルダ（インストール先フォルダ以外）

| フォルダ名 | 説明 |
|---|---|
| %Program Files%¥Hitachi¥HNTRLib2¥ | トレースライブラリのインストール先フォルダです。 |
| 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¥jp1itdm2sdm¥Database¥※ | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のデータの格納フォルダです。 |
| システムのプログラムメニュー¥JP1_IT Desktop Management2 - Smart Device Manager | プログラムフォルダです。 |

注※　10-50 からバージョンアップした場合に存在するフォルダです。11-00 以降で新規インストールした場合には作成されません。

## 付録 A.2　通信サーバに作成されるフォルダ

JP1/ITDM2 - SDM（通信サーバ）インストール時に通信サーバに作成されるフォルダについて説明します。

### JP1/ITDM2 - SDM（通信サーバ）インストール時に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ | JP1/ITDM2 - SDM（通信サーバ）のデータの格納フォルダです。<br>デフォルトパス：%Program Files%¥Hitachi¥jp1itdm2sdm |
| %WINDIR%¥Temp¥SDMINST | インストールで出力されるログファイルの格納フォルダです。 |

### インストール先フォルダの配下に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| log¥ | インストールで出力されるログファイルの格納フォルダです。 |
| cms¥ | 通信サーバのルートフォルダです。 |
| cms¥bin | 実行ファイルの格納フォルダです。 |
| cms¥conf¥ | 環境定義ファイル格納フォルダです。 |
| cms¥log¥ | トレースログの格納フォルダです。 |
| cms¥troubleshoot¥ | デフォルトのトラブルシュート情報格納フォルダです。 |
| cms¥uC¥ | アプリケーションサーバのインストール先フォルダです。 |
| cms¥uC¥httpsd¥htdocs¥download¥ | 配布するアプリケーションの格納フォルダです。 |

# 付録 A.3　メッセージングサーバに作成されるフォルダ

JP1/ITDM2 - SDM（メッセージングサーバ）インストール時にメッセージングサーバに作成されるフォルダについて説明します。

## JP1/ITDM2 - SDM（メッセージングサーバ）インストール時に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ | JP1/ITDM2 - SDM（メッセージングサーバ）のデータの格納フォルダです。<br>デフォルトパス：%Program Files%¥Hitachi¥jp1itdm2sdm |
| %WINDIR%¥Temp¥SDMINST | インストールで出力されるログファイルの格納フォルダです。 |

## インストール先フォルダの配下に作成されるフォルダ

| フォルダ名 | 説明 |
|---|---|
| log¥ | インストールで出力されるログファイルの格納フォルダです。 |
| mss¥ | メッセージングサーバのルートフォルダです。 |
| mss¥bin¥ | 実行ファイルの格納フォルダです。 |
| mss¥conf¥ | 環境定義ファイル格納フォルダです。 |
| mss¥log¥ | トレースログの格納フォルダです。 |
| mss¥troubleshoot¥ | デフォルトのトラブルシュート情報格納フォルダです。 |

# 付録 B　サービス、プロセス一覧

JP1/ITDM2 - SDM のサービスおよびプロセスについて説明します。

## 付録 B.1　サービス一覧

JP1/ITDM2 - SDM の各サービスのサービス名、対応するサービスプロセス名、サービスの説明、およびサービスが自動起動するかどうかについて、サーバごとに説明します。

### スマートデバイスマネージャー

| サービス名 | サービス表示名 | サービスプロセス名 | 説明 | サービスの自動起動 |
|---|---|---|---|---|
| JP1_ITDM2_SDM_MGRSVR | JP1/ITDM2 - Smart Device Manager Server Service | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥bin¥SdManagerServer.exe | スマートデバイスマネージャーのサービスです。 | ○ |
| HiRDBEmbeddedEdition_IS1 | JP1/ITDM2 - Smart Device Manager (DB Service) | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥db¥BIN¥pdservice.exe | スマートデバイスマネージャーのデータベースサービスです。 | ○ |
| JP1_ITDM2_SDM_WEBSVR | JP1/ITDM2 - Smart Device Manager Web Server | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥httpsd¥httpsd.exe | Web サーバのサービスです。 | ○ |

（凡例）

○：自動起動する

### 通信サーバ

| サービス名 | サービス表示名 | サービスプロセス名 | 説明 | サービスの自動起動 |
|---|---|---|---|---|
| JP1_ITDM2_SDM_COMSVR | JP1/ITDM2 - Smart Device Manager (Communication Server Service) | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥bin¥SdCommunicationServer.exe | 通信サーバのサービスです。 | ○ |
| JP1_ITDM2_SDM_WEBSVR | JP1/ITDM2 - Smart Device Manager Web Server | JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥httpsd.exe | Web サーバのサービスです。 | × |

（凡例）

○：自動起動する

×：手動起動

### メッセージングサーバ

| サービス名 | サービス表示名 | サービスプロセス名 | 説明 | サービスの自動起動 |
|---|---|---|---|---|
| JP1_ITDM2_SDM_MSGSVR | JP1/ITDM2 - Smart Device Manager (Messaging Server Service) | JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥bin¥SdMessagingServer.exe | メッセージングサーバのサービスです。 | ○ |

（凡例）

○：自動起動する

## 付録 B.2　プロセス一覧

JP1/ITDM2 - SDM の各プロセスの機能について、サーバごとに説明します。

### スマートデバイスマネージャー

| プロセス名 | 機能 | プロセスの常駐 |
|---|---|---|
| cjstartsv.exe | アプリケーションサーバのプロセスです。 | ○ |
| SdManagerServer.exe | サービスプロセスです。 | ○ |
| pdxxx.exe※ | データベースのプロセスです。 | ○ |
| httpsd.exe | Web サーバ機能のプロセスです。 | ○ |

（凡例）

○：常駐する。

注※　xxx は、3～8 文字の文字列です。

### 通信サーバ

| プロセス名 | 機能 | プロセスの常駐 |
|---|---|---|
| cjstartsv.exe | アプリケーションサーバのプロセスです。 | ○ |
| SdCommunicationServer.exe | サービスプロセスです。 | ○ |
| httpsd.exe | Web サーバ機能のプロセスです。 | ○ |

（凡例）

○：常駐する。

### メッセージングサーバ

| プロセス名 | 機能 | プロセスの常駐 |
|---|---|---|
| SdMessagingServer.exe | サービスプロセスです。 | ○ |

（凡例）

○：常駐する。

# 付録 C　ポート番号一覧

JP1/ITDM2 - SDM で使用するポート番号について、サーバごとに説明します。

### スマートデバイスマネージャー

| 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 |
|---|---|---|---|---|
| 26080 | ← | 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スマートデバイスマネージャーへの通信に使用されるポート番号です。 |
| 26055 | ← | JP1/IT Desktop Management 2 管理用サーバ | TCP | SSL 通信用 Hitachi Web Server の https ポート<br>JP1/IT Desktop Management 2 管理用サーバとの SSL 通信に使用されるポート番号です。 |
| 26056 | ← | スマートデバイスマネージャー [ephemeral] | TCP | sdmioutils コマンド実行時の内部通信用リクエスト受付ポート番号です。 |
| 26057 | ← | JP1/IT Desktop Management 2 管理用サーバ | TCP | JP1/IT Desktop Management 2 管理用サーバとの HTTP 通信に使用されるポート番号です。 |
| 26065 | ← | スマートデバイスマネージャー [ephemeral] | TCP | スマートデバイスマネージャー内 J2EE アプリケーションで使用する RMI レジストリのリクエスト受付ポート番号です。 |
| 26053 | ← | スマートデバイスマネージャー [ephemeral] | TCP | スマートデバイスマネージャー内 J2EE アプリケーションで使用するインプロセス HTTP サーバのリクエスト受付ポート番号です。 |
| 26052 | ← | スマートデバイスマネージャー [ephemeral] | TCP | スマートデバイスマネージャー内 J2EE アプリケーションで使用する管理用通信ポート番号です。 |
| 26066 | ← | スマートデバイスマネージャーまたは JP1/IT Desktop Management 2 管理用サーバ[ephemeral] | TCP | スマートデバイスマネージャー内に構築したデータベースとの通信用のポート番号です。 |
| 26067 | ← | 通信サーバ [26068-26077] | TCP | スマートデバイスマネージャー内に構築したデータベースとの通信用ポート番号です。 |

### 通信サーバ

| 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 |
|---|---|---|---|---|
| 26055 | ← | スマートデバイスマネージャー [ephemeral] | TCP | SSL 通信用の Hitachi Web Server の https ポート番号です。 |

| 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 |
|---|---|---|---|---|
| 26055 | ← | JP1/ITDM2 - SDM（スマートデバイス Android エージェント）[ephemeral] | TCP | SSL 通信用の Hitachi Web Server の https ポート番号です。 |
| | ← | JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）[ephemeral] | TCP | |
| 26065 | ← | 通信サーバ [ephemeral] | TCP | 通信サーバ内 J2EE アプリケーションで使用する RMI レジストリのリクエスト受付ポート番号です。 |
| 26053 | ← | 通信サーバ [ephemeral] | TCP | 通信サーバ内 J2EE アプリケーションで使用する、Web サーバ（リダイレクタ）からのリクエスト受付ポート番号です。 |
| 26052 | ← | 通信サーバ [ephemeral] | TCP | 通信サーバ内 J2EE アプリケーションで使用する管理用通信ポート番号です。 |
| 26068-26077 | ← | スマートデバイスマネージャー[26067] | TCP | スマートデバイスマネージャー内に構築したデータベースとの通信用のポート番号です。 |

### メッセージングサーバ

| 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 |
|---|---|---|---|---|
| 26078 | ← | 通信サーバ [ephemeral] | TCP | 通信サーバからメッセージングサーバへの要求送信用ポート番号です。 |
| 26079 | ← | JP1/ITDM2 - SDM（スマートデバイス Android エージェント）[ephemeral] | TCP | JP1/ITDM2 - SDM（スマートデバイス Android エージェント）との Comet 接続用ポート番号です。 |

# 付録 D　パラメーター一覧

各設定のパラメーターについて説明します。

## 付録 D.1　ユーザーアカウントの設定のパラメーター

［ユーザーアカウントの管理］画面のパラメーターについて説明します。

### ユーザーアカウントの設定のパラメーター

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| ユーザー ID | JP1/ITDM2 - SDM（スマートデバイスマネージャー）にログインするためのユーザーアカウントのユーザー ID を指定します。 | 8 文字以上、50 文字以下の半角文字列※1 | （空白） |
| パスワード | ユーザー ID に対するパスワードを指定します。 | 8 文字以上、20 文字以下の半角文字列※1※2 | （空白） |
| パスワード確認 | パスワードを再指定します。 | 8 文字以上、20 文字以下の半角文字列※1※2 | （空白） |
| ユーザー名 | ユーザーアカウントの名称を指定します。 | 20 文字以下の全角または半角文字列 | （空白） |
| メールアドレス | ユーザーアカウントの利用者のメールアドレスを指定します。 | 100 文字以下の E-mail 形式の文字列 | （空白） |
| 説明 | ユーザーアカウントの説明を指定します。 | 1000 文字以下の全角または半角文字列 | （空白） |
| 権限 | ユーザーアカウントに、システム管理権限を付与するかどうかを設定します。 | チェックあり<br>システム管理権限を付与します。<br>チェックなし<br>システム管理権限を付与しません。参照権限を付与します。 | チェックなし |
| アカウントロック | ユーザーアカウントがロックされた場合に、ユーザーアカウントのロックを解除できます。 | • 解除<br>• ロック中 | ロック中※3 |

注※1　使用できる文字は、ASCII 制御文字以外の ASCII 文字です。

注※2　パスワードを変更する場合は、現在のパスワードと異なる文字列を設定してください。

注※3　ロックされているユーザーアカウントの編集時にだけ表示されます。

# 付録 D.2　イベント通知の設定のパラメーター

［イベント通知の設定］画面のパラメーターについて説明します。

### 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。

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| 緊急 | 重大度が緊急の全種類のイベントについてメール通知したい場合はチェックします。 | チェックあり<br>イベントをメールで通知します。<br>チェックなし<br>イベントをメールで通知しません。 | チェックなし |
| 警戒 | 重大度が警戒の全種類のイベントについてメール通知したい場合はチェックします。 | | |
| 情報 | 重大度が情報の全種類のイベントについてメール通知したい場合はチェックします。 | | |
| セキュリティ | ポリシーの変更と割り当て、ポリシーの判定結果など、セキュリティ管理に関するイベントについてメール通知したい場合はチェックします。 | チェックあり<br>その種類のイベントをメールで通知します。<br>チェックなし<br>その種類のイベントをメールで通知しません。 | チェックなし |
| 不審操作 | 許可されていない電話番号への通話の検知、許可されていない WEB 閲覧の検知など、不審操作に関するイベントについてメール通知したい場合はチェックします。 | | |
| スマートデバイス | スマートデバイスの追加と削除など、スマートデバイスに関するイベントについてメール通知したい場合はチェックします。 | | |
| 配布 | 配布アプリケーションの追加・削除、アプリケーションの配布など、配布に関するイベントについてメール通知したい場合はチェックします。 | | |
| 設定 | ユーザーアカウントの管理、イベント通知の設定など設定に関するイベントについてメール通知したい場合はチェックします。 | | |
| エラー | 各機能で発生したエラーに関するイベントについてメール通知したい場合はチェックします。 | | |

