Optimal Biz

管理サイト　リファレンスマニュアル

最終更新日　2025 年 10 月 8 日

（Web サイト ver.9.22.0）

株式会社オプティム

はじめに

本マニュアルでは、Optimal Biz（以下、本製品と呼ぶ）の操作ほか、各機能の概要、画面の説明、設定操作について説明しています。

また、要点となる各種の内容を以下に記載しています。これらの内容をご理解の上、マニュアルをお読みください。

名称・呼称

本マニュアルに登場する特定の企業、人について、以下の定義で記載しています。

名称	説明
サービス企業	本製品を提供する企業。
管理者	本製品の管理サイト（機器の管理・運用を行う Web サイト）を運用する者。
端末使用者	本製品で管理している端末を使用する者。
システム管理者	企業の社内システム（サーバー・インフラなど）を管理する者。

注意・ポイントマーク

操作を行う場合に注意する点や、操作のポイントとなる点を示す場合は、以下のマークで記載しています。

マーク	説明
	データの破損や消失など、特に注意していただきたい内容を記載しています。
	操作のポイントや知っておくと便利な内容を記載しています。

記号

画面に表示されるボタンやメニュー、キーボードのキーなどを示す場合は、以下の記号で記載しています。

マーク	説明
［ ］	ボタン、メニュー、タブ、リンク、チェックボックス、ラジオボタンなどの名称を示しています。
「 」	画面名、機能名、項目名、マニュアル内の参照先などを示しています。
『 』	マニュアルや資料などの名称を示しています。
〈 〉	キーボードなどのハードキー名称（スペースキーは〈スペース〉と表記）を示しています。

参照マーク

他のマニュアルや他のページへなどの参照を示す場合は、以下のマークで記載しています。

マーク	説明
	他のページや Web サイトへの参照を示しています。クリックすると該当箇所にジャンプします。
	セクション内の画面への参照を示しています。クリックすると該当の画面にジャンプします。
	他のマニュアルや資料への参照を示しています。

用語集

不明な用語は、以下を参照してください。

『FAQ 一覧』

免責事項

●本マニュアルは、ユーザー種別が［管理者］のユーザーを対象としています。［管理者］以外のユーザー種別でログインした場合は、操作が制限されます。

●iPad OS の操作は iOS と同様です。差異がある場合は iPad OS 用の記載をしています。

●画面上のバージョン表記は、実際の表示と異なる場合があります。

●本マニュアルに記載されている Web サイトの URL は、予告なく変更される場合があります。

●OS のバージョンやブラウザーにより、一部の画面や操作が異なる場合があります。本マニュアルでは、Google Chrome を例に説明しています。

登録商標

●Apple、iPad、iPadOS、iPhone、Mac、macOS は、米国およびその他の国で登録された Apple Inc.の商標です。

●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。

●iPhone 商標は、アイホン株式会社のライセンスに基づき使用されています。

●App Store は、Apple Inc.のサービスマークです。

●Android、Google Chrome、Google Cloud、Google マップ、Google Play、Google Workspace は、Google LLC の商標です。

●Microsoft、Microsoft Edge 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 の正式名称は、Microsoft Windows Operating System 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。

●その他記載の会社名、製品名は、各社の登録商標および商標です。

目次

1 Optimal Biz とは | 2 基本操作 | 3 ダッシュボード | 4 機器
5 ユーザー | 6 組織 | 7 設定－Android | 8 設定－iOS
9 設定－Windows | 10 サービス環境設定 | 11 ログ | 12 サイトマップ

1 Optimal Biz とは 12
1.1 概要 13
1.2 特徴 13
1.3 管理サイトの役割 14
1.4 管理サイトの動作環境 15

2 基本操作 16
2.1 ログイン／ログアウト 17
2.2 管理サイト画面の構成 18
2.3 管理サイトの共通操作 20
2.4 設定画面の共通操作 25
2.4.1 新規作成 25
2.4.2 編集 27
2.4.3 複製 29
2.4.4 削除 31
2.4.5 一括削除 32
2.4.6 一覧項目の操作 33
2.4.7 詳細情報の表示 35

3 ダッシュボード 37
3.1 ダッシュボードの画面構成 38
3.2 お知らせ 40
3.3 インシデント 42
3.3.1 インシデント設定 46
3.3.2 インシデントの詳細画面 47
3.4 個人設定 49

4 機器 53
4.1 一覧 54
4.1.1 機器一覧 54
4.1.2 機器の詳細画面 59
4.1.3 機器の新規作成 61
4.1.4 機器の管理情報 67
4.1.5 機器との同期 70
4.1.6 機器検出の情報 72
4.1.7 機器の個別削除 73
4.1.8 機器の設定 74
4.1.8.1 （設定－Android）設定の割り当て 75

4.1.8.2 （設定－Android）設定テンプレートの割り当て....77
4.1.8.3 （設定－Android）パッケージ....78
4.1.8.4 （設定－Android）クライアント証明書....79
4.1.8.5 （設定－iOS）設定の割り当て....83
4.1.8.6 （設定－iOS）設定テンプレートの割り当て....85
4.1.8.7 （設定－iOS）クライアント証明書....86
4.1.8.8 （設定－iOS）Exchange（ActiveSync）設定....89
4.1.8.9 （設定－iOS）VPN 設定....94
4.1.8.10 （設定－iOS）個別構成プロファイル....98
4.1.8.11 （設定－iOS）「App とブック」設定....100
4.1.8.12 （設定－Windows）設定セットの割り当て....103
4.1.8.13 （設定－Windows）設定テンプレートの割り当て....105
4.1.8.14 （設定－Windows）クライアント証明書....106
4.1.9 機器の操作....109
4.1.9.1 （操作－Android）スクリーンロックパスワード変更....109
4.1.9.2 （操作－Android）リモートロック....110
4.1.9.3 （操作－Android）ロック解除....113
4.1.9.4 （操作－Android）リモートワイプ....114
4.1.9.5 （操作ーAndroid）Google Play ストアのキャッシュ削除....115
4.1.9.6 （操作－iOS）パスコード削除....116
4.1.9.7 （操作－iOS）リモートロック....117
4.1.9.8 （操作－iOS）リモートワイプ....118
4.1.9.9 （操作－iOS）リモートワイプ（管理領域）....121
4.1.9.10 （操作－iOS）紛失モード....122
4.1.9.11 （操作－iOS）位置情報取得....123
4.1.9.12 （操作－iOS）紛失モード解除....124
4.1.9.13 （操作－iOS）アクティベーションロック解除....125
4.1.9.14 （操作－iOS）OS アップデート....126
4.1.9.15 （操作－iOS）リモート再起動....127
4.1.9.16 （操作－iOS）リモートシャットダウン....128
4.1.9.17 （操作－iOS）MDM 構成プロファイル更新....129
4.1.9.18 （操作－Windows）リモートロック....130
4.1.9.19 （操作－Windows）ロック解除....131
4.1.9.20 （操作－Windows）リモートワイプ....131
4.1.10 機器の情報....134
4.1.10.1 （情報－Android）ログ....134
4.1.10.2 （情報－Android）デバイス....135
4.1.10.3 （情報－Android）エージェント....140
4.1.10.4 （情報－Android）アプリケーション....141
4.1.10.5 （情報－Android）アプリ構成....144
4.1.10.6 （情報－Android）位置....146
4.1.10.7 （情報－Android）Zone Management....148
4.1.10.8 （情報－Android）メッセージ....149
4.1.10.9 （情報－iOS）ログ....150
4.1.10.10 （情報－iOS）デバイス....151
4.1.10.11 （情報－iOS）エージェント....155
4.1.10.12 （情報－iOS）アプリケーション....157
4.1.10.13 （情報－iOS）プロファイル....162
4.1.10.14 （情報－iOS）位置....165
4.1.10.15 （情報－iOS）ADE....168

4.1.10.16 （情報－iOS）メッセージ 170
4.1.10.17 （情報－iOS）書籍 171
4.1.10.18 （情報－Windows）ログ 172
4.1.10.19 （情報－Windows）デバイス 173
4.1.10.20 （情報－Windows）エージェント 177
4.1.10.21 （情報－Windows）アプリケーション 178
4.1.10.22 （情報－Windows）セキュリティ 181
4.1.10.23 （情報－Windows）位置 183
4.1.10.24 （情報－Windows）Zone Management 185
4.1.10.25 （情報－Windows）Microsoft Update 更新プログラム 186
4.2 ネットワークマップ 187
4.2.1 ネットワークマップの見かた 187
4.2.1.1 機器の種類 190
4.2.1.2 機器アイコン一覧 191
4.2.2 管理外機器を管理対象機器に設定 194
4.2.3 管理外機器を除外機器に設定 196
4.2.4 除外機器を管理外機器に設定 197
4.3 認証手順 198
4.4 全機器一括設定 200
4.4.1 ［Android 設定］タブ 202
4.4.2 ［iOS 設定］タブ 204
4.4.3 ［Windows 設定］タブ 205
4.4.4 ［その他▼］タブ／Android リモート操作 206
4.4.5 ［その他▼］タブ／iOS リモート操作 210
4.4.6 ［その他▼］タブ／Windows リモート操作 215
4.5 入力項目のカスタマイズ 218
4.5.1 ［分類］タブ 219
4.5.2 ［自由入力］タブ 221
4.6 メッセージ通知 223
4.6.1 ［メッセージ］タブ 224
4.6.2 ［配信先］タブ 226
4.6.3 ［スケジュール］タブ 227
4.6.4 ［配信履歴］タブ 228
4.7 CSV で追加 229
4.8 CSV で編集 232
4.9 CSV で削除 233
4.10 CSV でクライアント証明書紐付け（iOS のみ） 235
4.11 CSV をダウンロード 237
4.11.1 機器レポート 237
4.11.2 アプリケーションレポート 241
4.11.3 アプリケーションレポート（高速版） 245
4.11.4 プロファイルレポート 249
4.12 旧デザイン 252

5 ユーザー 253
5.1 一覧 254
5.1.1 ［管理］タブ 257
5.1.2 ［操作］タブ 261
5.1.3 ［「App とブック」設定］タブ 262
5.1.4 ［その他▼］タブ／設定 270
5.2 入力項目のカスタマイズ 271
5.2.1 ［分類］タブ 272
5.2.2 ［自由入力］タブ 275
5.3 CSV で追加 277
5.4 CSV で編集 279
5.5 CSV をダウンロード 280

6 組織 281
6.1 一覧 282
6.1.1 ［管理］タブ 284
6.1.2 ［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ 286
6.1.3 ［その他▼］タブ／ユーザー設定 288
6.1.4 ［その他▼］タブ／「App とブック」設定 289
6.2 CSV で追加 293
6.3 CSV で編集 295
6.4 CSV をダウンロード 296

7 設定－Android 297
7.1 管理アプリの通信と動作 298
7.2 設定テンプレート 300
7.3 セキュリティ 304
7.3.1 画面ロック 304
7.3.2 位置情報管理 309
7.3.3 Secure Shield 311
7.3.4 機能制限 315
7.3.5 機能制限／カメラ 315
7.3.6 機能制限／SD カード 316
7.3.7 機能制限／Bluetooth 318
7.4 アプリケーション 320
7.4.1 アプリケーション禁止 320
7.4.1.1 ［設定］タブ 321
7.4.1.2 ［高度な設定］タブ 324

7.4.2 アプリケーション検知 325
7.4.3 Android Enterprise 327
7.4.4 Android Enterprise／アプリケーション配信 327
7.4.5 Android Enterprise／個別アプリケーション 333
7.4.6 Android Enterprise／企業許可アプリ 338
7.4.7 Android Enterprise／アプリ権限ポリシー 340
7.5 インターネット 342
7.5.1 Wi-Fi フィルタリング 342
7.6 便利機能 344
7.6.1 連絡先 344
7.6.2 SIM ステータス変更検知 347
7.7 証明書管理 348
7.7.1 クライアント証明書管理 348
7.7.2 クライアント証明書一括アップロード 352
7.7.3 クライアント証明書一括削除 354
7.7.4 CA 証明書管理 355
7.8 Zone Management 357
7.8.1 ゾーン 357
7.8.2 ポリシー 360
7.8.2.1 ［管理］タブ 360
7.8.2.2 ［Android 設定］タブ 361
7.8.3 ゾーンポリシー構成 362
7.9 Device Owner Mode 364
7.9.1 セキュリティ設定（DOM） 364
7.9.2 アプリケーション非表示 369
7.9.3 OS アップデート（DOM） 372
7.9.4 ファクトリーリセット保護（DOM） 374
7.10 ゼロタッチ登録 377
7.10.1 利用登録 377
7.10.2 機器一覧 380

8 設定－iOS 382
8.1 管理アプリの通信と動作 383
8.2 設定テンプレート 387
8.3 構成プロファイル 392
8.3.1 構成プロファイルアップロード 393
8.3.1.1 ［管理］タブ 393
8.3.1.2 ［一般］タブ 397
8.3.1.3 ［パスコード設定］タブ 398
8.3.1.4 ［iOS 制限設定］タブ 400
8.3.1.5 ［Wi-Fi 設定］タブ 412
8.3.1.6 ［その他▼］タブ／メール設定 423
8.3.1.7 ［その他▼］タブ／証明書設定 425
8.3.1.8 ［その他▼］タブ／グローバル HTTP プロキシ設定 426
8.3.1.9 ［その他▼］タブ／DNS プロキシ設定 428
8.3.1.10 ［その他▼］タブ／コンテンツフィルタ設定 430
8.3.1.11 ［その他▼］タブ／ドメイン設定 434
8.3.1.12 ［その他▼］タブ／VPN 設定 435
8.3.1.13 ［その他▼］タブ／カレンダー設定 485

8.3.1.14 ［その他▼］タブ／照会したカレンダー設定 486
8.3.1.15 ［その他▼］タブ／連絡先設定 487
8.3.1.16 ［その他▼］タブ／通知 488
8.3.1.17 ［その他▼］タブ／Web クリップ設定 490
8.3.1.18 ［その他▼］タブ／モバイル通信設定 492
8.3.1.19 ［その他▼］タブ／ロック画面のメッセージ 497
8.3.1.20 ［その他▼］タブ／変数項目と反映状況 498
8.3.2 構成プロファイル 500
8.4 ADE 502
8.4.1 ADE トークン登録 503
8.4.2 ADE 定義プロファイル 505
8.4.3 ADE 機器管理 509
8.5 Shared iPad セキュリティ 512
8.6 アプリケーション 514
8.6.1 「App とブック」ライセンス 514
8.6.1.1 ［管理］タブ 515
8.6.1.2 ［アプリケーション］タブ 518
8.6.1.3 ［書籍］タブ 519
8.6.2 「App とブック」設定テンプレート 520
8.6.3 管理対象アプリポリシー 523
8.6.4 オリジナルアプリ登録 524
8.6.4.1 ［設定］タブ 524
8.6.5 App Configuration 528
8.6.5.1 ［設定］タブ 528
8.6.6 アプリケーション配信 530
8.6.7 シングル APP モード（監視対象のみ） 535
8.6.8 アプリケーション検知 542
8.7 便利機能 545
8.7.1 ローミング設定 545
8.7.2 ホーム画面レイアウト（監視対象のみ） 546
8.7.3 SIM ステータス変更検知 552
8.8 証明書管理 553
8.8.1 クライアント証明書管理 553
8.8.2 クライアント証明書一括アップロード 557
8.8.3 クライアント証明書一括削除 559

9 設定－Windows 560
9.1 管理アプリの通信と動作 561
9.2 設定テンプレート 564
9.3 セキュリティ 568
9.3.1 画面ロック 568
9.3.2 暗号化 573
9.3.3 位置情報管理 576
9.3.4 システムセキュリティ 578
9.3.5 SIM 抜き差し監視 586
9.3.6 機能制限 590
9.3.7 機能制限／外部デバイス 590
9.3.8 機能制限／CD/DVD/ブルーレイ 600
9.4 アプリケーション 602
9.4.1 アプリケーション禁止 602
9.5 インターネット 609
9.5.1 Wi-Fi 609
9.5.2 Wi-Fi フィルタリング 612
9.5.3 プロキシ 613
9.5.4 お気に入り 615
9.6 証明書管理 616
9.6.1 クライアント証明書管理 616
9.6.2 クライアント証明書一括アップロード 620
9.6.3 クライアント証明書一括削除 622
9.6.4 CA 証明書管理 623
9.7 Zone Management 625
9.7.1 ゾーン 625
9.7.2 ポリシー 628
9.7.2.1 ［管理］タブ 628
9.7.2.2 ［Windows 設定］タブ 629
9.7.3 ゾーンポリシー構成 630

10 サービス環境設定 632
10.1 通知設定 633
10.2 アカウントポリシー 639
10.3 機器認証制御 641
10.4 ポータル表示 642
10.5 Android Enterprise（企業アカウント登録） 643
10.6 Apple Push 証明書 643
10.7 かんたん初期設定 644

11 ログ 645
11.1 ログ画面の見かた 646

12 サイトマップ 650
12.1 組織図 651
12.2 管理外機器エクスポート 652
12.3 ネットワーク 653
12.4 Android エージェント個別管理 658
12.5 Android リモートロック 659
12.6 Android リモートワイプ 662
12.7 Windows エージェント個別管理 664

1 Optimal Biz とは

この章では、製品の概要や動作環境などを説明します。

1.1 概要

本製品は、専門の知識を必要とせずに、機器の管理・運用を行うサポートサービスです。

機器の状態や位置情報を確認したり、管理サイトから端末のリモートロックやリモートワイプ（初期化）をしたりできます。管理サイトは特定のアプリをインストールすることなく、各パソコンのブラウザーから操作できます。

対応するブラウザーなどの動作環境は、事前にご確認ください。

「管理サイトの動作環境」15 ページ

1.2 特徴

本製品の特徴は、以下のとおりです。

●機器管理

管理サイトで、機器にユーザーやグループを設定すると、機器の資産管理を容易にできます。また、機器のバッテリー残量、デバイス容量、ハードディスク容量などを管理サイトから確認できます。

●リモートロック

機器を紛失してしまい手元にない場合も、管理サイトからロックできます。

●リモートワイプ

機器を紛失してしまった場合や所有者を変更するときなどに、管理サイトから機器のすべてのデータを削除し、初期化（原則、OS バージョンはそのまま）できます。

●アプリケーション禁止

Android 端末および Windows 端末に、端末の設定画面や端末にインストールされているアプリの起動を禁止できます。

●連絡先設定

Android 端末に、連絡先を機器で 1 件ずつ登録しなくても、管理サイトから一括で連絡先を登録できます。

1.3 管理サイトの役割

管理サイトの主な役割は、機器にリモートで設定変更や制御を行うことです。管理サイト操作を行う上で主となる要素の概念を以下で説明します。

●設定セット

・機器に対する設定や制御を定義したものです。この定義を「設定セット」と呼びます。
・管理サイトから設定セットの作成および対象機器への適用指示を行います。
・管理サイトから行った設定セットの適用指示は、管理サーバーと端末が同期を行うことで実際に反映されます。

●機器

・本製品が管理する主な対象です。
・機器分類やユーザーカスタム項目を作成しなくても単一指定および全指定での設定セットの適用ができます。

●機器カスタム項目（機器分類）

・機器に紐づけることができる情報です。機器カスタム項目単位で設定セットの一括適用ができるようになります。機器カスタム項目の作成については、以下を参照してください。

☞「入力項目のカスタマイズ」218 ページ

●ユーザー

・機器に紐づけることができる情報です。ユーザーの作成および機器への紐づけを行っても、ユーザー単位での設定セットの適用は行えませんが、紐づけたユーザーが所属する分類を用いた設定セットの一括適用ができるようになります。

●ユーザーカスタム項目（ユーザー分類）

ユーザーに紐づけることができる情報です。ユーザーに紐づけることによりユーザーカスタム項目単位で設定セットの適用ができるようになります。ただし、紐づけたユーザーが機器に紐づけられている場合に限ります。ユーザーカスタム項目の作成については、以下を参照してください。

☞「入力項目のカスタマイズ」271 ページ

1.4 管理サイトの動作環境

管理サイトは、以下の環境で利用できます。

項番	項目	動作環境
1	対応ブラウザー	以下のブラウザーに対応しています。 ●Microsoft Edge（Windows 版） ●Firefox ●Google Chrome Microsoft Edge（Windows 版）、Firefox、Google Chrome は最新版にのみ対応しています。 ディスプレイの解像度は、横 1,250 ピクセル以上の表示を推奨します。 対応ブラウザーのインストール方法や設定など、また OS に依存する設定については、対応いたしかねます。
2	ネットワーク接続	インターネットへ接続し、直接またはプロキシを介して管理サイトと HTTPS 通信（443 番ポート）ができる環境が必要です。
3	対応言語	以下の言語に対応しています。 ●日本語
4	Apple Configurator	Apple Configurator 2 対応 管理サイトからの編集は、画面上に存在する項目のみ対応しています。

2 基本操作

この章では、管理サイト画面の構成と各画面に共通する操作方法について説明します。

2.1 ログイン／ログアウト

管理サイトにログインの手順は、以下を参照してください。

『かんたん初期設定マニュアル』の「端末の管理を開始する」－「管理サイトにログインする」

パスワードの発行や更新、2 段階認証でのログイン、ログアウトの手順は、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「ログイン／ログアウト」