### 通知の対象外とするイベントを選択してください。

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| イベント番号 | 通知の対象外としたいイベント番号をチェックします。 | チェックあり<br>イベントを通知の対象外とします。<br>チェックなし<br>イベントを通知の対象外としません。 | チェックなし |

### メールの通知先を選択してください。

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| ユーザー ID | イベントを通知したいユーザー ID をチェックします。メールアドレスが設定されていない場合は、[ユーザーアカウントの編集] ダイアログでメールアドレスを設定してください。 | チェックあり<br>ユーザーにメールで通知します。<br>チェックなし<br>ユーザーにメールで通知しません。 | チェックなし |

### 通知の間隔

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| 通知の間隔（分） | 何分ごとに通知するか設定します。 | 1～1440 | 30 |

### 関連項目

- 6.3 ほかの管理者のユーザーアカウントを編集する手順

## 付録 D.3　メールサーバ設定のパラメーター

[メールサーバ設定] 画面のパラメーターについて説明します。

### メールサーバの設定のパラメーター

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| ホスト名 | SMTP サーバのホスト名を入力します。 | SMTP サーバのホスト名 | (空白) |
| セキュリティ保護の接続 | SMTP サーバと通信する際に使用するセキュリティ保護を選択します。 | • 使用しない<br>• SSL<br>• TLS | 使用しない |
| ポート番号 | SMTP サーバのポート番号を指定します。 | 1～65535 | 25 |
| 送信元メールアドレス | 通知メールの送信元とするメールアドレスを指定します。 | E-mail 形式の文字列 | (空白) |
| SMTP 認証を使用する | SMTP サーバでユーザー認証機能（SMTP Authentication）を使用する場合はチェックします。 | チェックあり<br>SMTP 認証を使用します。<br>チェックなし<br>SMTP 認証を使用しません。 | チェックなし |
| ユーザー ID | ユーザー認証機能で使用するユーザー ID を入力します。 | ユーザー認証機能で使用するユーザー ID | (空白) |

| 項目 | 内容 | 設定できる値 | デフォルト |
|---|---|---|---|
| パスワード | ユーザー ID に対するパスワードを入力します。 | ユーザー ID に対するパスワード | (空白) |
| パスワード確認 | 確認のためパスワードを再入力します。 | 確認のためのパスワード | (空白) |

# 付録 E　インポート・エクスポートファイルの出力形式

インポートまたはエクスポートするファイルの出力形式を説明します。

## 付録 E.1　スマートデバイス一覧エクスポート・インポート CSV ファイルの形式

スマートデバイス一覧エクスポート・インポート CSV ファイルの形式を説明します。

### スマートデバイス一覧エクスポート・インポート CSV ファイルの形式

| 項目※1 | 内容 | 設定できる値 | 最大バイト数※2 | インポート対象 |
|---|---|---|---|---|
| 名称 | 資産管理番号などの名称です。 | － | 128 | ○ |
| OS | スマートデバイスから取得した OS 情報です。 | 0：iOS<br>1：Android | 1 | ○ |
| IMEI/MEID | スマートデバイスから取得した IMEI/MEID です。 | 15 桁 | 15 | × |
| 電話番号 | スマートデバイスから取得した該当するスマートデバイスの電話番号です。 | 最大 20 文字<br>数字だけ。「-」は含まない。 | 20 | × |
| 管理状態 | 本製品での管理状態です。 | 0：管理対象外<br>1：管理対象 | 1 | × |
| 適用されているセキュリティポリシー | スマートデバイスに適用されているセキュリティポリシー名です。 | － | 36 | ○※3 |
| 適用する Android ポリシー/iOS プロファイル※6 | スマートデバイスに適用する Android ポリシーまたは iOS プロファイルです。 | － | 809 | ○※3 |
| 所属 | 利用者の所属です。 | － | 128 | ○※4 |
| アカウント | 利用者のアカウントです。 | － | 128 | ○※4 |
| 利用者 | 利用者の名称です。 | － | 128 | ○※4 |
| 最終更新日時 | スマートデバイスの登録やスマートデバイス情報のインポートによる情報更新の最終更新日時です。 | yyyy/MM/dd hh:mm:ss※5 | 19 | × |

| 項目※1 | 内容 | 設定できる値 | 最大バイト数※2 | インポート対象 |
|---|---|---|---|---|
| 製造者名 | スマートデバイスから取得した製造者名です。 | － | 256 | × |
| 型番 | スマートデバイスから取得した型番です。 | － | 256 | × |
| プロトコルバージョン | 本製品のプロトコルバージョンです。 | － | 64 | × |
| 言語設定 | スマートデバイスから取得した言語設定です。 | 最大 20 文字 | 80 | × |
| 製品名称 | スマートデバイスから取得した製品名称です。 | 最大 10 文字<br>Android<br>iOS | 40 | × |
| モデル名 | スマートデバイスから取得したモデル名です。 | － | 256 | × |
| シリアル番号 | スマートデバイスから取得したシリアル番号です。 | － | 256 | × |
| OS バージョン | スマートデバイスから取得した OS バージョンです。 | － | 32 | × |
| OEM 名称 | スマートデバイスから取得した OEM 名称です。 | － | 64 | × |
| ファームウェアバージョン | スマートデバイスから取得したファームウェアバージョンです。 | － | 64 | × |
| ソフトウェアバージョン | スマートデバイスから取得したソフトウェアバージョンです。 | － | 64 | × |
| モバイルネットワークの国コード | スマートデバイスから取得したモバイルネットワークの国コードです。 | 最大 10 文字 | 40 | × |
| モバイルネットワークオペレータコード | スマートデバイスから取得したモバイルネットワークオペレータコードです。 | 最大 20 文字 | 80 | × |
| モバイルネットワークオペレータ名称 | スマートデバイスから取得したモバイルネットワークオペレータ名称です。 | 最大 20 文字 | 80 | × |

| 項目※1 | 内容 | 設定できる値 | 最大バイト数※2 | インポート対象 |
|---|---|---|---|---|
| モバイルネットワークタイプ | スマートデバイスから取得したモバイルネットワークタイプです。 | 最大 20 文字 | 80 | × |
| SIM カードの国コード | スマートデバイスから取得した SIM カードの国コードです。 | 最大 10 文字 | 40 | × |
| SIM カードオペレータコード | スマートデバイスから取得した SIM カードオペレータコードです。 | 最大 20 文字 | 80 | × |
| SIM カードオペレータ名称 | スマートデバイスから取得した SIM カードオペレータ名称です。 | − | 256 | × |
| ICCID | スマートデバイスから取得した ICCID です。 | 19 桁 | 19 | × |
| SIM 状態コード | スマートデバイスから取得した SIM 状態コードです。 | − | 64 | × |
| IMSI | スマートデバイスから取得した IMSI です。 | 15 桁 | 15 | × |
| ユーザー名称 | スマートデバイスから取得したユーザー名称です。 | 最大 20 文字 | 80 | × |
| ローミング情報 | スマートデバイスから取得したローミング情報です。 | 0：通常<br>1：ローミング中 | 1 | × |
| Android ID/Apple ID | スマートデバイスから取得した Android ID または Apple ID です。 | − | 256 | × |
| メールアドレス | スマートデバイスから取得したメールアドレスです。 | − | 256 | × |
| パスワード（設定の有無） | スマートデバイスから取得したパスワード（設定の有無）です。 | 0：無<br>1：有 | 1 | × |
| 内部ストレージ（残量/容量[B]） | スマートデバイスから取得した内部ストレージ情報です。 | − | 64 | × |
| SD カード（残量/容量[B]） | スマートデバイスから取得した SD カード情報です。 | − | 64 | × |

| 項目※1 | 内容 | 設定できる値 | 最大バイト数※2 | インポート対象 |
|---|---|---|---|---|
| RAM（残量/容量[B]） | スマートデバイスから取得した RAM 情報です。 | − | 64 | × |
| Android ポリシー/iOS プロファイル適用日時※6 | スマートデバイスに適用されている Android ポリシーまたは iOS プロファイルの適用日時です。 | yyyy/MM/dd hh:mm:ss※5 | 199 | × |
| Android ポリシー/iOS プロファイルバージョン※6 | スマートデバイスに適用する Android ポリシーまたは iOS プロファイルのバージョンです。 | 最大 5 文字 | 59 | × |
| 最新情報取得日時 | スマートデバイスからインベントリ情報を取得した最新の日時です。 | yyyy/MM/dd hh:mm:ss※5 | 19 | × |
| バッテリー残量 | スマートデバイスから取得したバッテリー残量です。 | − | 4 | × |
| 3G MAC アドレス | スマートデバイスから取得した 3G の MAC アドレスです。 | − | 64 | × |
| WiFi MAC アドレス | スマートデバイスから取得した WiFi の MAC アドレスです。 | − | 64 | × |
| Bluetooth MAC アドレス | スマートデバイスから取得した Bluetooth の MAC アドレスです。 | − | 64 | × |
| UDID | スマートデバイスから取得した UDID です。 | − | 40 | × |
| IP アドレス | スマートデバイスから取得した IP アドレスです。 | − | 64 | × |
| プロクシサーバ | スマートデバイスから取得したプロクシサーバです。 | − | 256 | × |
| GPS 情報 | スマートデバイスから取得した GPS 情報です。 | − | 128 | × |
| 前回、ロック時に変更したロック解除パスワード | 前回、ロック時に変更したロック解除パスワードです。 | − | 10 | × |
| GPS 電源状態 | スマートデバイスから取得した GPS 電源状態です。 | − | 3 | × |

| 項目※1 | 内容 | 設定できる値 | 最大バイト数※2 | インポート対象 |
|---|---|---|---|---|
| 最終ロック解除成功日時 | スマートデバイスから取得した最終ロック解除成功日時です。 | － | 19 | × |
| 最終ロック解除失敗日時 | スマートデバイスから取得した最終ロック解除失敗日時です。 | － | 19 | × |
| エージェントバージョン | この製品のエージェントバージョンです。 | － | 128 | × |

（凡例）

○：インポート対象

×：インポート対象外

－：任意の値

注※1　CSV ファイルには 1 行目に項目情報を含みません。

注※2　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※3　指定しなかった場合、管理対象外として登録します。

注※4　任意項目ですが、値を指定することを推奨します。

注※5　yyyy：年、MM：月、dd：日、hh：時、mm：分、ss：秒

注※6　値が複数存在する場合は「;」（セミコロン）で区切られます。

### 関連項目

- 15. sdmioutils exportdevice（スマートデバイス情報のエクスポート）
- 15. sdmioutils importdevice（スマートデバイス情報のインポート）

## 付録 E.2　イベント一覧エクスポート CSV ファイルの形式

イベント一覧エクスポート CSV ファイルの形式を説明します。

### イベント一覧エクスポート CSV ファイルの形式

| 項目※1 | 内容 | 出力形式 | 最大バイト数※2 |
|---|---|---|---|
| 重大度 | 重大度を出力します。 | 0：情報<br>1：警戒<br>2：緊急 | 1 |
| 登録日時 | 登録日時を出力します。 | yyyy/MM/dd hh:mm:ss※3 | 19 |
| 発生元 | イベント発生元を出力します。 | • スマートデバイス<br>• スマートデバイス名称<br>• セキュリティ<br>• 配布 | 128 |

| 項目※1 | 内容 | 出力形式 | 最大バイト数※2 |
|---|---|---|---|
| 発生元 | イベント発生元を出力します。 | • 設定 | 128 |
| 内容 | イベント内容を出力します。 | 1024 文字＋埋め込み文字数分の文字列が出力されます。 | 4096 文字＋埋め込み文字数×4 |
| イベント番号 | イベント番号を出力します。 | イベント出力の対象となるメッセージが出力されます。 | 10 |
| 種類 | イベントの種類を出力します。 | 0：セキュリティ<br>1：不審操作<br>2：スマートデバイス<br>3：配布<br>4：設定<br>5：エラー | 1 |
| 詳細 | イベント詳細を出力します。 | 1024 文字＋埋め込み文字数分の文字列が出力されます。 | 4096 文字＋埋め込み文字数×4 |
| 確認状態 | 確認状態を出力します。 | 0：未確認<br>1：確認済み | 1 |

注※1　CSV ファイルには 1 行目に項目情報を含みません。

注※2　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※3　yyyy：年、MM：月、dd：日、hh：時、mm：分、ss：秒

### 関連項目

- 10.2 イベント情報をエクスポートする手順
- 17.2 イベントとして出力される JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ

## 付録 E.3　セキュリティポリシー一覧エクスポート XML ファイルの形式

セキュリティポリシー一覧エクスポート XML ファイルの形式を説明します。

### セキュリティポリシー一覧エクスポート XML ファイルの例

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<policy name="一般用">
    <note>ノートへの記載</note>
    <phones number="電話番号">
        <note>顧客A</note>
    </phones>
    <apps name="社内アプリ">
        <version>1.0</version>
        <alerttype>0</alerttype>
        <installtype>1</installtype>
        <os>1</os>
        <note>社内情報アクセス用</note>
    </apps>
```