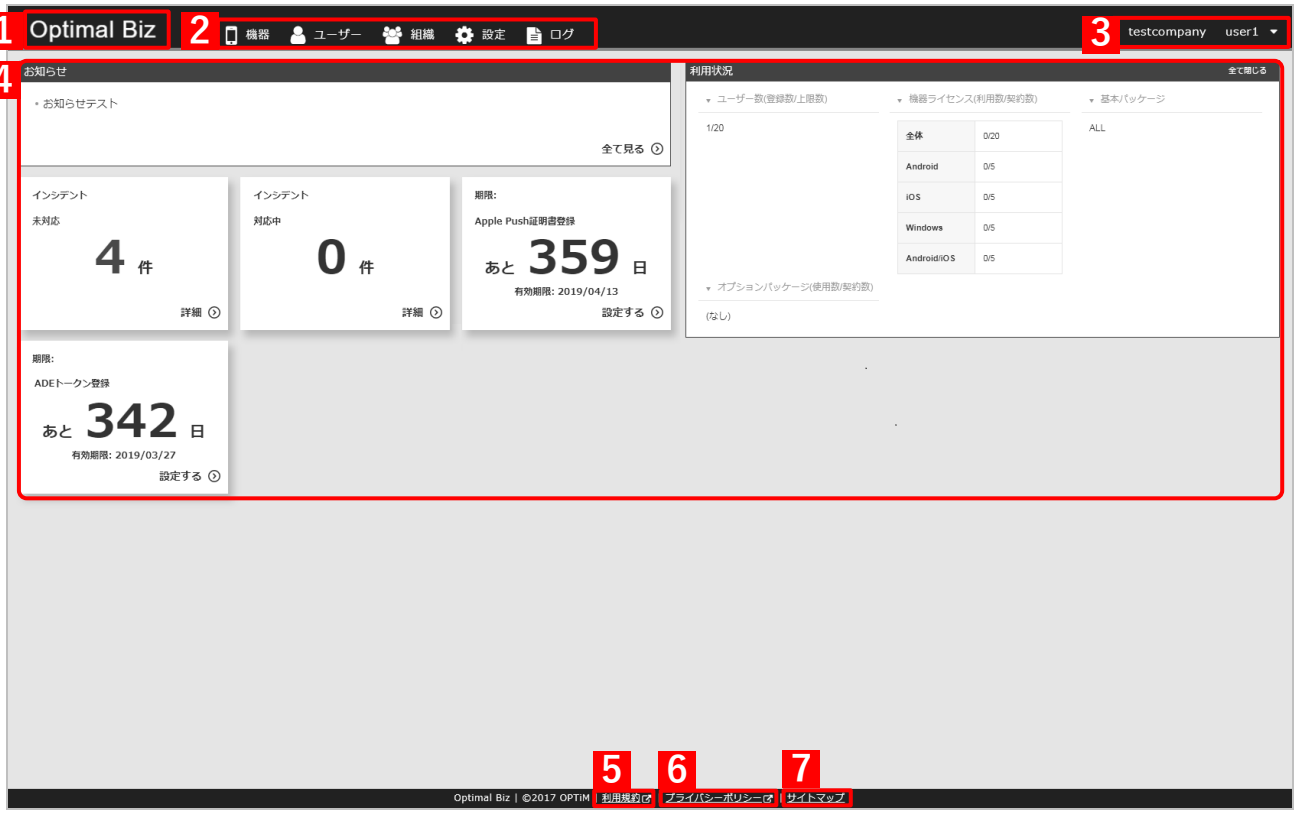
◆エラー一覧

文言	発生契機	対処方法
⚠ ログインしてください。	セッションが切れた状態でログインが必要なページを開いている。	再度ログインした状態でアクセスしてください。

2.2 管理サイト画面の構成

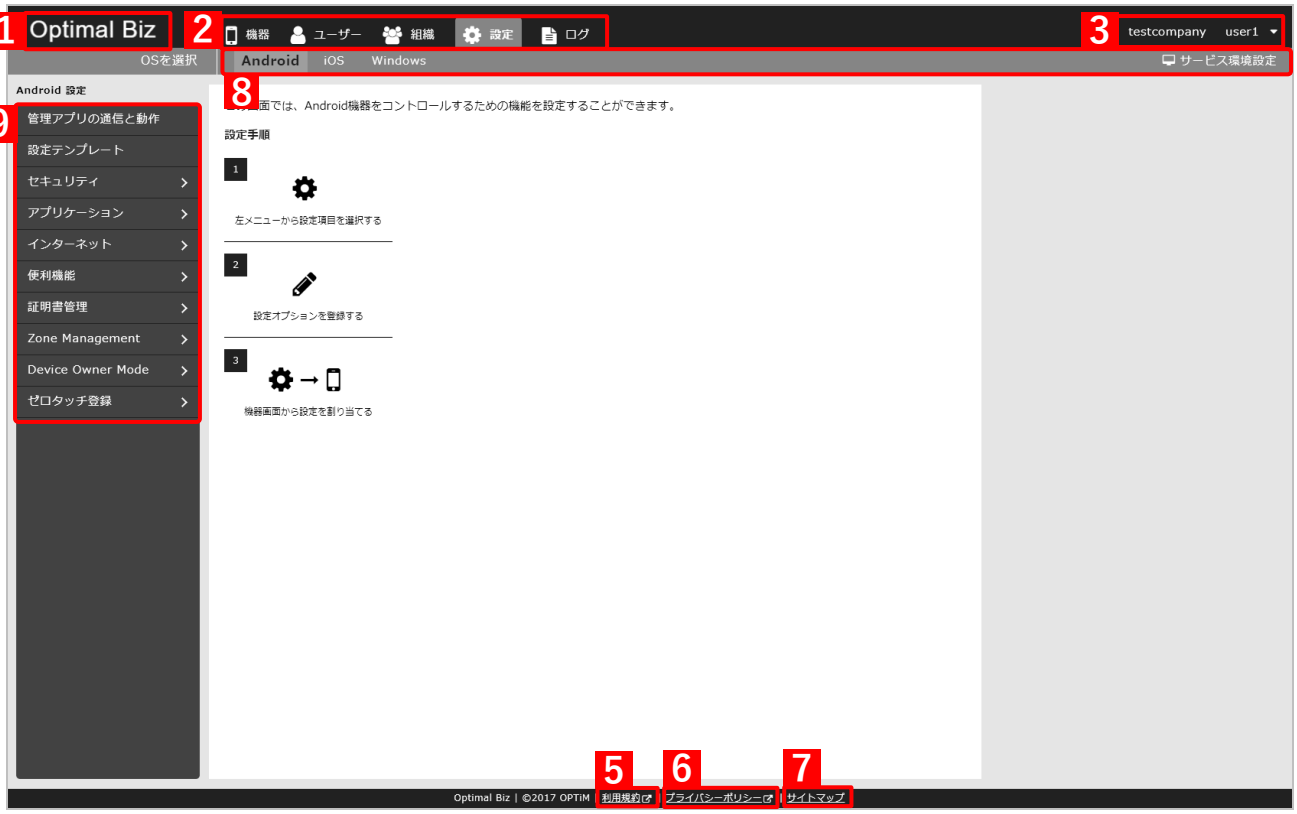
管理サイトの画面は、ダッシュボード画面と各種の設定画面で構成されています。

ダッシュボード



設定画面

画面はヘッダーメニューの［設定］画面を例に説明しています。



項番	名称	説明
1	製品名	製品名が表示されます。製品名をクリックすると、ダッシュボードに切り替わります。 「ダッシュボード」37 ページ
2	ヘッダーメニュー（※1）	［機器］、［ユーザー］、［組織］、［設定］、［ログ］をクリックすると、各カテゴリの画面に切り替わります。
3	ログイン情報	ログイン中の企業コードとユーザー名が表示されます。 ユーザー名をクリックすると、「個人設定」と「ログアウト」のメニューが表示されます。 「個人設定」49 ページ 『かんたん初期設定マニュアル』の「補足・便利な操作」－「ログイン／ログアウト」－「ログアウト」
4	ダッシュボード	ログイン後に表示されます。サービス企業からのお知らせや、インシデント、利用状況などを確認できます。 「ダッシュボード」37 ページ
5	利用規約	クリックすると、利用規約の画面が表示されます。
6	プライバシーポリシー	クリックすると、プライバシーポリシー一覧が表示されます。各［プライバシーポリシー］をクリックすることで、プライバシーポリシーの画面が表示されます。
7	サイトマップ	クリックすると、従来デザインのメニュー画面形式で、各種機能メニューが表示されます。サイトマップの詳細については、以下を参照してください。 「サイトマップ」650 ページ
8	サブヘッダーメニュー（※1）	ヘッダーメニューで［設定］をクリックした場合に表示されます。［Android］、［iOS］、［Windows］、［サービス環境設定］をクリックすると、各画面に切り替わります。
9	サイドメニュー（※1）	各カテゴリ、OS の画面のメニューが表示されます。メニューの右側に「＞」が表示されている場合は、クリックすると下の階層のメニューが表示されます。

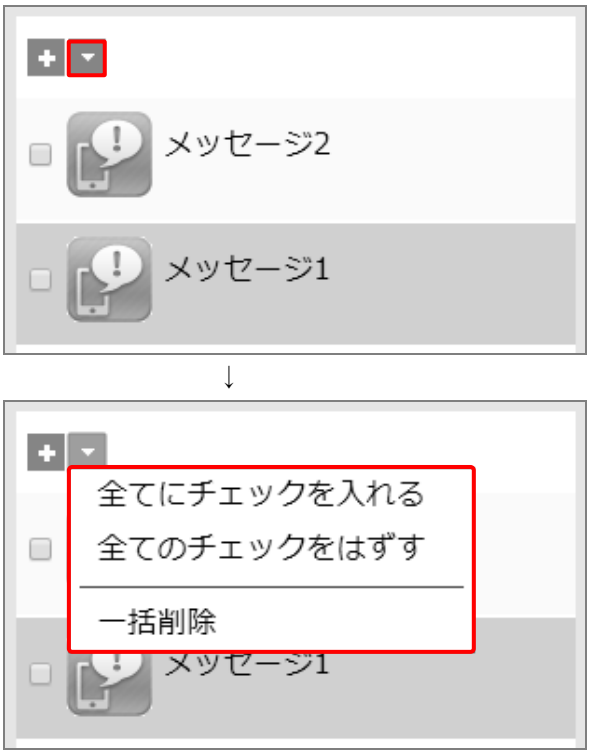
※1：以降、本マニュアルではこの名称を使い説明します。

2.3 管理サイトの共通操作

操作ボタンやメニューなど、共通の操作内容について説明します。

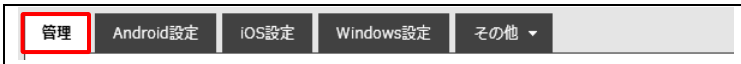
◆リストメニュー

［その他▼］、［操作▼］、 をクリックすると表示されるリストから、項目を選択します。

≪［その他▼］、［操作▼］の場合≫ 	［その他▼］をクリックすると、リストメニューが表示されます。 メニューをクリックすると、そのメニューの画面に切り替わります。 リストメニューに表示されるメニューは、機能によって異なります。
≪ の場合≫ 	をクリックすると、リストメニューが表示されます。 メニューをクリックすると、そのメニューが実行されます。 リストメニューに表示されるメニューは、機能によって異なります。

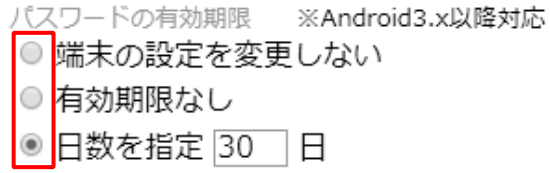
◆タブの切り替え

複数画面で構成されている画面は、タブをクリックして画面を切り替えます。

	表示する画面のタブをクリックすると画面が切り替わり、現在表示中のタブの色が白色に変わります。

◆ラジオボタン

必要な項目を 1 つだけ選択して設定します。

	項目に数値などの入力が必要な場合は、その項目を選択すると入力できるようになります。

◆チェックボックス

必要な項目にチェックを入れて設定します。

	クリックするたびに、チェックを入れたり、外したりできます。複数の項目にチェックを入れることができます。

◆テキストボックス

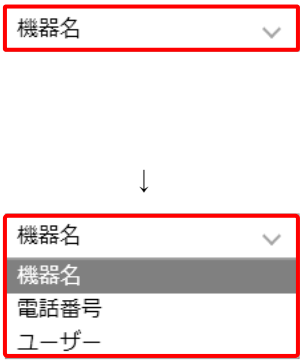
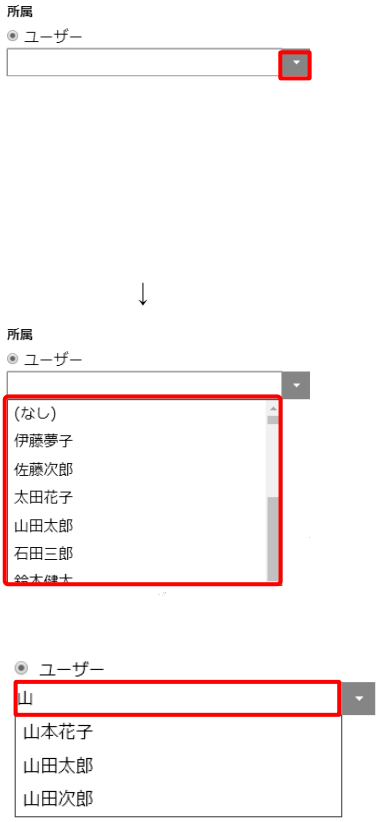
テキストボックス内に文字や数字を入力して設定します。

	テキストボックの中に、カーソルを置いてから、文字や数字を入力します。 入力する文字数や文字の種類は、項目によって異なります。 テキストボックスをクリックすると、項目が表示されて、選択できる場合があります。

◆リストボックス

リストボックスをクリックすると表示されるリストから、項目を選択します。

リストボックスには、以下の 2 種類があります。

≪リストボックス 1≫ 	リストボックスをクリックして、表示される項目から選択します。 文字の入力はできません。
≪リストボックス 2≫ 	をクリックして、表示される項目から選択します。 ボックスにキーワードを入力して、選択項目から該当する項目を絞り込んで表示してから選択できます。

◆ページ切り替え

一覧に表示する内容が複数ページに渡る場合は、以下の操作で表示するページを切り替えます。

	をクリックすると前のページが表示されます。 をクリックすると次のページが表示されます。 をクリックすると最初のページが表示されます。 をクリックすると最後のページが表示されます。 2 / 43 では、現在のページと総ページが表示されます。 テキストボックスにページを入力し、〈Enter〉キーを押すと、指定のページが表示されます。

◆スクロールバー

画面に表示できない部分がある場合に表示されます。

以下の操作で表示を切り替えます。

	バーの をスライドしたり、 や をクリックしたりすると、表示する部分を調節できます。

◆検索

キーワードを入力して対象を検索し、該当する項目を一覧に表示します。

すべての項目を一覧に再表示するには、テキストボックスにキーワードを入れないで をクリックするか、キーボードの〈F5〉キーを押します。

	テキストボックスにキーワードを入力して、キーボードの〈Enter〉キーを押すか、 をクリックすると、検索できます。 機能によっては、テキストボックスをクリックすると入力履歴のリストからキーワードを選択できる場合があります。

◆操作ボタン

編集、保存、検索、追加、削除などのボタンをクリックすると、画面によって必要な操作を行うことができます。

主な操作ボタンは以下のとおりです。

このほかのボタンについては、各画面の説明を参照してください。

ボタン	説明
（新規作成）	クリックすると、ユーザー、組織、各種設定などを新規作成画面が表示されます。
（追加）	クリックすると、設定行などが追加されます。
（削除）	クリックすると、該当の設定項目などが削除されます。
（編集）	クリックすると、該当の設定項目が編集できます。
（保存）	クリックすると、編集した内容が保存されます。
（取り消し）	クリックすると、編集した内容を取り消して、編集が終了します。
（検索）	ボタンの左側のテキストボックスにキーワードを入力して、クリックすると該当する項目を検索します。
（その他の操作）	クリックすると、リストメニューが表示されます。表示されるメニューの種類は機能によって異なります。
保存	クリックすると、設定内容が保存されます。
編集	クリックすると、編集画面に切り替わります。
取消	クリックすると、編集した内容を取り消して、編集が終了します。
	機器一覧やインシデント一覧で使用します。クリックすると、詳細画面が一覧の右側に表示されます。 「詳細情報の表示」35 ページ
	機器一覧やインシデント一覧の詳細画面で使用します。クリックすると、詳細画面を閉じます。
	機器一覧やインシデント一覧の詳細画面でメニューをクリックしたあとの画面で使用します。クリックすると、詳細画面に戻ります。
	カーソルを合わせると、対象の項目について、説明や注記などが表示されます。 Web サイト ver.9.12.0 以上の新機能の画面で表示されます。

2.4 設定画面の共通操作

設定画面で使われる基本的な操作手順について説明します。

各 OS によりボタンの配置などが異なりますが、同様の手順で操作することができます。

2.4.1 新規作成

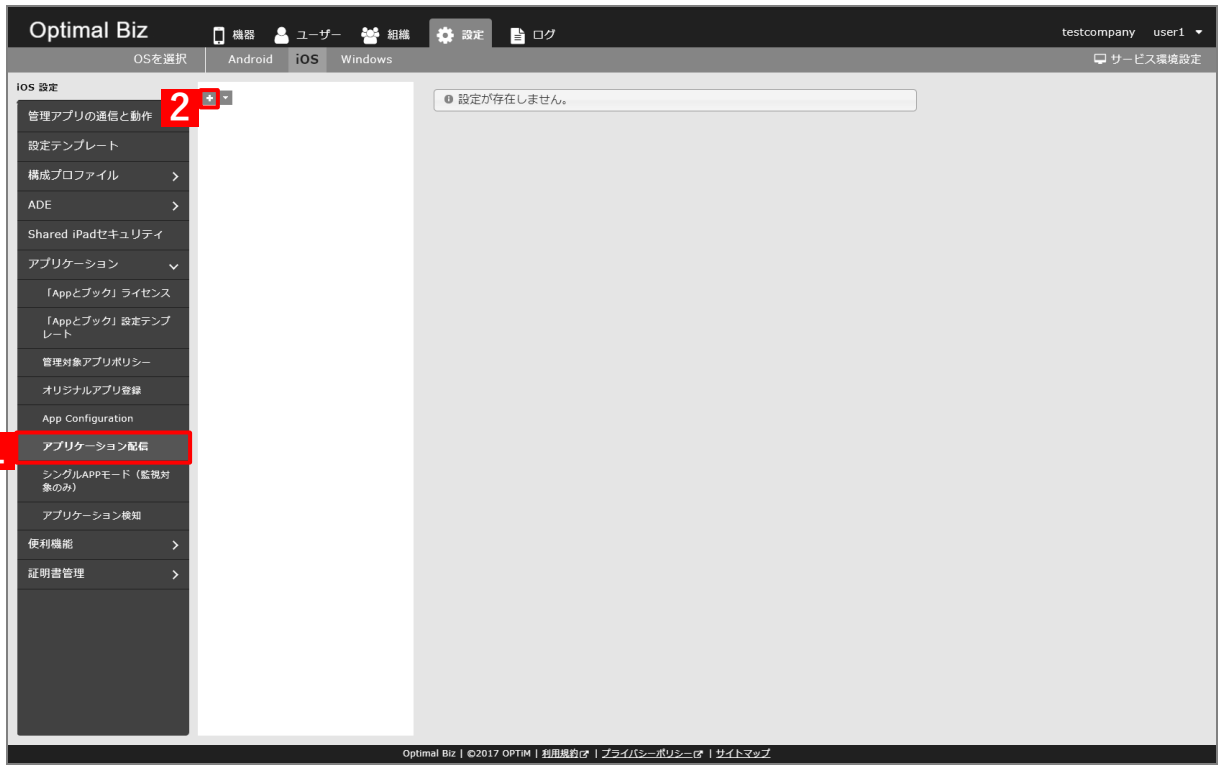
新規に設定を作成する手順について説明します。

ここでは、iOS のアプリケーション配信設定を例にしています。

【1】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。

【2】＋ をクリックします。

⇒新規作成画面が表示されます。



【3】各項目を設定します。

【4】［保存］をクリックします。

⇒設定が作成されます。

【5】作成された設定が、一覧に追加されたことを確認します。

2.4.2 編集

作成した設定を編集する手順について説明します。機能によっては、新規作成の画面と設定項目が異なる場合があります。

ここでは、iOS のアプリケーション配信設定を例にしています。

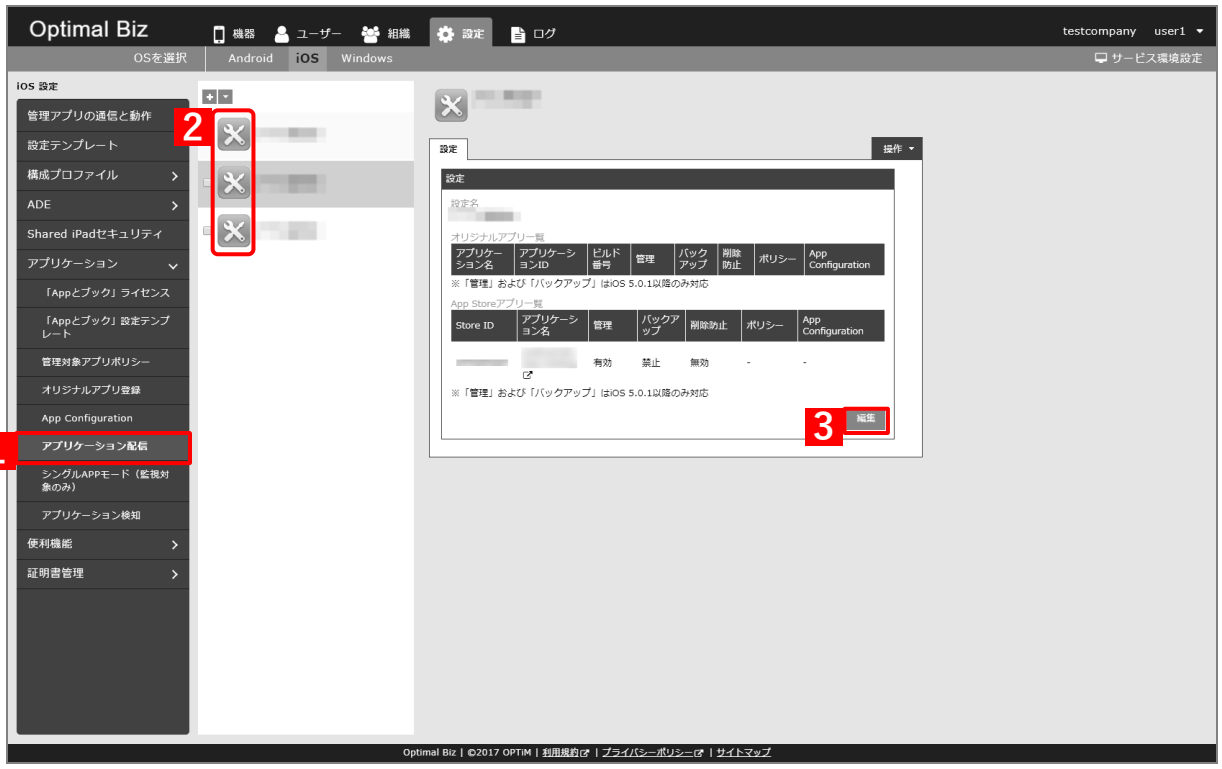
【1】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。