```
    <urls name="URL">
        <alerttype>0</alerttype>
        <note>検索サイト</note>
    </urls>
</policy>
```

**重要**

エクスポートしたファイルは編集しないでください。

### セキュリティポリシー一覧エクスポート XML ファイルの形式

| 要素名 | 内容 | 種類 | 値の出力形式 | 最大バイト数※ |
|---|---|---|---|---|
| policy | セキュリティポリシールート要素 | ! | × | 0 |
| name | セキュリティポリシー名 | @ | 最大 20 文字 | 80 |
| note | セキュリティポリシーの説明 | ! | 最大 1000 文字 | 4000 |
| phones | 電話番号リストのルート要素 | − | × | 0 |
| phone | 電話番号情報のルート要素 | + | × | 0 |
| number | 電話番号 | @ | • 最大 20 文字<br>• 「-」は含まない<br>• 数字だけ | 20 |
| note | 電話番号の説明 | ! | 最大 1000 文字 | 4000 |
| apps | アプリケーションリストのルート要素 | − | × | 0 |
| app | アプリケーション情報 | + | × | 0 |
| name | アプリケーション名 | @ | 最大 100 文字 | 400 |
| version | アプリケーションバージョン | ! | 最大 100 文字 | 400 |
| alerttype | 警告タイプ | ! | 0：許可<br>1：禁止 | 1 |
| installtype | インストールタイプ | ! | 0：インストール許可<br>1：インストール必須 | 1 |
| os | OS タイプ | ! | 0：iOS<br>1：Android | 1 |
| note | アプリケーションの説明 | ! | 最大 1000 文字 | 4000 |
| urls | Web サイトリストのルート要素 | − | × | 0 |
| url | Web サイト情報 | + | × | 0 |
| name | URL | @ | 最大 200 文字 | 800 |
| alerttype | 警告タイプ | ! | 0：許可<br>1：禁止 | 1 |

| 要素名 | 内容 | 種類 | 値の出力形式 | 最大バイト数※ |
|---|---|---|---|---|
| note | URL の説明 | ! | 最大 1000 文字 | 4000 |

(凡例)

×：値を出力しない

@：要素の属性値

！：必須

－：省略できる

＋：1 回以上の繰り返し

注※　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。

### 関連項目

- 15. sdmioutils exportpolicy（セキュリティポリシー設定情報のエクスポート）
- 15. sdmioutils importpolicy（セキュリティポリシー設定情報のインポート）

## 付録 E.4　スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式

スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式を説明します。

### スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの例

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sdmpolicy name="一般用">
    <os>0</os>
    <policy>AndroidポリシーまたはiOSプロファイル</policy>
    <note>説明</note>
</sdmpolicy>
```

**重要**

エクスポートしたファイルは編集しないでください。

### スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式

| 要素名 | 内容 | 種類 | 値の出力形式 | 最大バイト数※ |
|---|---|---|---|---|
| sdmpolicy | Android ポリシーまたは iOS プロファイルのルート要素 | ! | × | 0 |

| 要素名 | 内容 | 種類 | 値の出力形式 | 最大バイト数※ |
|---|---|---|---|---|
| name | Android ポリシー名または iOS プロファイル名 | @ | 最大 20 文字 | 80 |
| os | OS タイプ | ! | 0：iOS<br>1：Android | 1 |
| policy | Android ポリシーまたは iOS プロファイル | ! | <![CDATA[<br>Android ポリシーまたは iOS プロファイルの XML データ<br>]]> | 32000 |
| note | Android ポリシーまたは iOS プロファイルの説明 | ! | 最大 1000 文字 | 4000 |

（凡例）

×：値を出力しない

@：要素の属性値

！：必須

注※　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。

### 関連項目

- 15. sdmioutils exportsdpolicy（Android ポリシーまたは iOS プロファイルの情報のエクスポート）
- 15. sdmioutils importsdpolicy（Android ポリシーまたは iOS プロファイルの情報のインポート）

## 付録 E.5　配布アプリケーションエクスポート XML ファイルの形式

配布アプリケーションエクスポート XML ファイルの形式を説明します。

### 配布アプリケーションエクスポート XML ファイルの例

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<delivery name="サンプルアプリケーション">
    <os>OS種別</os>
    <identifier>バンドルID</identifier>
    <version>パッケージバージョン</version>
    <description>説明</description>
    <binary>配布アプリケーションパッケージ</binary>
    <installparam>installParam</installparam>
    <mime>パッケージ種別</mime>
    <pkg_no>パッケージNo</pkg_no>
    <pkg_id>パッケージID</pkg_id>
</delivery>
```

**重要**

エクスポートしたファイルは編集しないでください。

### 配布アプリケーションエクスポート XML ファイルの形式

| 要素名 | 内容 | 種類 | 値の出力形式 | 最大バイト数※1 |
|---|---|---|---|---|
| delivery | 配布アプリケーションのルート要素 | ！ | × | 0 |
| name | 配布アプリケーション名 | @ | 最大 100 文字 | 400 |
| os | OS 種別 | －※2 | 0：iOS<br>1：Android | 1 |
| identifier | バンドル ID | Android の場合<br>－<br>iOS の場合<br>！ | Android の場合<br>×<br>iOS の場合<br>最大 256 文字 | Android の場合<br>0<br>iOS の場合<br>1024 |
| version | パッケージバージョン | Android の場合<br>－<br>iOS の場合<br>！ | 最大 100 文字 | 400 |
| description | 説明 | ！ | 最大 1000 文字 | 4000 |
| binary | 配布アプリケーションパッケージ | ！ | バイナリ値 | パッケージサイズ |
| installparam | インストールパラメータ | － | Android の場合<br>最大 256 文字<br>iOS の場合<br>最大 1000 文字 | Android の場合<br>1024<br>iOS の場合<br>4000 |
| mime | パッケージ種別 | ！ | 最大 256 文字 | 1024 |
| pkg_no | パッケージ No. | ！ | UUID 値 | 36 |
| pkg_id | パッケージ ID | ！ | UUID 値 | 36 |

（凡例）

×：値を出力しない

@：要素の属性値

！：必須

－：省略できる

注※1　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　OS 種別が定義されていない配布アプリケーションエクスポート XML ファイルをインポートした場合、OS 種別は Android となります。

### 関連項目

- 15. sdmioutils exportdeliveryapp（アプリケーション配布情報のエクスポート）
- 15. sdmioutils importdeliveryapp（アプリケーション配布情報のインポート）

## 付録 E.6　配布許可定義ファイルの形式

配布許可定義ファイル（CSV 形式）の形式を説明します。

### 配布許可定義ファイルの例（インポート時に-mode all の場合またはエクスポートの場合）

```
OS種別,アプリケーション名,バージョン,配布許可対象種別,配布許可対象名
Android,app2,v1,0,device4
Android,app2,v1,0,device5
Android,app3,v1,0,device5
iOS,app1,v1,0,device1
iOS,app1,v1,0,device2
iOS,app1,v1,0,device3
```

### 配布許可定義ファイルの例（インポート時に-mode app の場合）

```
配布許可対象種別,配布許可対象名
0,device1
0,device2
0,device3
```

### 配布許可定義ファイルの例（インポート時に-mode device の場合）

```
アプリケーション名,バージョン
app1,v1
app2,v1
app3,v1
```

### 配布許可定義ファイルの形式

| 列 | 項目 | 内容 | インポート時の-mode | | | エクスポート時 |
|---|---|---|---|---|---|---|
| | | | all | app | device | |
| 1 | OS 種別 | OS 種別を指定します。<br>• iOS<br>• Android | ○ | × | × | ◎ |
| 2 | アプリケーション名 | アプリケーションの名称を指定します。 | ○ | × | ○ | ◎ |
| 3 | バージョン | アプリケーションのバージョンを指定します。 | ○ | × | ○ | ◎ |
| 4 | 配布許可対象種別 | 0 固定です。 | ○ | ○ | × | ◎ |

| 列 | 項目 | 内容 | インポート時の-mode | | | エクスポート時 |
|---|---|---|---|---|---|---|
| | | | all | app | device | |
| 5 | 配布許可対象名 | スマートデバイスの名称を指定します。 | ○ | ○ | × | ◎ |

(凡例)

○：必須です。

×：不要です。

◎：出力されます。

### 配布許可定義ファイルの記述規則

- 1 行目はタイトル行とし、2 行目以降にデータを記述します。
- 最終行には改行コードを入力してください。
- 文字コードは ISO-8859-1、UTF-8 または UTF-16 で記述してください。

### 関連項目

- 15. sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
- 15. sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）

## 付録 E.7　アプリケーション配布情報ファイルの形式

アプリケーション配布情報ファイル（CSV 形式）の形式を説明します。

### アプリケーション配布情報ファイルの例

```
操作,OS種別,配布アプリケーション,バージョン,スマートデバイス名
install,iOS,ApplicationA,1.0,Device1
install,iOS,ApplicationA,1.0,Device2
install,iOS,ApplicationA,1.0,Device3
install,iOS,ApplicationB,1.0,Device1
install,iOS,ApplicationB,1.0,Device2
```

### アプリケーション配布情報ファイルの形式

| 列 | 項目 | 設定できる値 |
|---|---|---|
| 1 列目 | 操作 | インストールまたは配布の種別を指定します。<br>• install<br>• distribute※ |
| 2 列目 | OS 種別 | スマートデバイスの OS 種別を指定します。<br>• iOS<br>• Android |

| 列 | 項目 | 設定できる値 |
|---|---|---|
| 3 列目 | 配布アプリケーション | 配布するアプリケーションの名称を指定します。 |
| 4 列目 | バージョン | 配布するアプリケーションのバージョンを指定します。 |
| 5 列目 | スマートデバイス名 | インストール対象のスマートデバイス名を指定します。 |
| 6 列目 | コメント | コメントを指定します。<br>省略する場合、5 列目のあとの「,」（カンマ）も省略できます。 |

注※　Android だけ指定できます。

### アプリケーション配布情報ファイルの記述規則

- 1 行目はタイトル行とし、2 行目以降にデータを記述します。
- 最終行には改行コードを入力してください。
- 文字コードは UTF-8（BOM 付き）で記述してください。

### 関連項目

- 15. sdmdistributeapp（アプリケーションのインストール指示）

## 付録 E.8　iOS プロファイル情報ファイルの形式

iOS プロファイル情報ファイル（CSV 形式）の形式を説明します。

### iOS プロファイル情報ファイルの例

```
操作,プロファイル名,名称,コメント
apply,ProfileA,Device1
apply,ProfileA,Device2
```

### iOS プロファイル情報ファイルの形式

| 列 | 項目 | 設定できる値 |
|---|---|---|
| 1 列目 | 操作 | iOS プロファイルの適用または適用解除を指定します。<br>apply：適用<br>remove：適用解除 |
| 2 列目 | プロファイル名 | 適用または適用解除対象の iOS プロファイルの名称を指定します。 |
| 3 列目 | 名称 | iOS プロファイルの適用または適用解除対象のスマートデバイス名を指定します。 |
| 4 列目 | コメント | コメントを指定します。<br>省略する場合、3 列目のあとの「,」（カンマ）も省略できます。 |

### iOS プロファイル情報ファイルの記述規則

- 1 行目はタイトル行とし、2 行目以降にデータを記述します。
- 最終行には改行コードを入力してください。
- 文字コードは UTF-8（BOM 付き）で記述してください。
- 1 つの iOS プロファイル情報ファイルには、操作「apply」と「remove」を混在させないでください。

### 関連項目

- 15. sdmapplyprofile（iOS プロファイルの適用または適用解除）

## 付録 E.9　デバイス情報ファイルの形式

デバイス情報ファイル（CSV 形式）の形式を説明します。

### デバイス情報ファイルの例

```
インベントリ種別,名称,コメント
All,Device1
All,Device2
All,Device3
```

### デバイス情報ファイルの形式

| 列 | 項目 | 設定できる値 |
|---|---|---|
| 1 列目 | インベントリ種別 | All 固定です。 |
| 2 列目 | 名称 | インベントリ取得対象のスマートデバイスの名称を指定します。 |
| 3 列目 | コメント | コメントを指定します。<br>省略する場合、2 列目のあとの「,」（カンマ）も省略できます。 |

### デバイス情報ファイルの記述規則

- 1 行目はタイトル行とし、2 行目以降にデータを記述します。
- 最終行には改行コードを入力してください。
- 文字コードは UTF-8 で記述してください。

### 関連項目

- 15. sdmgetinventory（インベントリ情報の取得）

## 付録 E.10　配布状況出力ファイルの形式

配布状況出力ファイル（CSV 形式）の形式を説明します。

### 配布状況出力ファイルの例（iOS の場合）

-version を指定した場合

```
Name,Status,Package name,Version
”Device1”,”0”,”PackageA”,”1.0”
”Device2”,”1”,”PackageA”,”1.0”
”Device3”,”4”,”PackageA”,”1.0”
”Device4”,”3”,”PackageA”,”1.0”
”Device5”,”3”,”PackageA”,”1.0”
”Device6”,”1”,”PackageA”,”1.0”
```

-version を省略した場合

```
Name,Status,Package name,Version
”Device1”,”0”,”PackageA”,”1.0”
”Device1”,”0”,”PackageA”,”1.5”
”Device1”,”1”,”PackageA”,”2.0”
”Device2”,”1”,”PackageA”,”1.0”
”Device2”,”1”,”PackageA”,”1.5”
”Device2”,”0”,”PackageA”,”2.0”
”Device3”,”4”,”PackageA”,”1.0”
”Device3”,”0”,”PackageA”,”1.5”
”Device3”,”0”,”PackageA”,”2.0”
```

### 配布状況出力ファイルの例（Android の場合）

-version を指定した場合

```
Name,Distribute Status,Last Distribute Control Status,Last Installation Control
Status,Package name,Version
”Device 1”,”0”,”0”,”9”,”Package A”,”1.0”
”Device 2”,”1”,”0”,”0”,”Package A”,”1.0”
”Device 3”,”1”,”0”,”2”,”Package A”,”1.0”
”Device 4”,”1”,”1”,”9”,”Package A”,”1.0”
”Device 5”,”0”,”3”,”9”,”Package A”,”1.0”
”Device 6”,”0”,”4”,”9”,”Package A”,”1.0”
```

-version を省略した場合

```
Name,Distribute Status,Last Distribute Control Status,Last Installation Control
Status,Package name,Version
”Device 1”,”0”,”0”,”9”,”Package A”,”1.0”
”Device 1”,”0”,”0”,”9”,”Package A”,”1.5”
”Device 1”,”1”,”0”,”0”,”Package A”,”2.0”
”Device 2”,”0”,”0”,”9”,”Package A”,”1.0”
”Device 2”,”1”,”3”,”9”,”Package A”,”1.5”
”Device 2”,”0”,”0”,”9”,”Package A”,”2.0”
”Device 3”,”0”,”0”,”9”,”Package A”,”1.0”
”Device 3”,”0”,”0”,”9”,”Package A”,”1.5”
”Device 3”,”1”,”0”,”2”,”Package A”,”2.0”
```

### 配布状況出力ファイルの形式（iOS の場合）

| 列 | 項目（ヘッダ名） | 出力される値 |
|---|---|---|
| 1 列目 | 名称（Name） | 資産管理番号などのスマートデバイスの名称 |
| 2 列目 | 配布状況（Status） | 0：未インストール<br>1：インストール済み<br>3：インストール要求済み<br>4：インストール要求失敗<br>5：インストール失敗<br>6：インストール中<br>13：アンインストール要求済み<br>14：アンインストール要求失敗<br>15：アンインストール失敗 |
| 3 列目 | パッケージ名（Package name） | アプリケーションのパッケージ名 |
| 4 列目 | バージョン（Version） | アプリケーションのバージョン |

### 配布状況出力ファイルの形式（Android の場合）

| 列 | 項目（ヘッダ名） | 出力される値 |
|---|---|---|
| 1 列目 | 名称（Name） | 資産管理番号などのスマートデバイスの名称 |
| 2 列目 | 配布状況（Distribute Status） | 0：未配布<br>1：配布済み |
| 3 列目 | 最終配布制御状態（Last Distribution Control Status） | 0：正常<br>1：削除失敗<br>2：削除処理中<br>3：配布処理中<br>4：配布失敗 |
| 4 列目 | 最終インストール制御状態（Last Installation Control Status） | 0：正常<br>1：アンインストール失敗<br>2：インストール失敗<br>9：未インストール |
| 5 列目 | パッケージ名（Package name） | アプリケーションのパッケージ名 |
| 6 列目 | バージョン（Version） | アプリケーションのバージョン |

### 配布状況出力ファイルの出力値の説明

- 文字コードは UTF-8 で出力されます。
- スマートデバイスの名称でソートして出力されます。コマンドの引数でバージョンを省略した場合は、第 1 ソートキー：名称、第 2 ソートキー：バージョンでソートされて出力されます。

- 管理対象のスマートデバイスだけが出力されます。

### 関連項目

- 15. sdmexportdistributestatus（アプリケーション配布状況の出力）

## 付録 E.11　インストールソフトウェア情報出力ファイルの形式

インストールソフトウェア情報出力ファイル（CSV 形式）の形式を説明します。

### インストールソフトウェア情報出力ファイルの例

```
Name,Application name,Version
”Device1”,”ApplicationA”,”1.0”
”Device1”,”ApplicationB”,”2.0”
”Device1”,”ApplicationC”,”3.0”
”Device2”,”ApplicationB”,”2.0”
”Device2”,”ApplicationD”,”1.5”
”Device3”,”ApplicationB”,”2.0”
```

### インストールソフトウェア情報出力ファイルの形式

| 列 | 項目 | 出力される値 |
|---|---|---|
| 1 列目 | 名称 | 資産管理番号などのスマートデバイスの名称 |
| 2 列目 | アプリケーション名 | アプリケーションの名称 |
| 3 列目 | バージョン | アプリケーションのバージョン |

### インストールソフトウェア情報出力ファイルの出力値の説明

- 文字コードは UTF-8 で出力されます。
- 第 1 ソートキー：名称、第 2 ソートキー：アプリケーション名、第 3 ソートキー：バージョンでソートして出力されます。
- 管理対象のスマートデバイスだけが出力されます。

### 関連項目

- 15. sdmexportinstallapp（インストールソフトウェア情報の出力）

# 付録 F　サポートに必要な情報の格納先または入手方法

ユーザー環境でsdmgetlogs コマンドを使用できない状況で、サポートに必要な情報を入手しなければならない場合の、情報の格納先または入手方法を説明します。情報の格納先または入手方法をユーザーに連絡してください。

### サポートに必要な情報の格納先または入手方法

| 情報 | 内容 | 格納先または入手方法 |
|---|---|---|
| スマートデバイスマネージャーの情報 | JP1/ITDM2 - SDM（スマートデバイスマネージャー）のログ | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥log |
| | JP1/ITDM2 - SDM（スマートデバイスマネージャー）の環境設定ファイル | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥conf |
| | JP1/ITDM2 - SDM（スマートデバイスマネージャー）の uC フォルダにあるファイル | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC |
| | JP1/ITDM2 - SDM（スマートデバイスマネージャー）の db フォルダにあるファイル | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥db |
| 通信サーバの情報 | JP1/ITDM2 - SDM（通信サーバ）のログ | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥log |
| | JP1/ITDM2 - SDM（通信サーバ）の環境設定ファイル | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥conf |
| | JP1/ITDM2 - SDM（通信サーバ）の uC フォルダにあるファイル | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC |
| メッセージングサーバの情報 | JP1/ITDM2 - SDM（メッセージングサーバ）のログ | 次のフォルダに格納されているファイル<br>JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥log |
| | JP1/ITDM2 - SDM（メッセージングサーバ）の環境設定ファイル | 次のファイル<br>JP1/ITDM2 - SDM（メッセージングサーバ）のインストール先フォルダ¥mss¥conf¥SdMessagingServer.ini |
| JP1/ITDM2 - SDM（スマートデバイス Android エージェント）の情報 | JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のログ | 該当スマートデバイスのログを収集後、次のフォルダに格納されているファイルを入手します。<br>JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥log¥agent¥名称_yyyyMMdd_hhmmss※.log |

| 情報 | 内容 | 格納先または入手方法 |
|---|---|---|
| JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）の情報 | JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）のログ | 該当スマートデバイスのログを収集後、次のフォルダに格納されているファイルを入手します。<br>JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥log¥agent¥名称_yyyyMMdd_hhmmss※.log |

注※　yyyy：年、MM：月、dd：日、hh：時、mm：分、ss：秒

**ヒント**

ユーザーの環境によっては、情報を入手できない場合もあります。その場合は、できる範囲で入手してください。

# 付録 G　SSL 通信用証明書の取得に使用するコマンド

SSL 通信用証明書の取得に使用するコマンドについて説明します。

コマンドは次のフォルダに格納されています。

JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール先フォルダ¥mgr¥uC¥httpsd¥sbin

JP1/ITDM2 - SDM（通信サーバ）のインストール先フォルダ¥cms¥uC¥httpsd¥sbin

## 付録 G.1　Web サーバの秘密鍵の作成（keygen）

Web サーバの秘密鍵を作成します。作成した Web サーバの秘密鍵のファイルは、SSLCertificateKeyFile ディレクティブに指定します。

### 形式

```
keygen -rand ファイル名［暗号種別］-out 鍵ファイル［-bits ビット長］
```

### 引数

-rand ファイル名

乱数生成に利用する任意のファイルを指定します。乱数生成用のファイルは、十分大きい適当なファイル（例：C:¥WINNT¥NOTEPAD.EXE）を指定してください。

暗号種別

秘密鍵を暗号化する場合、暗号種別を指定します。この引数を指定すると、秘密鍵作成時にパスワードの入力要求があります。パスワードは 64 文字以内です。

また、証明書発行要求（CSR）の作成時および Web サーバ起動時にパスワードの入力要求があります。なお、Web サーバ起動時のパスワードの入力は、sslpasswd コマンドでパスワードファイルを作成することで省略できます。使用できる暗号種別は次のとおりです。

- -des

  暗号種別として DES（Data Encryption Standard）が選択されます。

- -des3

  暗号種別としてトリプル DES が選択されます。Web サーバと Web ブラウザ間の通信での暗号種別とは関係ありません。

-out 鍵ファイル

Web サーバの秘密鍵を出力するファイルを指定します。

-bits ビット長

作成する Web サーバの秘密鍵のビット長を指定します。指定できるビット長は次のとおりです。

- 512

- 1024
- 2048
- 4096

この引数を省略した場合、「1024」が仮定されます。

### 使用例

Web サーバの秘密鍵 httpsdkey.pem を作成する場合の使用例を次に示します。

```
keygen -rand C:¥WINNT¥NOTEPAD.EXE -out httpsdkey.pem -bits 1024
```

### 関連項目

- 付録 G.2 証明書発行要求（CSR）の作成（certutil reqgen）
- 付録 G.6 パスワードファイルの作成（sslpasswd）

## 付録 G.2　証明書発行要求（CSR）の作成（certutil reqgen）

証明書発行要求（CSR）を作成します。ここで作成した CSR ファイルを認証局（CA）に提出して、署名済みの証明書を発行してもらいます。CSR は、PKCS#10 に準拠した形式で作成されます。

### 形式

```
certutil reqgen [-sign 署名アルゴリズム] -key 鍵ファイル -out CSRファイル
```

### 引数

-sign 署名アルゴリズム

CSR 作成時に使用する署名アルゴリズムを指定します。使用できる署名アルゴリズムは次のとおりです。

- MD5
  md5WithRSAEncryption を使用します。
- SHA1
  sha1WithRSAEncryption を使用します。
- SHA224
  sha224WithRSAEncryption を使用します。
- SHA256
  sha256WithRSAEncryption を使用します。
- SHA384
  sha384WithRSAEncryption を使用します。
- SHA512

sha512WithRSAEncryption を使用します。

この引数を省略した場合、「SHA1」が仮定されます。

-key 鍵ファイル

Web サーバの秘密鍵のファイルを指定します。keygen コマンドで作成した秘密鍵のファイルを指定してください。

-out CSR ファイル

作成した CSR を出力するファイルを指定します。

**使用例**

Web サーバの秘密鍵 httpsdkey.pem を使用して証明書発行要求（CSR）を作成する場合の使用例を次に示します。

```
certutil reqgen -sign SHA1 -key httpsdkey.pem -out httpsd.csr
```

Web サーバの秘密鍵作成時にパスワードを設定した場合は、パスワードの入力要求があります。また、設定する項目については証明書発行要求（CSR）を提出する認証局（CA）の指示に従ってください。

## 付録 G.3　証明書発行要求（CSR）の内容表示（certutil req）

証明書発行要求（CSR）の内容を表示します。

**形式**

```
certutil req -in CSRファイル -text
```

**引数**

-in CSR ファイル

表示する CSR ファイルを指定します。

**使用例**

証明書発行要求 httpsd.csr を表示する場合の使用例を次に示します。

```
certutil req -in httpsd.csr -text
```

## 付録 G.4　証明書の内容表示（certutil cert）

証明書ファイルの内容を表示します。"-----BEGIN CERTIFICATE-----"から、"-----END CERTIFICATE----"の証明書ファイルの内容を表示します。

### 形式

```
certutil cert -in 証明書ファイル -text
```

### 引数

-in 証明書ファイル

表示する証明書ファイルを指定します。

### 使用例

証明書 httpsd.pem を表示する場合の使用例を次に示します。

```
certutil cert -in httpsd.pem -text
```

## 付録 G.5　証明書の形式変換（certutil cert）

証明書の形式を変換します。必要に応じて使用します。

### 形式

```
certutil cert -inform 入力形式 -outform 出力形式 -in 入力ファイル -out 出力ファイル
```

### 引数

-inform 入力形式

変換前の証明書ファイルの入力形式を指定します。指定できる入力形式は次のとおりです。

- DER
- PEM

この引数を省略した場合、「PEM」が仮定されます。

-outform 出力形式

変換後の証明書ファイルの出力形式を指定します。指定できる出力形式は次のとおりです。

- DER
- PEM

この引数を省略した場合、「PEM」が仮定されます。

-in 入力ファイル

変換前の証明書ファイルを指定します。

-out 出力ファイル

変換後の証明書ファイルを指定します。

# 付録 G.6　パスワードファイルの作成（sslpasswd）

Web サーバ起動時のパスワードの入力を省略する場合は、パスワードファイルを作成します。

パスワードによって保護されているサーバ秘密鍵を使用する場合、パスワードをあらかじめファイルに格納しておき、ディレクティブを設定することで、サーバ起動時のパスワード入力を省略できます。その流れを次に示します。パスワードによって保護されているサーバ秘密鍵を使用する場合には、この作業は必須です。

1. keygen コマンドによって、パスワード付きのサーバ秘密鍵を作成する
2. sslpasswd コマンドによって、パスワードファイルを作成する
3. 作成したパスワードファイルを指定した SSLCertificateKeyPassword ディレクティブを、サーバ秘密鍵ファイルを指定した SSLCertificateKeyFile ディレクティブとともに httpsd.conf に設定する
4. サーバを起動または再起動する

> **重要**
>
> パスワードファイルの内容の漏えいには注意する必要があります。サーバ秘密鍵の格納ディレクトリに加え、パスワードファイルの格納ディレクトリでも、他ユーザーからのアクセスを禁止するようにディレクトリパーミッションやファイルパーミッションの設定をしてください。

### 形式