【2】一覧から対象を選択（ をクリック）します。

⇒右側に選択した設定の設定内容が表示されます。

【3】［編集］をクリックします。

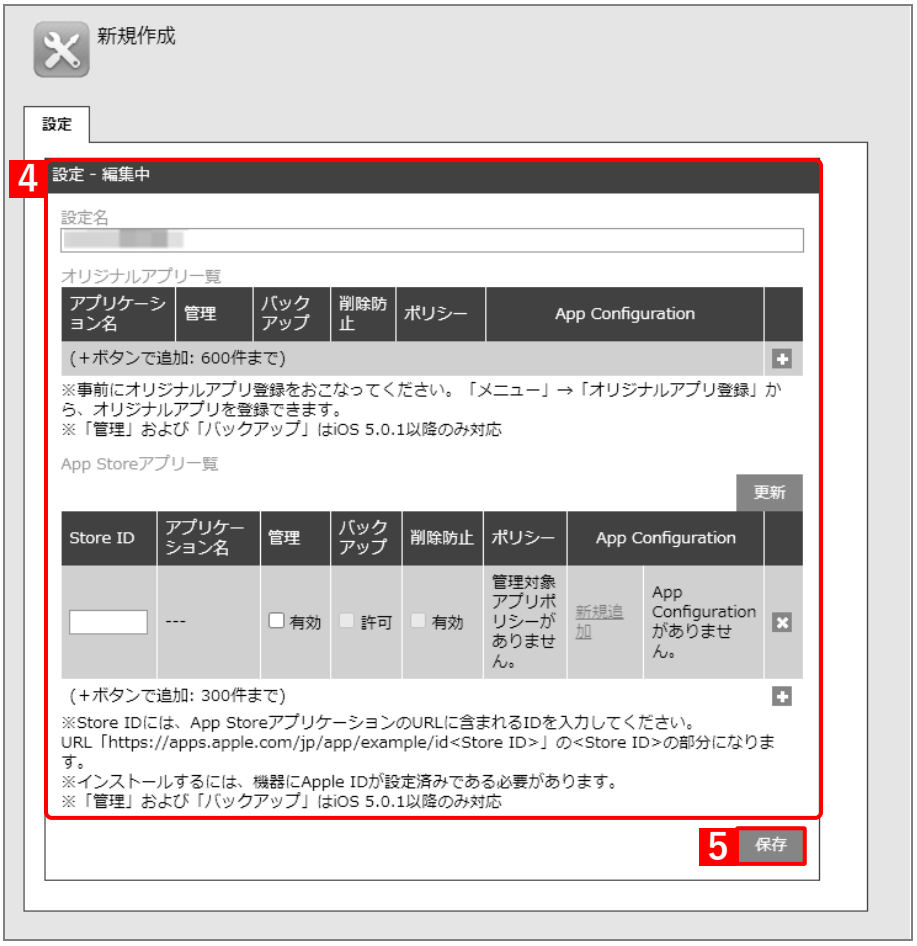
⇒編集画面に切り替わります。



【4】各項目を編集します。

【5】［保存］をクリックします。

⇒設定が保存されます。



2.4.3 複製

作成した設定を複製し、新しい設定を作成する手順について説明します。

ここでは、iOS のアプリケーション配信設定を例にしています。

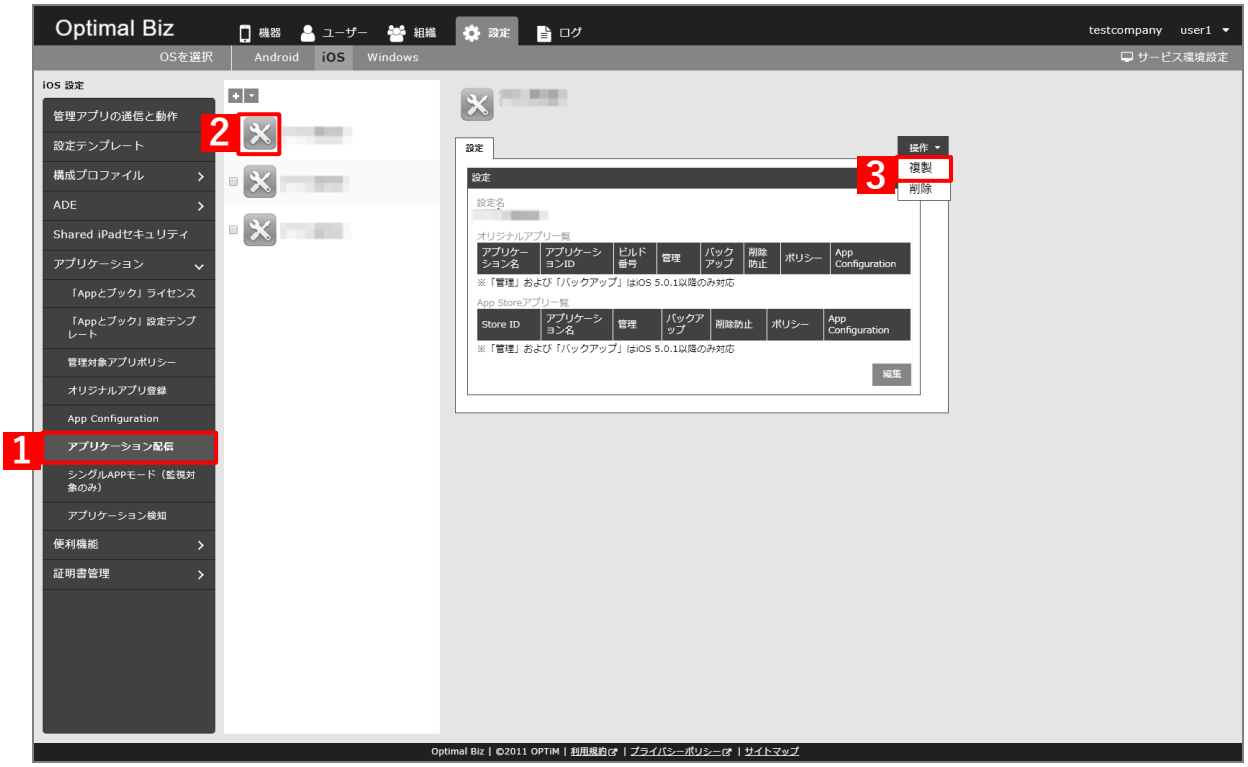
【1】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。