```
sslpasswd サーバ秘密鍵ファイル名 パスワードファイル名
```

### 引数

#### サーバ秘密鍵ファイル名

パスワードによって保護されたサーバ秘密鍵を指定します。keygen コマンドで作成した秘密鍵のファイルを指定してください。

#### パスワードファイル名

パスワードファイルを出力するファイル名を指定します。

> **重要**
>
> パスワードファイル名として、既存のファイル名は指定できません。

### 使用例

パスワードファイル keypasswd を作成する場合の使用例を次に示します。

```
sslpasswd httpsdkey.pem .keypasswd
```

**関連項目**

- 付録 G.1 Web サーバの秘密鍵の作成（keygen）

# 付録 H　インベントリ情報一覧

JP1/ITDM2 - SDM で取得できるインベントリ情報について説明します。

### インベントリ情報一覧

| 分類 | 項目 | 説明 | iOS | Android |
|---|---|---|---|---|
| スマートデバイス一覧 | 重大度 | 該当するスマートデバイスのイベントのうち、最も高い重大度です。 | ○ | ○ |
| | 名称 | 資産管理番号などの名称です。 | ○ | ○ |
| | IMEI/MEID | スマートデバイスから取得した IMEI/MEID です。 | ○ | ○ |
| | ICCID | スマートデバイスから取得した ICCID です。 | ○ | ○ |
| | 電話番号 | スマートデバイスから取得した該当するスマートデバイスの電話番号です。 | ○ | ○ |
| | 所属 | 利用者の所属です。 | ○ | ○ |
| | 利用者名 | 利用者の名称です。 | ○ | ○ |
| | 最終更新日時 | スマートデバイスの登録やスマートデバイス情報のインポートによる情報更新の最終更新日時です。 | ○ | ○ |
| ［イベント］タブ | 確認状態 | イベントの確認状態です。 | ○ | ○ |
| | 重大度 | イベントの重大度です。 | ○ | ○ |
| | イベント番号 | イベント番号です。 | ○ | ○ |
| | 内容 | イベントの内容です。 | ○ | ○ |
| | 登録日時 | イベントの登録日時です。 | ○ | ○ |
| | 種類 | イベントの種類です。 | ○ | ○ |
| ［通話履歴］タブ | 確認状態 | 通話履歴の確認状態です。 | × | ○ |
| | 重大度 | 通話履歴の重大度です。 | × | ○ |
| | 相手電話番号 | スマートデバイスから取得した通話相手の電話番号です。 | × | ○ |
| | 区分 | スマートデバイスから取得した通話の区分（発信、着信、不在着信、通知不可能、非通知）です。 | × | ○ |
| | 通話開始時間 | スマートデバイスから取得した通話開始時間です。 | × | ○ |

| 分類 | 項目 | 説明 | iOS | Android |
|---|---|---|---|---|
| ［通話履歴］タブ | 通話時間 | スマートデバイスから取得した通話時間です。 | × | ○ |
| ［Web 閲覧履歴］タブ | 確認状態 | Web 閲覧履歴の確認状態です。 | × | ○ |
| | 重大度 | Web 閲覧履歴の重大度です。 | × | ○ |
| | URL | スマートデバイスから取得した Web 閲覧した URL です。 | × | ○ |
| | 閲覧日時 | スマートデバイスから取得した Web 閲覧した日時です。 | × | ○ |
| ［ソフトウェア］タブ | 確認状態 | ソフトウェアの確認状態です。 | ○ | ○ |
| | 重大度 | ソフトウェアの重大度です。 | ○ | ○ |
| | アプリケーション名 | スマートデバイスにインストールされているアプリケーション名です。 | ○ | ○ |
| | バージョン | アプリケーションのバージョンです。 | ○ | ○ |
| | 製造元 | アプリケーションの製造元です。 | ○ | ○ |
| ［ハードウェア］タブ | IMEI/MEID | スマートデバイスから取得した IMEI/MEID です。 | ○ | ○ |
| | ICCID | スマートデバイスから取得した ICCID です。 | ○ | ○ |
| | シリアル番号 | スマートデバイスから取得したシリアル番号です。 | ○ | ○ |
| | 型番 | スマートデバイスから取得した型番です。 | ○ | ○ |
| | モデル名 | スマートデバイスから取得したモデル名です。 | ○ | ○ |
| | 製造者名 | スマートデバイスから取得した製造者名です。 | ○ | ○ |
| | バッテリー残量 | スマートデバイスから取得したバッテリー残量です。 | ○ | ○ |
| | 内部ストレージ（残量/容量[B]） | スマートデバイスから取得した内部ストレージ情報です。 | ○ | ○ |
| | SD カード（残量/容量[B]） | スマートデバイスから取得した SD カード情報です。 | × | ○ |
| | RAM（残量/容量[B]） | スマートデバイスから取得した RAM 情報です。 | × | ○ |

| 分類 | 項目 | 説明 | iOS | Android |
|---|---|---|---|---|
| ［ハードウェア］タブ | 3G MAC アドレス | スマートデバイスから取得した 3G の MAC アドレスです。 | × | ○ |
| | WiFi MAC アドレス | スマートデバイスから取得した WiFi の MAC アドレスです。 | ○ | ○ |
| | Bluetooth MAC アドレス | スマートデバイスから取得した Bluetooth の MAC アドレスです。 | ○ | ○ |
| | UDID | スマートデバイスから取得した UDID です。 | ○ | × |
| ［起動中アプリケーション］タブ | アプリケーション名 | スマートデバイスから取得した起動中のアプリケーション名です。 | × | ○ |
| | バージョン | アプリケーションのバージョンです。 | × | ○ |
| | 製造元 | アプリケーションの製造元です。 | × | ○ |
| ［動作中サービス］タブ | サービス名 | スマートデバイスから取得した動作中サービスのサービス名です。 | × | ○ |
| | バージョン | サービスのバージョンです。 | × | ○ |
| | 製造元 | サービスの製造元です。 | × | ○ |
| ［システム情報］タブ | OS | スマートデバイスから取得した OS 情報です。 | ○ | ○ |
| | OS バージョン | スマートデバイスから取得した OS バージョンです。 | ○ | ○ |
| | 電話番号 | スマートデバイスから取得した電話番号です。 | ○ | ○ |
| | モバイルネットワーク | スマートデバイスから取得したモバイルネットワーク情報です。 | ○ | ○ |
| | SIM カード | スマートデバイスから取得した SIM カード情報です。 | ○ | ○ |
| | ローミング情報 | スマートデバイスから取得したローミング情報です。 | ○ | ○ |
| | Android ID/ Apple ID | スマートデバイスから取得した Android ID または Apple ID です。 | × | ○ |
| | メールアドレス | スマートデバイスから取得したメールアドレスです。 | ○ | ○ |
| | IP アドレス | スマートデバイスから取得した IP アドレスです。 | ○※ | ○ |

| 分類 | 項目 | 説明 | iOS | Android |
|---|---|---|---|---|
| ［システム情報］タブ | プロクシサーバ | スマートデバイスから取得したプロクシサーバです。 | ○ | ○ |
| | GPS 情報 | スマートデバイスから取得した GPS 情報です。 | × | ○ |
| | 前回、ロック時に変更したロック解除パスワード | 前回、ロック時に変更したロック解除パスワードです。 | × | ○ |
| | 所属 | 利用者の所属です。 | ○ | ○ |
| | アカウント | 利用者のアカウントです。 | ○ | ○ |
| | 利用者 | 利用者の名称です。 | ○ | ○ |
| ［セキュリティ］タブ | 適用されているセキュリティポリシー | スマートデバイスに適用されているセキュリティポリシー名です。 | ○ | ○ |
| | 適用する Android ポリシー/iOS プロファイル | スマートデバイスに適用する Android ポリシーまたは iOS プロファイルです。 | ○ | ○ |
| | Android ポリシー/iOS プロファイル適用日時 | スマートデバイスに適用されている Android ポリシーまたは iOS プロファイルの適用日時です。 | ○ | ○ |
| | Android ポリシー/iOS プロファイルバージョン | スマートデバイスに適用する Android ポリシーまたは iOS プロファイルのバージョンです。 | ○ | ○ |
| | GPS 電源状態 | スマートデバイスから取得した GPS 電源状態です。 | ○※ | ○ |
| | 最終ロック解除成功日時 | スマートデバイスから取得した最終ロック解除成功日時です。 | × | ○ |
| | 最終ロック解除失敗日時 | スマートデバイスから取得した最終ロック解除失敗日時です。 | × | ○ |
| | エージェント Ver | この製品のエージェントバージョンです。 | ○ | ○ |
| ［Bluetooth 接続情報］タブ | 確認状態 | Bluetooth 接続情報の確認状態です。 | × | ○ |
| | 重大度 | Bluetooth 接続情報の重大度です。 | × | ○ |
| | 接続名称 | スマートデバイスから取得した Bluetooth 接続名称です。 | × | ○ |

| 分類 | 項目 | 説明 | iOS | Android |
|---|---|---|---|---|
| ［Bluetooth 接続情報］タブ | 接続アドレス | スマートデバイスから取得した Bluetooth 接続アドレスです。 | × | ○ |

（凡例）

○：取得できます。

×：取得できません。

注※　スマートデバイスで［インベントリ送信］をタップしたときだけ、インベントリ情報を取得できます。

# 付録 I　各バージョンの変更内容

各バージョンでの変更点を次に示します。

## 付録 I.1　11-10 の変更内容

11-10 での変更点を次に示します。

- 利用者の操作でアプリケーションをインストールできる Pull 配布機能を追加した。
- 大容量なアプリケーションを配布できる標準配布機能を追加した。
- 次のコマンドを追加した。
  - sdmioutils exportdeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報のエクスポート）
  - sdmioutils importdeliverypermit（利用者の操作でインストールできるアプリケーションの設定）
  - sdmioutils deletedeliverypermit（利用者の操作でインストールできるアプリケーションの設定情報の削除）
  - sdmdistributeapp（アプリケーションのインストール指示）
  - sdmapplyprofile（iOS プロファイルの適用または適用解除）
  - sdmgetinvenroty（インベントリ情報の取得）
  - sdmexportdistributestatus（アプリケーション配布状況の出力）
  - sdmexportinstallapp（全端末のインストールソフトウェア情報の出力）
- Windows Server 2016 をサポート対象とした。

## 付録 I.2　11-00 の変更内容

11-00 での変更点を次に示します。

- iOS 端末に、iOS アプリケーションを配布できるようにした。
- iOS 端末の定期インベントリ収集時刻を指定する機能を追加した。また、インベントリ収集の実行タイミングのデフォルトを変更した。
- スマートデバイス一覧のエクスポートでエクスポートできる項目を追加した。
- ［管理対象のスマートデバイス一覧］画面の［イベント］タブでイベント詳細を確認できるようにした。
- iOS 端末に対する要求の送信が滞留している場合に、定期的に要求を再送する機能を追加した。
- 通信サーバ環境設定ファイルの次のプロパティの初期値を 1440 分に変更した。
  - ios.request.getinventory.timeout.time

    - ios.request.wipe.timeout.time
    - ios.request.lock.timeout.time
    - ios.request.clearpasscode.timeout.time
    - ios.request.unmanage.timeout.time
    - ios.request.applyprofile.timeout.time
    - ios.request.removeprofile.timeout.time
- JP1/IT Desktop Management 2 の MDM システム連携機能で、次の項目を収集できるようにした。
    - 型番（Android）
    - 製造者名（iOS）
    - シリアルナンバー（Android）
    - パスコード設定状況（Android）
- iOS プロファイル情報の編集機能を追加した。
- 定期的なインベントリ収集およびバッテリー情報の取得を抑止する機能を追加した。
- 構成プロファイル作成ツールをサポートした。
- セキュリティポリシーに登録したアプリケーションを任意のバージョンで判定できるようにした。
- iOS 端末に対する要求のタイムアウト機能を追加した。
- iOS プロファイルの適用を解除できるようにした。
- 複数の iOS プロファイル情報を管理できるようにした。
- iOS 端末がロック中に iOS プロファイル適用を実行した場合も、即時失敗としないで、最大 24 時間はリトライするようにした。
- Windows Server 2008（Windows Server 2008 R2 を除く）をサポート対象外とした。

# 付録 J　このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

## 付録 J.1　関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- JP1 Version 11 資産・配布管理 基本ガイド（3021-3-B51）
- JP1 Version 11 JP1/IT Desktop Management 2 導入・設計ガイド（3021-3-B52）
- JP1 Version 11 JP1/IT Desktop Management 2 構築ガイド（3021-3-B53）
- JP1 Version 11 JP1/IT Desktop Management 2 運用ガイド（3021-3-B54）
- JP1 Version 11 JP1/IT Desktop Management 2 配布機能 運用ガイド（3021-3-B55）
- JP1 Version 11 JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド（3021-3-B56）
- JP1 Version 11 JP1/IT Desktop Management 2 - Asset Console アクセス定義ファイル作成ガイド（3021-3-B57）
- JP1 Version 11 JP1/IT Desktop Management 2 メッセージ（3021-3-B58）
- JP1 Version 11 JP1/IT Desktop Management 2 - Agent (UNIX(R)用)（3021-3-B62）

## 付録 J.2　このマニュアルで使用する書式

このマニュアルで使用する書式を次の表に示します。

| 書式 | 説明 |
|---|---|
| **文字列** | 可変の値を示します。<br>（例）日付は yyyyMMdd の形式で指定します。 |
| [ ] － [ ] | メニューを連続して選択することを示します。<br>（例）［ファイル］メニュー－［新規作成］を選択します。<br>上記の例では、［ファイル］メニュー内の［新規作成］を選択することを示します。 |

## 付録 J.3　コマンドの文法に使用する書式

コマンド、およびパラメーターの説明で使用する書式を次の表に示します。

| 書式 | 説明 |
|---|---|
| **文字列** | 可変の値を示します。 |

| 書式 | 説明 |
|---|---|
| \|<br>（ストローク） | 複数の項目に対して項目間の区切りを示し、「または」の意味を示します。<br>**(例)**<br>A\|B\|C は、「A、B、または C」を示します。 |
| { }<br>（波括弧） | この記号で囲まれている複数の項目の中から、1 組の項目を必ず選択します。項目と項目の区切りは「\|」で示します。<br>**(例)**<br>{A\|B\|C}は、「A、B、または C のどれかを必ず指定する」ことを示します。 |
| [ ]<br>（角括弧） | この記号で囲まれている項目は任意に指定できます（省略もできます）。<br>**(例)**<br>[A] は「何も指定しない」か「A を指定する」ことを示します。<br>[B\|C] は「何も指定しない」か「B または C を指定する」ことを示します。 |

## 付録 J.4　製品名の表記

このマニュアルでの Windows のメニュー名の表記、製品名の表記について説明します。

このマニュアルに記載している Windows のメニュー名の表記は、Windows Server 2008 を前提としています。

Windows Server 2012 の場合は［スタート］メニューが表示されないため、画面左下から表示できる［スタート］画面からメニューを選択してください。

このマニュアルでは、製品名を次のように表記しています。

| このマニュアルでの表記 | | | 正式名称 |
|---|---|---|---|
| Firefox | | | Firefox(R) |
| JP1/ITDM2 - SDM | JP1/ITDM2 - SDM（スマートデバイスエージェント） | JP1/ITDM2 - SDM（スマートデバイス Android エージェント） | JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイス Android エージェント） |
| | | JP1/ITDM2 - SDM（スマートデバイス iOS エージェント） | JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイス iOS エージェント） |
| | JP1/ITDM2 - SDM（スマートデバイスマネージャー） | | JP1/IT Desktop Management 2 - Smart Device Manager（スマートデバイスマネージャー） |
| | JP1/ITDM2 - SDM（通信サーバ） | | JP1/IT Desktop Management 2 - Smart Device Manager（通信サーバ） |
| | JP1/ITDM2 - SDM（メッセージングサーバ） | | JP1/IT Desktop Management 2 - Smart Device Manager（メッセージングサーバ） |

# 付録 J.5　英略語

このマニュアルで使用する英略語を次に示します。

| 英略語 | 英字での表記 |
|---|---|
| APNs | Apple Push Notification Service |
| CD | Compact Disc |
| CPU | Central Processing Unit |
| CSV | Comma Separated Values |
| DB | Database |
| DMZ | DeMilitarized Zone |
| DVD | Digital Versatile Disk |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| ICCID | Integrated Circuit Card ID |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| ID | IDentification |
| IP | Internet Protocol |
| IT | Information Technology |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MDM | Mobile Device Management |
| OEM | Original Equipment Manufacturer |
| OMA-DM | Open Mobile Alliance Device Management |
| OS | Operating System |
| PC | Personal Computer |
| RAM | Random Access Memory |
| SD | Secure Digital |
| SIM | Subscriber Identity Module |
| SSL | Secure Socket Layer |
| Subject DN | Subject Distinguished Name |
| TCP | Transmission Control Protocol |

| 英略語 | 英字での表記 |
|---|---|
| TLS | Transport Layer Security |
| UAC | User Account Control |
| UDID | Unique Device IDentifier |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| UUID | Universally Unique IDentifier |
| VPN | Virtual Private Network |
| WWW | World Wide Web |
| XML | Extensible Markup Language |

## 付録 J.6　KB（キロバイト）などの単位表記

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）、1PB（ペタバイト）はそれぞれ 1,024 バイト、$1{,}024^2$ バイト、$1{,}024^3$ バイト、$1{,}024^4$ バイト、$1{,}024^5$ バイトです。

## 付録 J.7　オンラインマニュアルについて

JP1/ITDM2 - SDM では、Web ブラウザで参照できる HTML マニュアルを提供しています。HTML マニュアルの内容は、このマニュアルと同じです。

JP1/ITDM2 - SDM の操作画面の［ヘルプ］－［IT Desktop Management2 - Smart Device Manager のヘルプ］から起動できます。

# 付録 K　用語解説

## (英字)

### Android ポリシー

JP1/ITDM2 - SDM で Android 端末の機能や利用ルールを一括設定するためのポリシーです。スマートデバイスマネージャーで設定し、管理対象のスマートデバイスに適用します。

### APNs

Apple 社が提供する Apple Push Notification Service の略称です。

### Comet

Web アプリケーションを構築する際に利用される技術の名称で、サーバがクライアントからのリクエストに対しすぐに応答しないで保留状態にしておき、サーバ上でイベントが発生したタイミングでレスポンスを返すことができる技術のことです。

### Comet 接続

JP1/ITDM2 - SDM では Android 端末への要求実行を実現する手段として Comet の技術を使用しています。Android 端末と JP1/ITDM2 - SDM との Comet の技術を用いた HTTP 接続を指します。

### iOS プロファイル

JP1/ITDM2 - SDM で iOS 端末の機能や利用ルールを一括設定するためのポリシーです。スマートデバイスマネージャーで設定し、管理対象のスマートデバイスに適用します。事前に iPhone 構成ユーティリティで構成プロファイルとして作成し、JP1/ITDM2 - SDM で iOS プロファイルとして使用します。

### iPhone 構成ユーティリティ

Apple 社が提供する構成プロファイルの作成ツールです。構成プロファイルの作成のほかに、構成プロファイルをスマートデバイスにインストールするときにも使用します。

### JP1/IT Desktop Management 2

機器管理、セキュリティ管理、資産管理の観点から、IT 資産を管理するシステムです。

### JP1/ITDM2 - SDM（スマートデバイス Android エージェント）

JP1/ITDM2 - SDM の、Android 端末に対するエージェント機能を提供するプログラムです。

### JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）

JP1/ITDM2 - SDM の、iOS 端末に対するエージェント機能を提供するプログラムです。

### JP1/ITDM2 - SDM（スマートデバイスエージェント）

JP1/ITDM2 - SDM（スマートデバイス Android エージェント）と JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）の総称です。

### JP1/ITDM2 - SDM（スマートデバイスマネージャー）

JP1/ITDM2 - SDM のサーバ機能を提供するプログラムです。

### JP1/ITDM2 - SDM（通信サーバ）

JP1/ITDM2 - SDM の通信サーバ機能を提供するプログラムです。

### JP1/ITDM2 - SDM（メッセージングサーバ）

Android 端末との Comet 機能を提供するプログラムです。

### OMA-DM

Open Mobile Alliance (OMA) Device Management (DM)の略称です。モバイル関連のアプリケーションの標準化を進める Open Mobile Alliance が策定したデバイス管理プロトコルのことです。OMA-DM では、プロビジョニング、デバイスの設定、ソフトウェアのアップグレードなどの機能を提供します。

### OMA-DM Client

Android 端末側に配置する OMA-DM のクライアントプログラムです。

## （カ行）

### 管理者のコンピュータ

JP1/ITDM2 - SDM の管理者が、JP1/ITDM2 - SDM にログインするためのコンピュータです。

### 構成プロファイル

デバイス・セキュリティポリシー、VPN 構成情報、Wi-Fi 設定、APN 設定、Exchange アカウント設定、メール設定、iPhone や iPad からのエンタープライズシステムの操作を許可する証明書を含む、XML ファイルです。Apple 社が提供する iPhone 構成ユーティリティで作成できます。

## （サ行）

### 参照権限

JP1/ITDM2 - SDM のユーザーアカウントを作成すると設定される権限です。設定画面以外の画面を参照できます。各画面での情報追加、設定変更などはできません。

### システム管理権限

JP1/ITDM2 - SDM のユーザーアカウントに設定できる権限の一つです。この権限をユーザーアカウントに設定することで、JP1/ITDM2 - SDM を管理する機能全般を使用できます。

### 重大度

管理者による JP1/ITDM2 - SDM 操作時のイベントや、セキュリティポリシーの検証結果を表します。「緊急」、「警戒」、「情報」の 3 種類です。

### 初期化

スマートデバイスを遠隔操作して、工場出荷状態に初期化（ワイプ）します。スマートデバイスの紛失・盗難時に、第三者からの不正使用を防止するなどの目的で使用します。

### スマートデバイス

携帯式の小型端末機です。スマートフォン、タブレット PC などが該当します。

### スマートデバイスマネージャー

JP1/ITDM2 - SDM（スマートデバイスマネージャー）がインストールされたコンピュータです。

### セキュリティのルール

スマートデバイスを管理するための、次の 3 つのルールの総称です。

- セキュリティポリシー
- Android ポリシー
- iOS プロファイル

### セキュリティポリシー

JP1/ITDM2 - SDM で、スマートデバイスの利用状況を監視するためのポリシーです。利用を監視する電話番号、Web サイトおよびアプリケーションを、スマートデバイスの危険レベルを判定するための条件として設定できます。スマートデバイスマネージャーで設定して、管理対象のスマートデバイスに適用します。

## （タ行）

### 通信サーバ

JP1/ITDM2 - SDM（通信サーバ）がインストールされたコンピュータです。

## （ハ行）

### パスコード

iOS 端末でロックを解除するためのパスワードです。

### プロビジョニング

JP1/ITDM2 - SDM が管理するスマートデバイス上で稼働する JP1/ITDM2 - SDM（スマートデバイスエージェント）に対して、接続先 URL やインベントリ取得間隔などの設定を自動で変更する機能のことです。

## （マ行）

### メッセージングサーバ

JP1/ITDM2 - SDM（メッセージングサーバ）がインストールされたコンピュータです。

### メニューエリア

操作画面の左側に表示されるエリアです。選択した画面に応じてメニューが表示されます。各メニューの項目を選択すると、操作画面の右側のインフォメーションエリアに、対応する情報が表示されます。

## （ラ行）

### ロック

スマートデバイスを遠隔操作して、操作できない状態にします。スマートデバイスの紛失・盗難時に、第三者からの不正使用を防止するなどの目的で使用します。

# 索引


## 記号

［iOS プロファイル情報の編集］ダイアログ　254

## A

［Android アプリケーション］画面　276
［Android アプリケーション］画面で表示されるタブ　277
Android アプリケーションの管理　54
［Android アプリケーションの参照］ダイアログ　282
［Android アプリケーションの追加］ダイアログ　281
［Android アプリケーションの編集］ダイアログ　282
Android 端末　23
Android 端末で再度管理対象にする手順　171
Android 端末の管理　106
Android 端末のパスワードの変更手順　178
Android 端末のパスワードを変更する流れ　130
Android 端末のパスワードを忘れた場合の対処　130
Android ポリシー　44
［Android ポリシー一覧］画面　248
Android ポリシーに設定できる項目　46
Android ポリシーの管理　46
Android ポリシーの削除手順　155
［Android ポリシーの参照］ダイアログ　251
［Android ポリシーの追加］ダイアログ　249
Android ポリシーの追加手順　154
Android ポリシーの適用手順　156
［Android ポリシーの編集］ダイアログ　250
Android ポリシーの編集手順　154
Android ポリシーの利用　154
Android ポリシーまたは iOS プロファイルの情報のインポート〔sdmioutils importsdpolicy コマンド〕　319
Android ポリシーまたは iOS プロファイルの情報のエクスポート〔sdmioutils exportsdpolicy コマンド〕　316
［Android ポリシーを適用する］ダイアログ　269
Android ポリシーを適用する流れ　125
Android ポリシー〔用語解説〕　480
APNs サーバ　23
APNs サーバの SSL 通信用クライアント証明書（MDM 用）を取得する流れ　78