【2】一覧から複製元にする設定を選択（ をクリック）します。

⇒右側に選択した設定の設定内容が表示されます。

【3】［操作］→［複製］をクリックします。

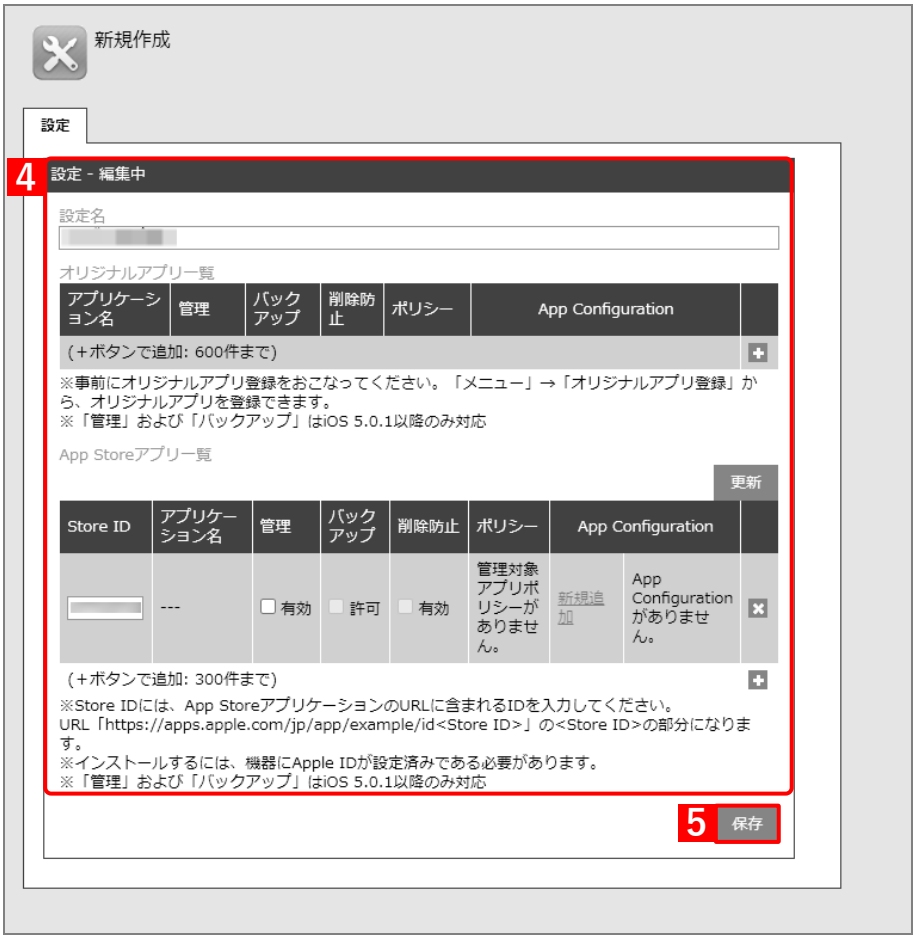
⇒設定を複製し、新規作成画面に切り替わります。



【4】複製された設定内容を編集します。

【5】［保存］をクリックします。

⇒設定が作成されます。



【6】作成された設定が、一覧に追加されたことを確認します。

2.4.4 削除

設定を削除する手順について説明します。

ここでは、iOS のアプリケーション配信設定を例にしています。

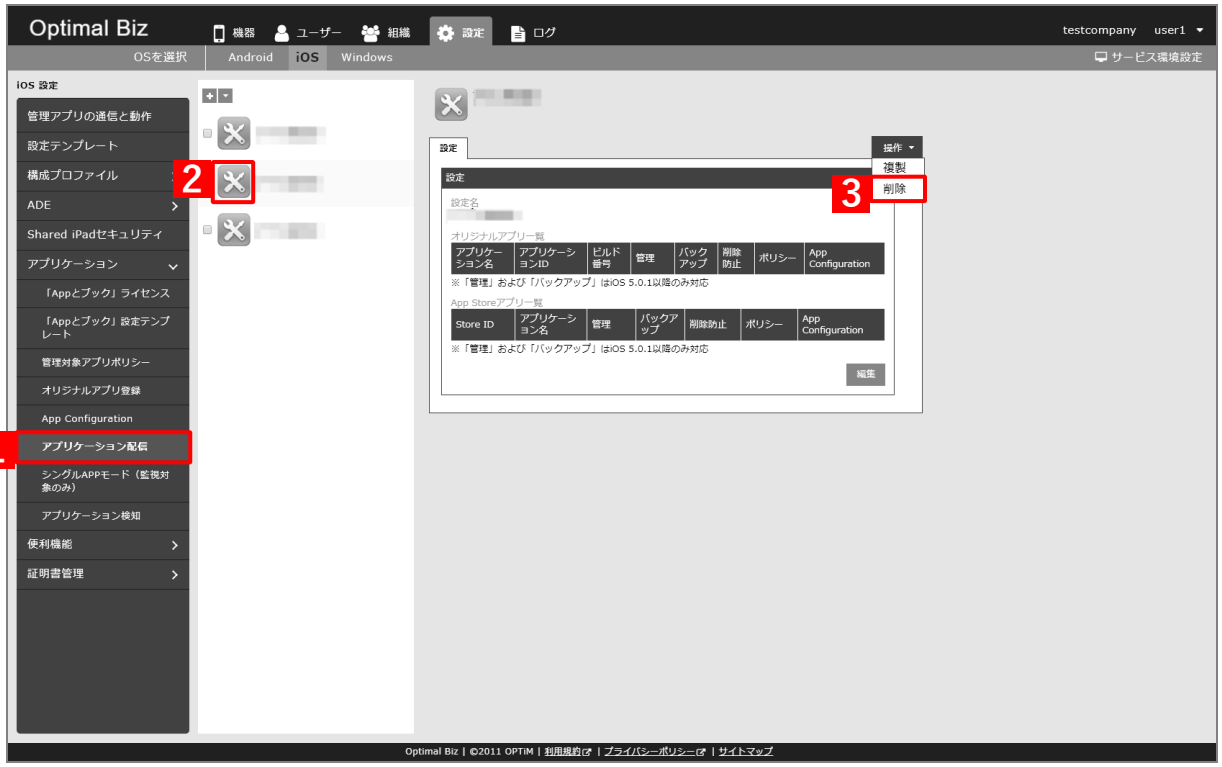
【1】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。