APNs サーバの SSL 通信用クライアント証明書の設定手順〔通信サーバ〕　88
APNs サーバの SSL 通信用証明書　73
APNs サーバの SSL 通信用ルート証明書の取得手順 77
APNs サーバの SSL 通信用ルート証明書の設定手順〔通信サーバ〕　86
APNs〔用語解説〕　480

## B

［Bluetooth 接続情報］タブ〔［管理対象のスマートデバイス一覧］画面〕　263

## C

certutil cert コマンド〔証明書の形式変換〕　466
certutil cert コマンド〔証明書の内容表示〕　465
certutil reqgen コマンド　464
certutil req コマンド　465
Comet 接続〔用語解説〕　480
Comet〔用語解説〕　480
CommunicationServerEngine.properties〔通信サーバ環境設定ファイル〕　367

## E

eventmail.properties〔イベントメールフォーマット情報ファイル〕　363

## I

［iOS アプリケーション］画面　279
［iOS アプリケーション］画面で表示されるタブ　280
iOS アプリケーションのインストールでのトラブルシューティング　224
iOS アプリケーションのインストールに失敗する場合の対処方法　224
iOS アプリケーションの管理　55
［iOS アプリケーションの参照］ダイアログ　285
［iOS アプリケーションの追加］ダイアログ　283

［iOS アプリケーションの編集］ダイアログ　284
iOS 端末　23
iOS 端末で再度管理対象にする手順　172
iOS 端末の管理　106
iOS 端末のパスコードのリセット手順　179
iOS 端末のパスコードをリセットする流れ　131
iOS 端末のパスコードを忘れた場合の対処　130
iOS プロファイル　44
［iOS プロファイル一覧］画面　252
iOS プロファイル情報の編集手順　162
iOS プロファイル情報ファイルの形式　456
iOS プロファイルに設定できる項目について　49
iOS プロファイルのエクスポート手順　159
iOS プロファイルの管理　48
iOS プロファイルの削除手順　159
［iOS プロファイルの追加］ダイアログ　254
［iOS プロファイルの適用解除］ダイアログ　270
iOS プロファイルの適用解除手順　161
［iOS プロファイルの適用］ダイアログ　270
iOS プロファイルの適用手順　160
iOS プロファイルの適用または適用解除〔sdmapplyprofile コマンド〕　339
iOS プロファイルの利用　158
iOS プロファイルを適用する流れ　126
iOS プロファイル〔追加手順〕　158
iOS プロファイル〔用語解説〕　480
iPhone 構成ユーティリティ〔用語解説〕　480
ITDM2 管理用サーバ　23

## J

JP1/IT Desktop Management 2〔用語解説〕　480
JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のアンインストール手順〔Android 端末の設定メニュー〕　100
JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のアンインストール手順〔Google Play ストアアプリ〕　101
JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のインストール手順〔Android 端末の場合〕　96
JP1/ITDM2 - SDM（スマートデバイス Android エージェント）のインストール手順〔PC の場合〕　97
JP1/ITDM2 - SDM（スマートデバイス Android エージェント）〔用語解説〕　480
JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）のアンインストール手順　102
JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）のインストール手順　98
JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）〔用語解説〕　480
JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ　92
JP1/ITDM2 - SDM（スマートデバイスエージェント）〔用語解説〕　481
JP1/ITDM2 - SDM（スマートデバイスマネージャー）のインストール手順　66
JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ一覧　384
JP1/ITDM2 - SDM（スマートデバイスマネージャー）〔用語解説〕　481
JP1/ITDM2 - SDM（通信サーバ）のインストール手順　68
JP1/ITDM2 - SDM（通信サーバ）〔用語解説〕　481
JP1/ITDM2 - SDM（メッセージングサーバ）のインストール手順　70
JP1/ITDM2 - SDM（メッセージングサーバ）のメッセージ一覧　426
JP1/ITDM2 - SDM（メッセージングサーバ）〔用語解説〕　481
JP1/ITDM2 - SDM に登録されているスマートデバイスを準備する流れ　111
JP1/ITDM2 - SDM のアンインストール手順　99
JP1/ITDM2 - SDM を構成するコンポーネント　65

## K

keygen コマンド　463

## M

manager.properties〔スマートデバイスマネージャー環境設定ファイル〕　357
MDM 用クライアント証明書の作成手順　81
［MDM 用証明書の状況］パネル　236

MDM 用証明書要求ファイルのダウンロード手順 78
MDM 用署名済み証明書要求ファイルの作成手順 80
MDM 用署名済み証明書要求ファイルの作成〔sdmcreatemdmcertreq コマンド〕 350

## O

OMA-DM Client〔用語解説〕 481
OMA-DM〔用語解説〕 481

## P

provisioning.properties〔Provisioning 情報設定ファイル〕 361
Provisioning 情報設定ファイル(provisioning.properties) 361
Pull 配布 53
Push 配布 53

## S

sdmapplyprofile コマンド 339
sdmcreatemdmcertreq コマンド 350
sdmdistributeapp コマンド 337
SdMessagingServer.ini〔メッセージングサーバ設定ファイル〕 371
sdmexportdb コマンド 302
sdmexportdistributestatus コマンド 343
sdmexportinstallapp コマンド 346
sdmgetinventory コマンド 341
sdmgetlogs コマンド 352
sdmimportdb コマンド 305
sdmioutils deletedeliverypermit コマンド 334
sdmioutils exportdeliveryapp コマンド 321
sdmioutils exportdeliverypermit コマンド 326
sdmioutils exportdevice コマンド 308
sdmioutils exportpolicy コマンド 312
sdmioutils exportsdpolicy コマンド 316
sdmioutils importdeliveryapp コマンド 324
sdmioutils importdeliverypermit コマンド 330
sdmioutils importdevice コマンド 310
sdmioutils importpolicy コマンド 314
sdmioutils importsdpolicy コマンド 319
sdmnetchange コマンド 347
sslpasswd コマンド 467
SSL 通信用サーバ証明書の設定手順〔スマートデバイスマネージャー〕 84
SSL 通信用サーバ証明書の設定手順〔通信サーバ〕 87
SSL 通信用証明書の取得 75
SSL 通信用証明書の取得に使用するコマンド 463
SSL 通信用証明書の種類 73
SSL 通信用証明書の配置 74
SSL 通信用ルート証明書の設定手順〔Android 端末〕 95
SSL 通信用ルート証明書の設定手順〔iOS 端末〕 96

## T

testmail.properties〔テストメール送信フォーマット情報ファイル〕 366

## W

[WEB 閲覧履歴] タブ〔[管理対象のスマートデバイス一覧] 画面〕 260
Web サーバの秘密鍵の作成〔keygen コマンド〕463
[Web サイトの追加] ダイアログ 245
[Web サイトの編集] ダイアログ 245

## あ

アプリーションのインストール結果が [iOS アプリケーション] 画面に反映されない場合の対処方法 224
アプリケーションのアンインストール手順〔Android 端末〕 194
アプリケーションのアンインストール手順〔iOS 端末〕 196
アプリケーションのインストール指示〔sdmdistributeapp コマンド〕 337
アプリケーションをインストールする流れ〔iOS 端末〕 120
アプリケーションのインストールの指示手順〔Android 端末〕 192
アプリケーションのインストールの指示手順〔iOS 端末〕 195
アプリケーションの管理 53, 182
アプリケーションの削除手順 188

［アプリケーションの追加］ダイアログ　246
アプリケーションの配布手順〔Android 端末〕　190
アプリケーションの配布・インストールする流れ〔Android 端末〕　118
［アプリケーションの編集］ダイアログ　247
アプリケーション配布状況の出力〔sdmexportdistributestatus コマンド〕　343
アプリケーション配布情報のインポート〔sdmioutils importdeliveryapp コマンド〕　324
アプリケーション配布情報のエクスポート〔sdmioutils exportdeliveryapp コマンド〕　321
アプリケーション配布情報ファイルの形式　455
アンインストール手順〔Android アプリケーション〕　194
アンインストール手順〔iOS アプリケーション〕　196
アンインストール手順〔JP1/ITDM2 - SDM（スマートデバイス Android エージェント）〕　100, 101
アンインストール手順〔JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）〕　102
アンインストール手順〔JP1/ITDM2 - SDM〕　99

## い

イベント一覧エクスポート CSV ファイルの形式　448
［イベント一覧］画面　286
イベント画面　286
イベント画面でできること　32
イベント画面の画面遷移　229
イベント出力される JP1/ITDM2 - SDM（スマートデバイスマネージャー）のメッセージ　375
［イベント詳細］ダイアログ　288
イベント情報のエクスポート手順　204
［イベント］タブ〔［管理対象外のスマートデバイス一覧］画面〕　265
［イベント］タブ〔［管理対象のスマートデバイス一覧］画面〕　259
［イベント通知の設定］画面　293
イベント通知の設定手順　206
イベントの形式　58
イベントの参照　202
イベントの種類　57
［イベントの状況］パネル　234
イベントの詳細の確認手順　203
イベントの表示　57
イベントメールフォーマット情報ファイル（eventmail.properties）　363
［インストール済みスマートデバイス一覧］タブ〔［Android アプリケーション］画面〕　278
［インストール済みスマートデバイス一覧］タブ〔［iOS アプリケーション］画面〕　280
インストールソフトウェア情報出力ファイルの形式　460
インストールソフトウェア情報の出力〔sdmexportinstallapp コマンド〕　346
インストール手順〔JP1/ITDM2 - SDM（スマートデバイス Android エージェント）〕　96, 97
インストール手順〔JP1/ITDM2 - SDM（スマートデバイス iOS エージェント）〕　98
インストール手順〔JP1/ITDM2 - SDM（スマートデバイスマネージャー）〕　66
インストール手順〔JP1/ITDM2 - SDM（通信サーバ）〕　68
インストール手順〔JP1/ITDM2 - SDM（メッセージングサーバ）〕　70
インストールの指示手順〔Android アプリケーション〕　192
インストールの指示手順〔iOS アプリケーション〕　195
インフォメーションエリア　26
インベントリ情報一覧　469
インベントリ情報の取得〔sdmgetinventory コマンド〕　341
インポート・エクスポートファイルの出力形式　444

## う

運用中にできること　108
運用方法　105

## え

エクスポート手順〔iOS プロファイル〕　159
エクスポート手順〔イベント情報〕　204
エクスポート手順〔スマートデバイス一覧〕　169

## か

概況表示　38
確認手順〔イベントの詳細〕　203
画面構成　25
画面遷移図　226
画面遷移〔イベント画面〕　229
画面遷移〔スマートデバイス画面〕　227
画面遷移〔セキュリティ画面〕　227
画面遷移〔設定画面〕　229
画面遷移〔配布画面〕　228
画面遷移〔ログイン画面からログイン直後〕　226
画面操作時のトラブルシューティング　221
管理者のコンピュータ　23
管理者のコンピュータ〔用語解説〕　481
［管理対象外にする］ダイアログ　268
［管理対象外のスマートデバイス一覧］画面　264
［管理対象外のスマートデバイス一覧］画面で表示されるタブ　265
管理対象外のスマートデバイスの管理　51
管理対象外のスマートデバイスを管理対象にする 170
管理対象外の設定手順　173
［管理対象のスマートデバイス一覧］画面　256
［管理対象のスマートデバイス一覧］画面で表示されるタブ　259
管理対象のスマートデバイスの管理　50
管理対象のスマートデバイスを管理対象外にする手順　173
管理対象の設定手順　170
管理〔Android アプリケーション〕　54
管理〔Android ポリシー〕　46
管理〔iOS アプリケーション〕　55
管理〔iOS プロファイル〕　48
管理〔管理対象外のスマートデバイス〕　51
管理〔管理対象のスマートデバイス〕　50
管理〔スマートデバイス〕　50
管理〔セキュリティポリシー〕　45
管理〔配布アプリケーション〕　53
管理〔ユーザーアカウント〕　40

## き

［起動中アプリケーション］タブ〔［管理対象のスマートデバイス一覧］画面〕　262
機能一覧　37
基本的な画面構成　25

## こ

構成プロファイルの作成手順〔通信サーバ〕　88
構成プロファイル〔用語解説〕　481
この製品でできること　20
コマンド　296
コマンド一覧　299
コマンドの説明形式　297
コマンドのメッセージ一覧　430
コマンドを実行する流れ　298

## さ

サーバ間での通信エラー発生時のトラブルシューティング　219
サーバのファイアウォールの設定　72
サービス一覧　435
再度管理対象とするための設定手順〔Android 端末〕　171
再度管理対象とするための設定手順〔iOS 端末〕　172
削除手順〔Android ポリシー〕　155
削除手順〔iOS プロファイル〕　159
削除手順〔アプリケーション〕　188
削除手順〔スマートデバイス〕　174
削除手順〔セキュリティポリシー〕　151
削除手順〔ユーザーアカウント〕　144
作成手順〔MDM 用クライアント証明書〕　81
作成手順〔MDM 用署名済み証明書要求ファイル〕　80
サポートに必要な情報の格納先または入手方法　461
参照権限　40
参照権限で実行できない操作一覧　41
参照権限〔用語解説〕　481

## し

システム管理権限　40

システム管理権限〔用語解説〕 482
システム構成例 24
システム構築 60
[システムサマリ] パネル 233
[システム情報] タブ〔[管理対象外のスマートデバイス一覧] 画面〕 266
[システム情報] タブ〔[管理対象のスマートデバイス一覧] 画面〕 263
システムの概況表示 38
システムの構成要素 23
システムを構築する流れ 61
実行できない操作一覧〔参照権限〕 41
自分のパスワードの変更手順 145
自分のユーザーアカウントの編集手順 142
重大度〔用語解説〕 482
出力されるイベント 57
取得手順〔スマートデバイスの最新のインベントリ情報〕 175
取得手順〔スマートデバイスのログ〕 181
証明書の形式変換〔certutil cert コマンド〕 466
証明書の取得手順〔APNs サーバの SSL 通信用ルート証明書〕 77
証明書の取得〔APNs サーバの SSL 通信用クライアント証明書（MDM 用）〕 78
証明書の取得〔スマートデバイスマネージャーの SSL 通信用証明書〕 76
証明書の取得〔通信サーバの SSL 通信用証明書〕 75
証明書の設定手順〔Android 端末〕 95
証明書の設定手順〔iOS 端末〕 96
証明書の設定〔スマートデバイスマネージャー〕 83
証明書の設定〔通信サーバ〕 86
証明書の内容表示〔certutil cert コマンド〕 465
証明書発行要求（CSR）の作成〔certutil reggen コマンド〕 464
証明書発行要求（CSR）の内容表示〔certutil reg コマンド〕 465
初期化されたスマートデバイスを管理対象にする流れ 131
初期化手順〔スマートデバイス〕 176
初期化手順〔ほかの管理者のパスワード〕 146
初期化〔用語解説〕 482
新規に購入したスマートデバイスを準備する流れ 110

## す

スマートデバイス一覧エクスポート・インポート CSV ファイルの形式 444
[スマートデバイス一覧のインポート] ダイアログ 272
スマートデバイス一覧のエクスポート手順 169
スマートデバイス画面 256
スマートデバイス画面でできること 29
スマートデバイス画面の画面遷移 227
スマートデバイスから利用者の操作でアプリケーションをインストールする流れ 122
スマートデバイス情報のインポート〔sdmioutils importdevice コマンド〕 310
スマートデバイス情報のエクスポート〔sdmioutilsexportdevice コマンド〕 308
スマートデバイスセキュリティポリシー（Android ポリシーまたは iOS プロファイル）エクスポート XML ファイルの形式 451
スマートデバイスでのトラブルシューティングの手順 217
スマートデバイスに JP1/ITDM2 - SDM（スマートデバイスエージェント）を導入する流れ 92
スマートデバイスの JP1/ITDM2 - SDM への登録 165
スマートデバイスの管理 50, 164
スマートデバイスの管理の流れ 21
スマートデバイスの最新のインベントリ情報の取得手順 175
スマートデバイスの削除手順 174
スマートデバイスの準備 110
[スマートデバイスの初期化] ダイアログ 266
スマートデバイスの初期化手順 176
[スマートデバイスの追加] ダイアログ 271
スマートデバイスの登録手順 165
スマートデバイスの登録手順〔CSV ファイル〕 167
[スマートデバイスのパスコードのリセット] ダイアログ 268
スマートデバイスの利用者を変更する流れ 114
[スマートデバイスのロック] ダイアログ 267
スマートデバイスのロック手順 177

スマートデバイス紛失時の対処　128
[スマートデバイスへのメッセージ通知]ダイアログ　273
スマートデバイスマネージャー　23
スマートデバイスマネージャー環境設定ファイル(manager.properties)　357
スマートデバイスマネージャーで管理対象外のスマートデバイスを管理対象にする手順　170
スマートデバイスマネージャーでの SSL 通信用証明書の設定　83
スマートデバイスマネージャーでのトラブルシューティングの手順　216
スマートデバイスマネージャーと通信サーバ間で通信エラーが発生する場合の対処方法　219
スマートデバイスマネージャーの SSL 通信用証明書 73
スマートデバイスマネージャーの SSL 通信用証明書を取得する流れ　76
スマートデバイスマネージャーまたは通信サーバのネットワーク構成変更〔sdmnetchange コマンド〕　347
スマートデバイスマネージャー〔用語解説〕　482
スマートデバイスを新規に配布する流れ　112
スマートデバイスを保管する流れ　116
スマートデバイスを滅却する流れ　117
スマートデバイスをリプレースする流れ　113
スマートデバイス〔用語解説〕　482

## せ

製品概要　20
セキュリティ画面　238
セキュリティ画面でできること　27
セキュリティ画面の画面遷移　227
セキュリティ状況の管理　148
[セキュリティ]タブ〔[管理対象のスマートデバイス一覧]画面〕　263
セキュリティの管理　44
セキュリティのルールの管理　125
セキュリティのルールの種類　44
セキュリティのルール〔用語解説〕　482
セキュリティポリシー　44
セキュリティポリシー一覧エクスポート XML ファイルの形式　449
[セキュリティポリシー一覧]画面　238
セキュリティポリシー設定情報のインポート〔sdmioutils importpolicy コマンド〕　314
セキュリティポリシー設定情報のエクスポート〔sdmioutils exportpolicy コマンド〕　312
セキュリティポリシーに設定できる項目　45
セキュリティポリシーの管理　45
セキュリティポリシーの削除手順　151
[セキュリティポリシーの参照]ダイアログ　242
[セキュリティポリシーの追加]ダイアログ　240
セキュリティポリシーの追加手順　149
セキュリティポリシーの適用手順　152
[セキュリティポリシーの編集]ダイアログ　241
セキュリティポリシーの編集手順　150
セキュリティポリシーの利用　149
[セキュリティポリシーを適用する]ダイアログ　269
セキュリティポリシー〔用語解説〕　482
設定画面　289
設定画面でできること　33
設定画面の画面遷移　229
設定できる項目〔Android ポリシー〕　46
設定できる項目〔iOS プロファイル〕　49
設定できる項目〔セキュリティポリシー〕　45
設定手順〔イベント通知〕　206
設定手順〔メールサーバ〕　207
設定手順〔ユーザーアカウント情報〕　137
前提 OS　63
前提プログラム　64

## そ

操作画面　25
組織のセキュリティ方針の策定　93
[ソフトウェア]タブ〔[管理対象のスマートデバイス一覧]画面〕　261

## た

対処方法〔iOS アプリケーションのインストールに失敗する場合〕　224

対処方法〔アプリーションのインストール結果が［iOS アプリケーション］画面に反映されない場合〕 224
対処方法〔スマートデバイスマネージャーと通信サーバ間で通信エラーが発生する場合〕 219
対処方法〔通信サーバとメッセージングサーバ間で通信エラーが発生する場合〕 219
対処方法〔ディスクの空き容量が少ないとき〕 218
対処方法〔データベース接続エラーが発生する場合〕 222
対処方法〔データベースのアクセスエラーが発生する場合〕 222
対処方法〔データベースのバックアップが失敗する場合〕 222
対処方法〔データベースのリストアが失敗する場合〕 222
ダウンロード手順〔MDM 用証明書要求ファイル〕 78
タブ 26

## つ

追加手順〔Android ポリシー〕 154
追加手順〔iOS プロファイル〕 158
追加手順〔セキュリティポリシー〕 149
追加手順〔ユーザーアカウント〕 141
通信エラーが発生する場合の対処方法〔スマートデバイスマネージャーと通信サーバ間〕 219
通信エラーが発生する場合の対処方法〔通信サーバとメッセージングサーバ間〕 219
通信サーバ 23
通信サーバ環境設定ファイル (CommunicationServerEngine.properties) 367
通信サーバでの SSL 通信用証明書の設定 86
通信サーバとメッセージングサーバ間で通信エラーが発生する場合の対処方法 219
通信サーバの SSL 通信用証明書 73
通信サーバの SSL 通信用証明書を取得する流れ 75
通信サーバの SSL 通信用ルート証明書の設定手順〔スマートデバイスマネージャー〕 83
通信サーバをバージョンアップインストールするときの作業 103
通信サーバ〔用語解説〕 482
通知手順〔メッセージ〕 180
［通話履歴］タブ〔［管理対象のスマートデバイス一覧］画面〕 259

## て

定義ファイル 355
定義ファイル一覧 356
ディスクの空き容量が少ないときの対処方法 218
データベース障害のトラブルシューティング 222
データベース接続エラーが発生する場合の対処方法 222
［データベースとディスクの状況］パネル 235
データベースのアクセスエラーが発生する場合の対処方法 222
データベースの管理 208
データベースの接続先ポート番号の変更手順 213
データベースのバックアップが失敗する場合の対処方法 222
データベースのバックアップ手順 209
データベースのリストアが失敗する場合の対処方法 222
データベースのリストア手順 211
適用解除手順〔iOS プロファイル〕 161
適用手順〔Android ポリシー〕 156
適用手順〔iOS プロファイル〕 160
適用手順〔セキュリティポリシー〕 152
できること〔イベント画面〕 32
できること〔スマートデバイス画面〕 29
できること〔セキュリティ画面〕 27
できること〔設定画面〕 33
できること〔配布画面〕 31
できること〔ホーム画面〕 27
テストメール送信フォーマット情報ファイル (testmail.properties) 366
デバイス情報ファイルの形式 457
デフォルトパスワードの設定手順 138
［電話番号の追加］ダイアログ 243
［電話番号の編集］ダイアログ 244

## と


[動作中サービス] タブ〔[管理対象のスマートデバイス一覧] 画面〕 262
登録したアプリケーションの情報の編集手順 186
登録手順〔スマートデバイス〕 165
登録手順〔スマートデバイス〕－〔CSV ファイル〕 167
登録手順〔配布するアプリケーション〕 183
トラブルシューティング 215
トラブルシューティング〔iOS アプリケーションのインストール〕 224
トラブルシューティング〔画面操作時〕 221
トラブルシューティング〔サーバ間での通信エラー発生時〕 219
トラブルシューティング〔スマートデバイスマネージャー〕 216
トラブルシューティング〔スマートデバイス〕 217
トラブルシューティング〔データベース障害〕 222


## は


[ハードウェア] タブ〔[管理対象のスマートデバイス一覧] 画面〕 262
[配布アプリケーション一覧] 画面 274
配布アプリケーションエクスポート XML ファイルの形式 452
配布アプリケーションの管理 53
配布アプリケーションの最大同時ダウンロード数を制限する手順 201
配布画面 274
配布画面でできること 31
配布画面の画面遷移 228
配布許可定義ファイルの形式 454
配布状況出力ファイルの形式 457
[配布済みスマートデバイス一覧] タブ〔[Android アプリケーション] 画面〕 278
配布するアプリケーションの登録手順 183
配布するアプリケーションを通信サーバに配置する手順 185
配布手順〔Android アプリケーション〕 190
パスコードのリセット〔iOS 端末〕 131
パスコード〔用語解説〕 483
[パスワードの変更] ダイアログ 231
パスワードの変更〔Android 端末〕 130
パスワードファイルの作成〔sslpasswd コマンド〕 467
バックアップデータのリストア〔sdmimportdb コマンド〕 305
バックアップ手順〔データベース〕 209
バックアップの取得〔sdmexportdb コマンド〕 302
発生したイベントをメールで通知する流れ 133
パラメーター一覧 440
パラメーター〔イベント通知の設定〕 441
パラメーター〔メールサーバ設定〕 442
パラメーター〔ユーザーアカウントの設定〕 440


## ふ


フォルダー一覧 432
フォルダ〔スマートデバイスマネージャー〕 432
フォルダ〔通信サーバ〕 433
フォルダ〔メッセージングサーバ〕 434
不要となったアプリケーションを削除する流れ 124
不要となったアプリケーションを通信サーバから削除する手順 189
プリインストールされている SSL 通信用ルート証明書の確認手順〔スマートデバイス〕 94
プロセス一覧 436
プロビジョニングの設定 94
プロビジョニング〔用語解説〕 483
紛失したスマートデバイスを初期化する流れ 129
紛失したスマートデバイスをロックする流れ 128


## へ


変更手順〔Android 端末のパスワード〕 178
変更手順〔自分のパスワード〕 145
変更手順〔データベースの接続先ポート番号〕 213
変更手順〔デフォルトパスワード〕 138
編集手順〔Android ポリシー〕 154
編集手順〔iOS プロファイル情報〕 162
編集手順〔自分のユーザーアカウント〕 142
編集手順〔セキュリティポリシー〕 150

編集手順〔登録したアプリケーションの情報〕 186
編集手順〔ほかの管理者のユーザーアカウント〕 143

## ほ

ポート開放およびファイアウォールの設定 72
ポート番号一覧 438
ホーム画面 233
ホーム画面でできること 27
ほかの管理者のパスワードの初期化手順 146
ほかの管理者のユーザーアカウントの編集手順 143

## み

[未インストールスマートデバイス一覧] タブ〔[iOS アプリケーション] 画面〕 280
[未配布スマートデバイス一覧] タブ〔[Android アプリケーション] 画面〕 277

## め

[メールサーバ設定] 画面 294
メールサーバの設定手順 207
メッセージ 373
メッセージ一覧〔JP1/ITDM2 - SDM（スマートデバイスマネージャー)〕 384
メッセージ一覧〔JP1/ITDM2 - SDM（メッセージングサーバ)〕 426
メッセージ一覧〔コマンド〕 430
メッセージの形式 374
メッセージの通知手順〔Android 端末〕 180
メッセージングサーバ 23
メッセージングサーバ設定ファイル (SdMessagingServer.ini) 371
メッセージングサーバ〔用語解説〕 483
メニューエリア 26
メニューエリア〔用語解説〕 483

## ゆ

ユーザーアカウント情報の設定手順 137
ユーザーアカウントの管理 40, 140
[ユーザーアカウントの管理] 画面 289
ユーザーアカウントの権限 40
ユーザーアカウントの削除手順 144
[ユーザーアカウントの追加] ダイアログ 290
ユーザーアカウントの追加手順 141
[ユーザーアカウントの編集] ダイアログ 291
ユーザーアカウントのロック 40
ユーザーアカウントのロック解除手順 147

## り

リストア手順〔データベース〕 211
リセット手順〔iOS 端末のパスコード〕 179
利用者が Android 端末のパスワードまたは iOS 端末のパスコードを忘れた場合の対処 130
利用者の操作でアプリケーションをインストールする手順〔Android 端末〕 199
利用者の操作でアプリケーションをインストールする手順〔iOS 端末〕 200
利用者の操作でインストールできるアプリケーションの設定情報のエクスポート〔sdmioutils exportdeliverypermit コマンド〕 326
利用者の操作でインストールできるアプリケーションの設定情報の削除〔sdmioutils deletedeliverypermit コマンド〕 334
利用者の操作でインストールできるアプリケーションの設定〔sdmioutils importdeliverypermit コマンド〕 330

## る

ルータのポート開放 72

## ろ

ログアウト手順 139
ログイン画面 231
ログイン画面からログイン直後までの画面遷移 226
ログイン手順 135
ログ情報の取得〔sdmgetlogs コマンド〕 352
ログの取得手順〔スマートデバイス〕 181
ロック解除手順〔ユーザーアカウント〕 147
ロック手順〔スマートデバイス〕 177
ロック〔用語解説〕 483

株式会社 日立製作所

〒 100-8280　東京都千代田区丸の内一丁目 6 番 6 号