【2】一覧から削除する設定の を選択します。

⇒右側に選択した設定の設定内容が表示されます。

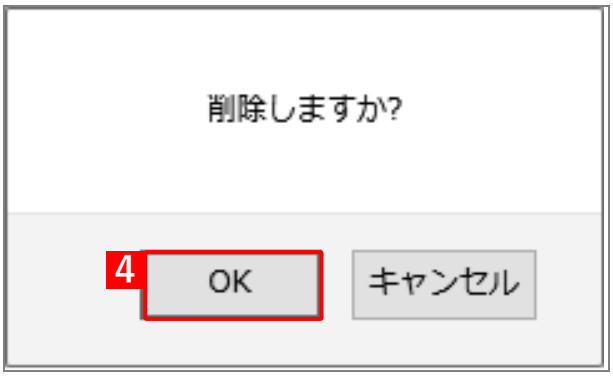
【3】［操作］→［削除］をクリックします。

⇒削除の確認メッセージが表示されます。



【4】［OK］をクリックします。

⇒設定が削除されます。



2.4.5 一括削除

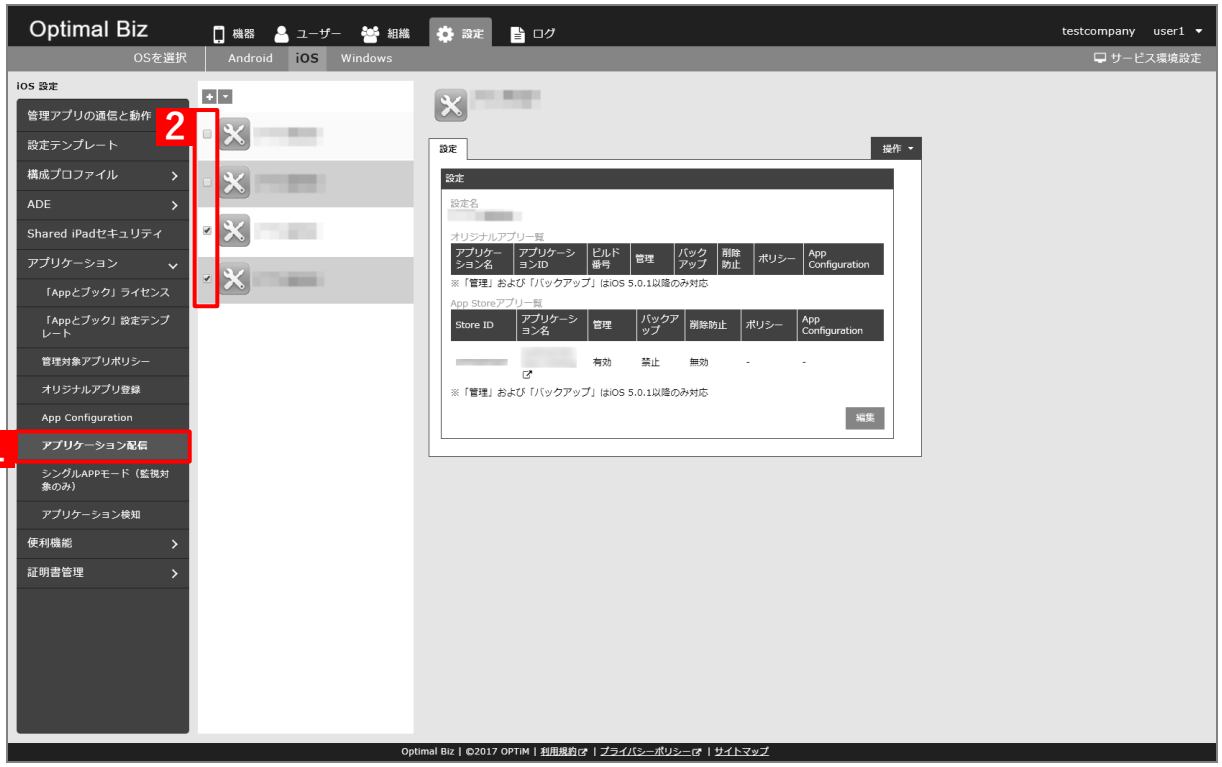
不要な設定をすべて選択し、一括で削除する手順について説明します。

ここでは、iOS のアプリケーション配信設定を例にしています。

【1】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。

【2】削除する設定にチェックを入れます。

すべての設定にチェックを入れたり、外したりするには、▼ →［全てにチェックを入れる］または［全てのチェックをはずす］をクリックします。



【3】▼ →［一括削除］をクリックします。

⇒削除の確認メッセージが表示されます。

【4】［OK］をクリックします。

⇒チェックを入れた設定が、一括で削除されます。

2.4.6 一覧項目の操作

設定画面に表示される、アプリや連絡先などの一覧項目の操作手順について説明します。

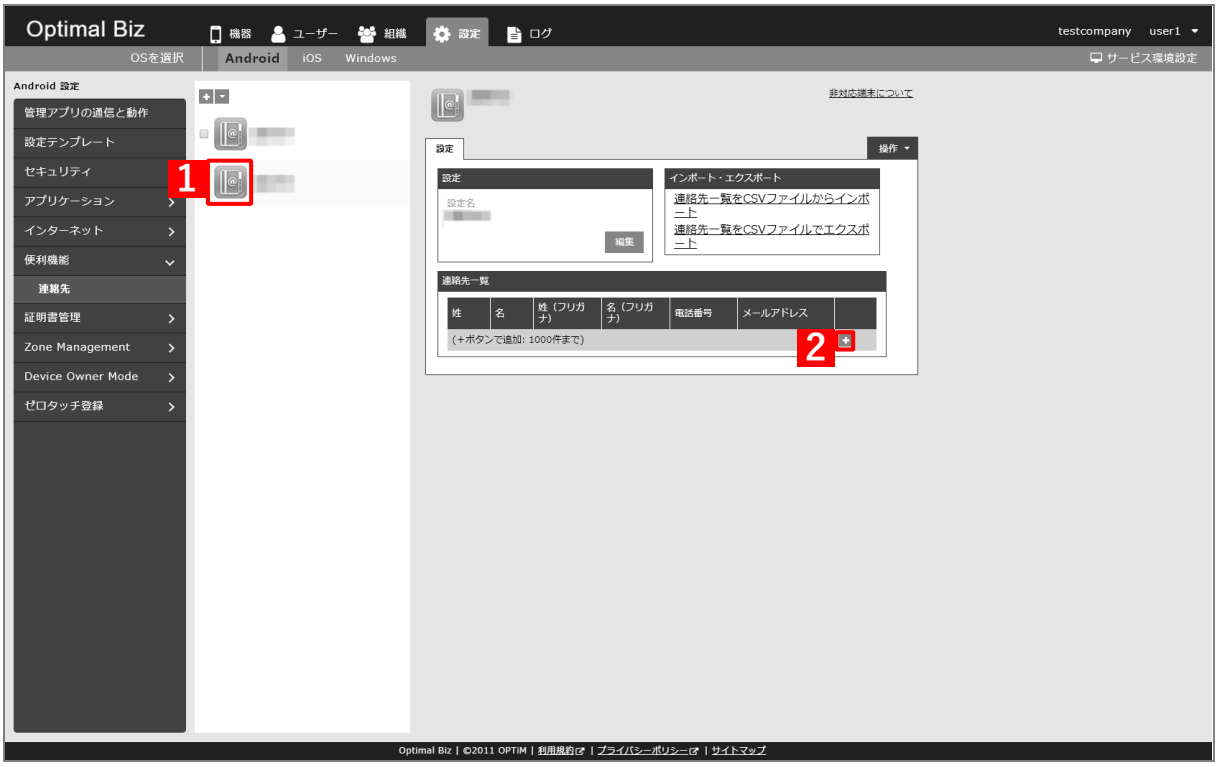
ここでは、Android の連絡先一覧を例にしています。

設定画面によっては、追加と削除だけの場合もあります。

【1】［設定］→［Android］→［便利機能］→［連絡先］→一覧から対象を選択します。

【2】「連絡先一覧」の ＋ をクリックします。

⇒連絡先の登録行が 1 行追加されます。



【3】連絡先情報を入力します。

【4】 ✓ をクリックします。

現在の操作を取り消したい場合は、（A） ↩ をクリックします。
追加登録の場合は追加を取り消し、編集の場合は編集を取り消し、操作する前の状態に戻ります。

【5】保存した連絡先を確認します。

登録した内容を編集するには、（A）　をクリックします。

登録した内容を削除するには、（B）　をクリックし、確認画面で［OK］をクリックします。

2.4.7 詳細情報の表示

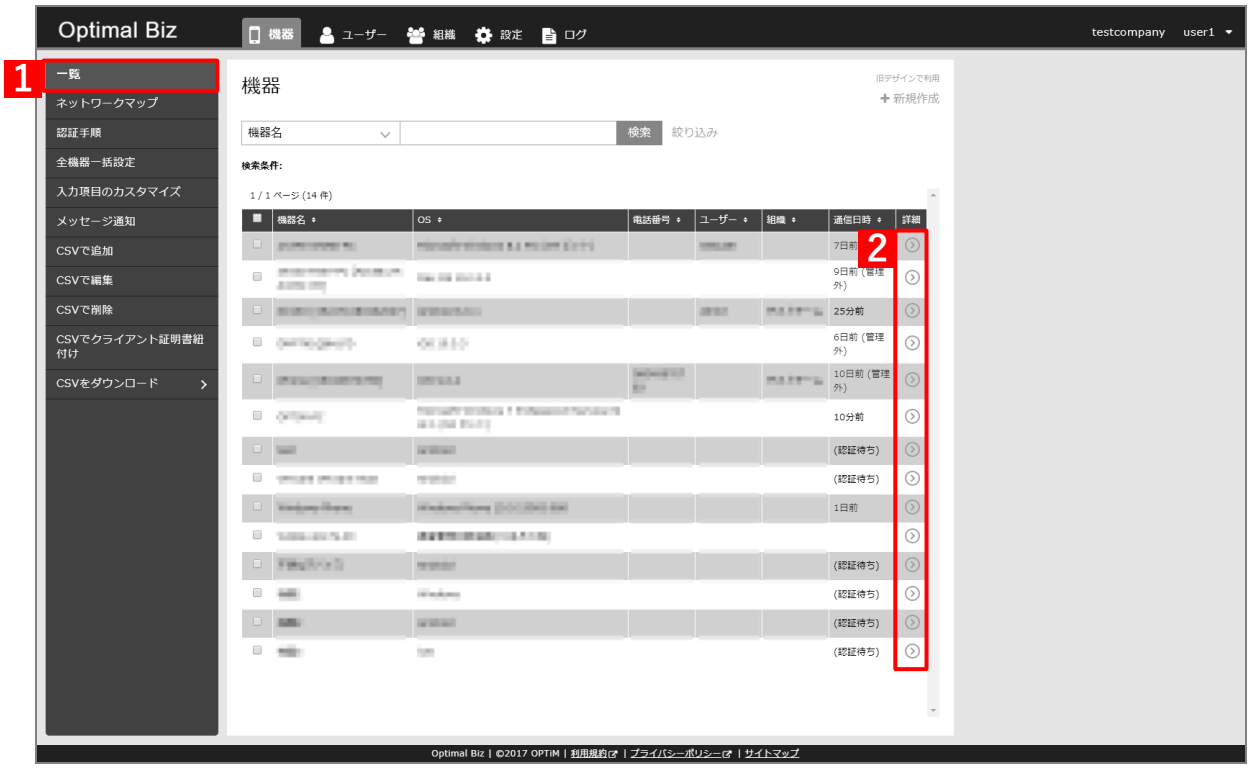
［機器］の［一覧］や［インシデント］画面などから詳細画面を表示する手順について説明します。

ここでは、［機器］の［一覧］を例にしています。

【1】［機器］→［一覧］をクリックします。

【2】詳細を確認する機器の「詳細」の ⓘ をクリックします。

⇒機器一覧の右側に詳細画面が表示されます。



【3】詳細情報を確認します。

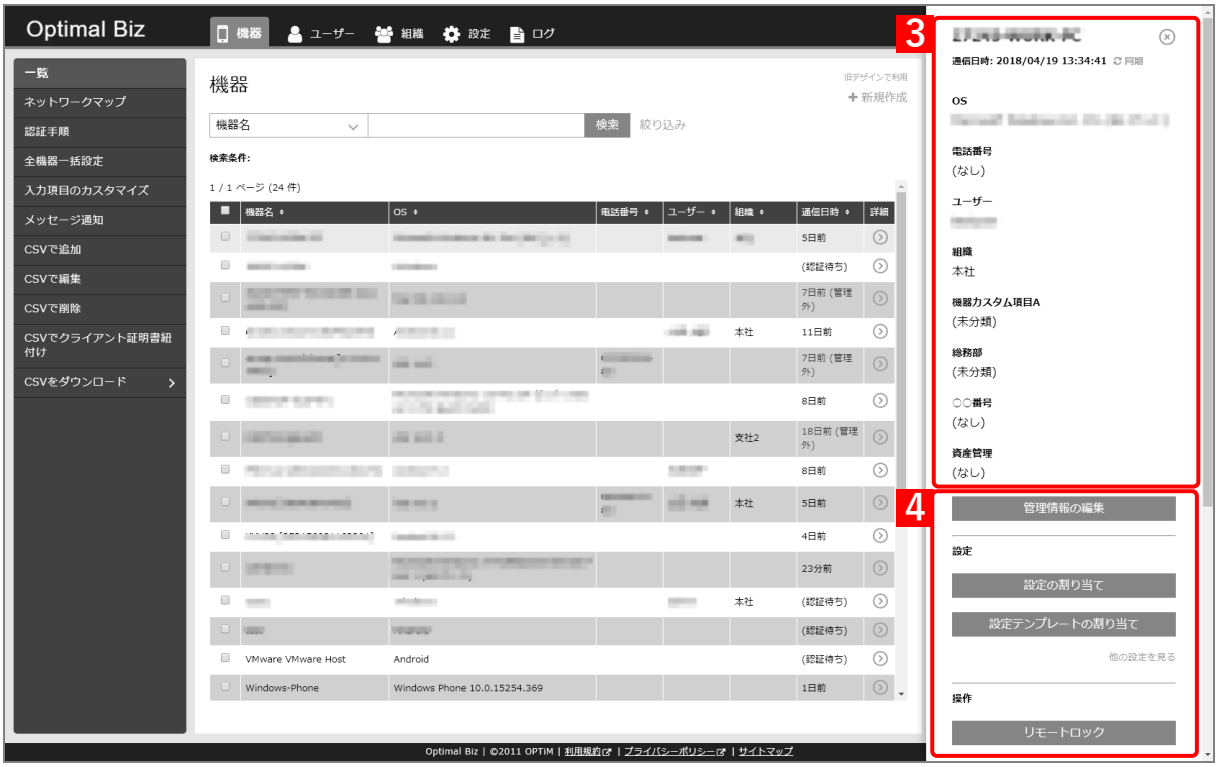
表示される項目は、一覧の種類によって異なります。

詳細画面を閉じる場合は、 をクリックするか、「詳細」の を再度クリックします。

【4】必要に応じて各種操作をします。

操作できるメニューは、一覧の種類によって異なります。

表示されていないメニューを表示するには、［他の○○を見る］をクリックします。
メニューをクリックしたあとの画面で をクリックすると、詳細画面に戻ります。



3 ダッシュボード

この章では、ダッシュボードに表示される各種の情報やダッシュボードから設定する内容について説明します。

3.1 ダッシュボードの画面構成

ダッシュボードは管理サイトにログインすると表示され、「お知らせ」や「利用状況」など各種の情報を確認できます。また、ヘッダーメニューから、［機器］、［ユーザー］、［組織］、［設定］、［ログ］などの設定画面を表示することができます。

◆画面

表示操作 ログイン画面でログイン情報入力→［ログイン］

項番	項目	説明
1	製品名	製品名が表示されます。 ダッシュボード以外の画面で製品名をクリックすると、ダッシュボードに切り替えることができます。
2	ヘッダーメニュー	［機器］、［ユーザー］、［組織］、［設定］、［ログ］をクリックすると、各カテゴリの画面に切り替わります。
3	お知らせ	サービス企業からの連絡内容が表示されます。詳細については、以下を参照してください。 「お知らせ」40 ページ サービス企業の設定によっては、お知らせ欄が表示されない場合があります。
4	インシデント 未対応	未対応のインシデント件数が表示されます。 1 件以上ある場合は件数が赤字で表示されます。 クリックすると、インシデント画面が表示されます。
5	インシデント 対応中	対応中のインシデント件数が表示されます。 クリックすると、インシデント画面が表示されます。

項番	項目	説明
6	期限： Apple Push 証明書登録	Apple Push 証明書の状態および有効期限を表示します。 ●状態 Apple Push 証明書の状態が、以下のいずれかで表示されます。 ・未設定 Apple Push 証明書を登録していない場合に表示されます。 ・あと XXX 日 Apple Push 証明書の有効期限が切れるまでの残日数が表示されます。 ●有効期限 Apple Push 証明書が登録されている場合は、有効期限が表示されます。 クリックすると、Apple Push 証明書の登録画面が表示されます。詳しい内容は、以下を参照してください。 『Apple Push 証明書年次更新マニュアル』
7	期限： ADE トークン登録	ADE トークンの状態および有効期限を表示します。 ●状態 ADE トークンの状態が、以下のいずれかで表示されます。 ・未設定 ADE トークンを登録していない場合に表示されます。 ・あと XXX 日 ADE トークンの有効期限が切れるまでの残日数が表示されます。 ●有効期限 ADE トークンが登録されている場合は、有効期限が表示されます。 クリックすると、ADE トークンの登録画面が表示されます。詳しい内容は、以下を参照してください。 ☞「ADE トークン登録」503 ページ
8	かんたん初期設定	クリックすると本製品導入時の初期設定作業を簡略化する「かんたん初期設定」を開始します。かんたん初期設定の詳細については、以下を参照してください。 ☞「かんたん初期設定」644 ページ 以下の条件を満たす場合に表示します。 ●認証済みの機器がない場合 ●ログインしているユーザーの種別が「管理者」または「操作」
9	利用状況	以下の状況が表示されます。 ●ユーザー数（登録数/上限数） ユーザーの作成状況をグラフと数値で表示します。最大 50,000 ユーザーまで作成できます。ユーザーの新規作成は、以下を参照してください。 ☞「［管理］タブ」257 ページ ●機器ライセンス（利用数/契約数） 機器の作成状況をグラフと数値で表示します。最大 50,000 機器まで作成できます。機器の新規作成は、以下を参照してください。 ☞「機器の新規作成」61 ページ ●基本パッケージ 利用できる基本機能です。すべての機器で、ご利用いただけます。 ●オプションパッケージ（使用数/契約数） 利用できるオプション機能と利用状況をグラフと数値で表示します。オプションパッケージを割り当てた機器でのみ、ご利用いただけます。 使用数が契約数に達している場合は、新たにオプションパッケージを割り当てることができません。 機器へのオプションパッケージ割り当ては、以下を参照してください。 ☞「（設定－Android）パッケージ」78 ページ

3.2 お知らせ

サービス企業からの連絡内容が表示されます。サービス企業での設定により表示内容は異なります。

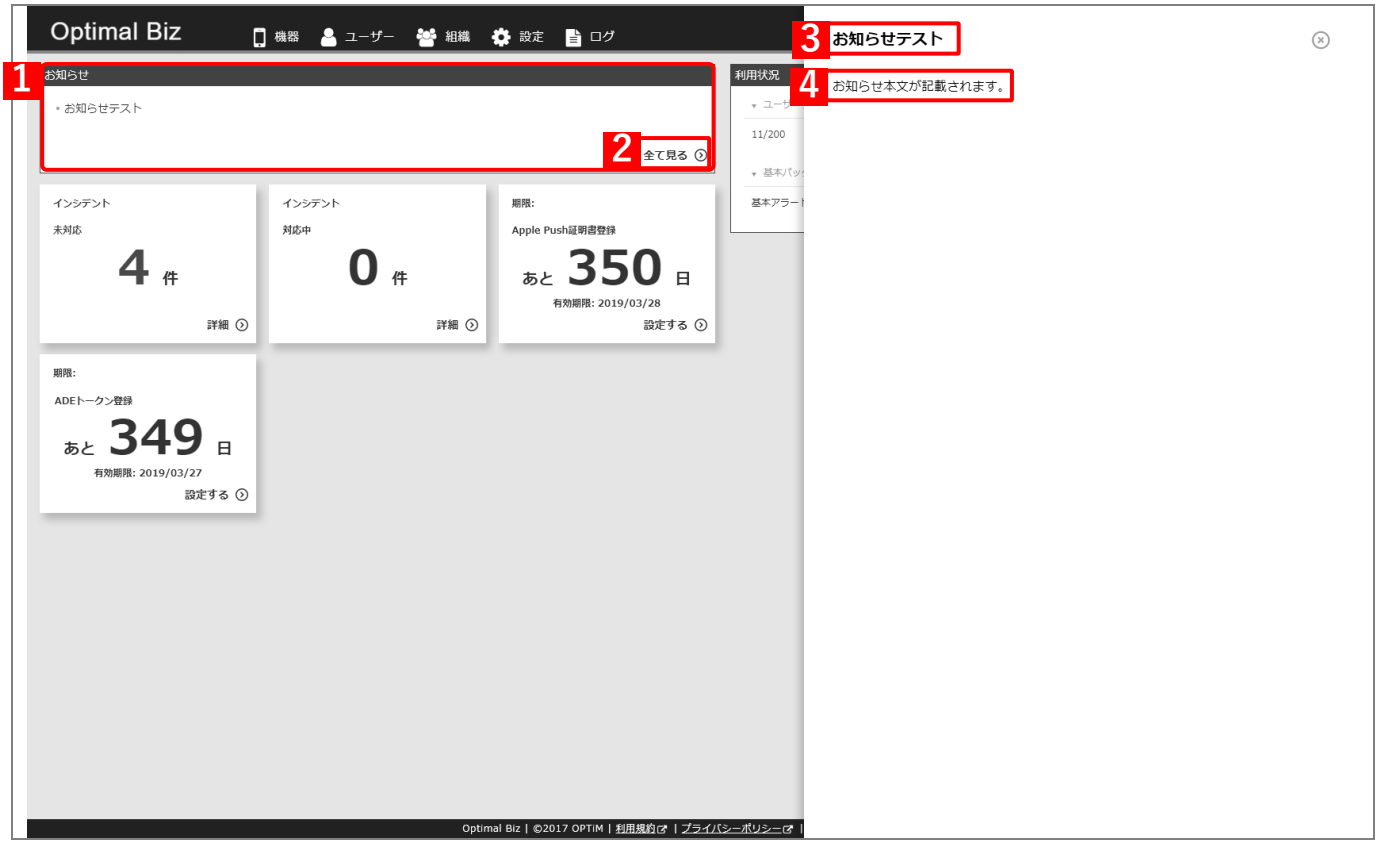
画面

画面（全て見る）

サービス企業の設定によっては、「お知らせ」が表示されない場合もあります。

◆画面

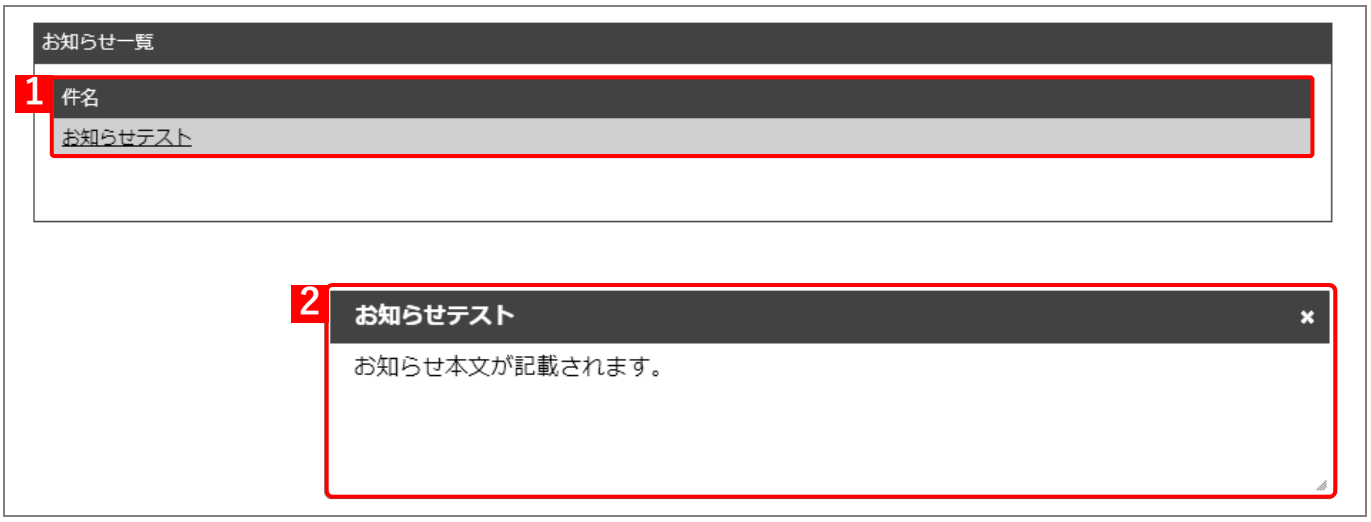
表示操作 ダッシュボードの「お知らせ」でお知らせの件名を選択



項番	項目	説明
1	お知らせ	お知らせの件名が表示されます。件名をクリックすると、お知らせの内容が表示されます。この画面では、4 件までのお知らせが表示されます。それ以外のお知らせは、「全て見る」をクリックすると確認いただけます。
2	全て見る	クリックすると、すべてのお知らせを表示します。 「画面（全て見る）」41 ページ
3	件名	お知らせの件名が表示されます。
4	お知らせ内容	お知らせの内容が表示されます。

◆画面（全て見る）

表示操作　ダッシュボードの「お知らせ」の［全て見る］→お知らせの件名を選択



項番	項目	説明
1	件名	お知らせの件名の一覧が表示されます。件名をクリックすると、お知らせの内容の画面が表示されます。
2	内容	お知らせの件名と内容が表示されます。

3.3 インシデント

ダッシュボードに表示されているインシデントを一覧で表示します。インシデントの対象の設定、およびインシデントに該当する端末について対応状況を管理できます。

画面

画面（絞り込み）

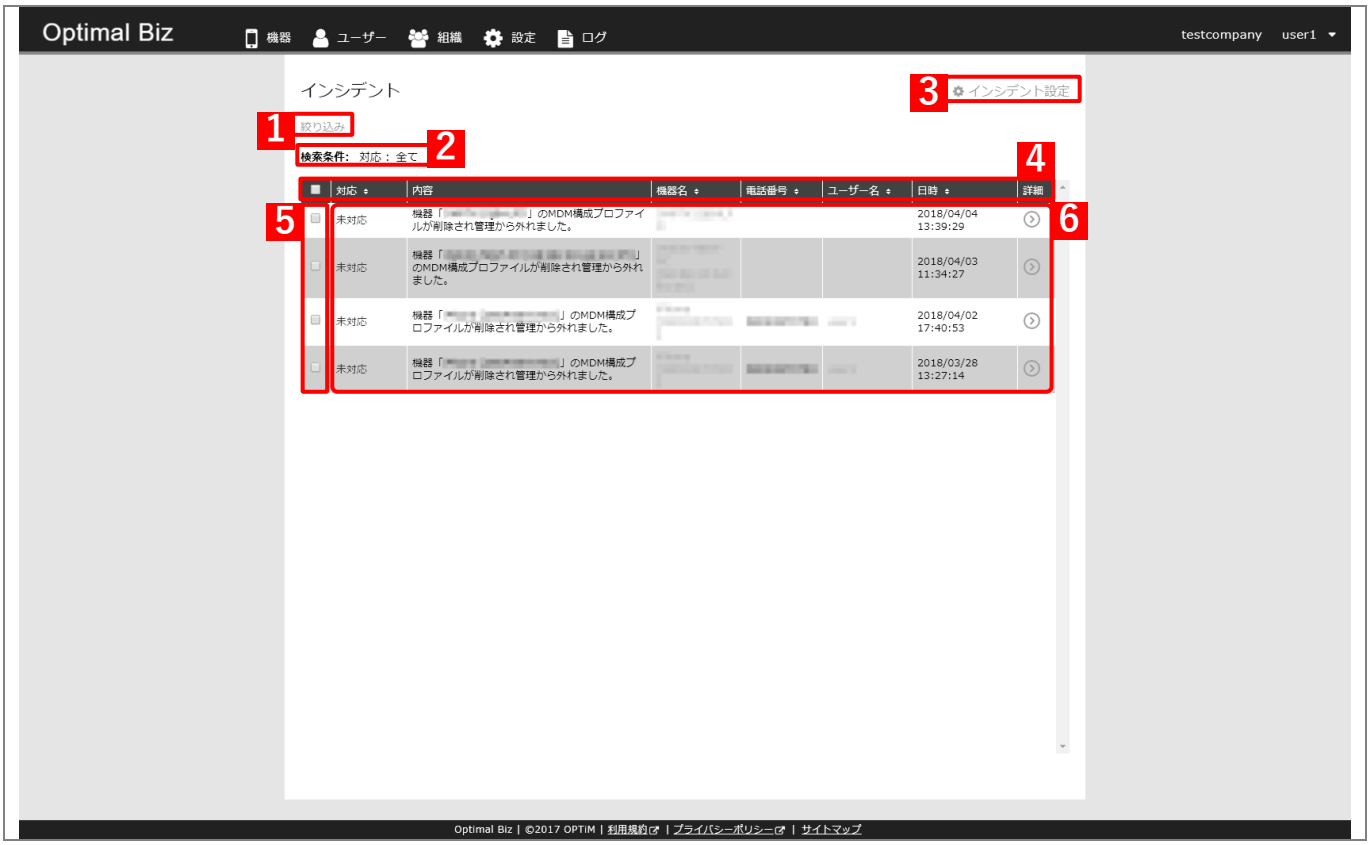
画面（対応の変更）

インシデントの対象を設定するには、以下を参照してください。

「インシデント設定」46 ページ

◆画面

表示操作　ダッシュボードで［インシデント　対応中］もしくは、［インシデント　未対応］をクリック

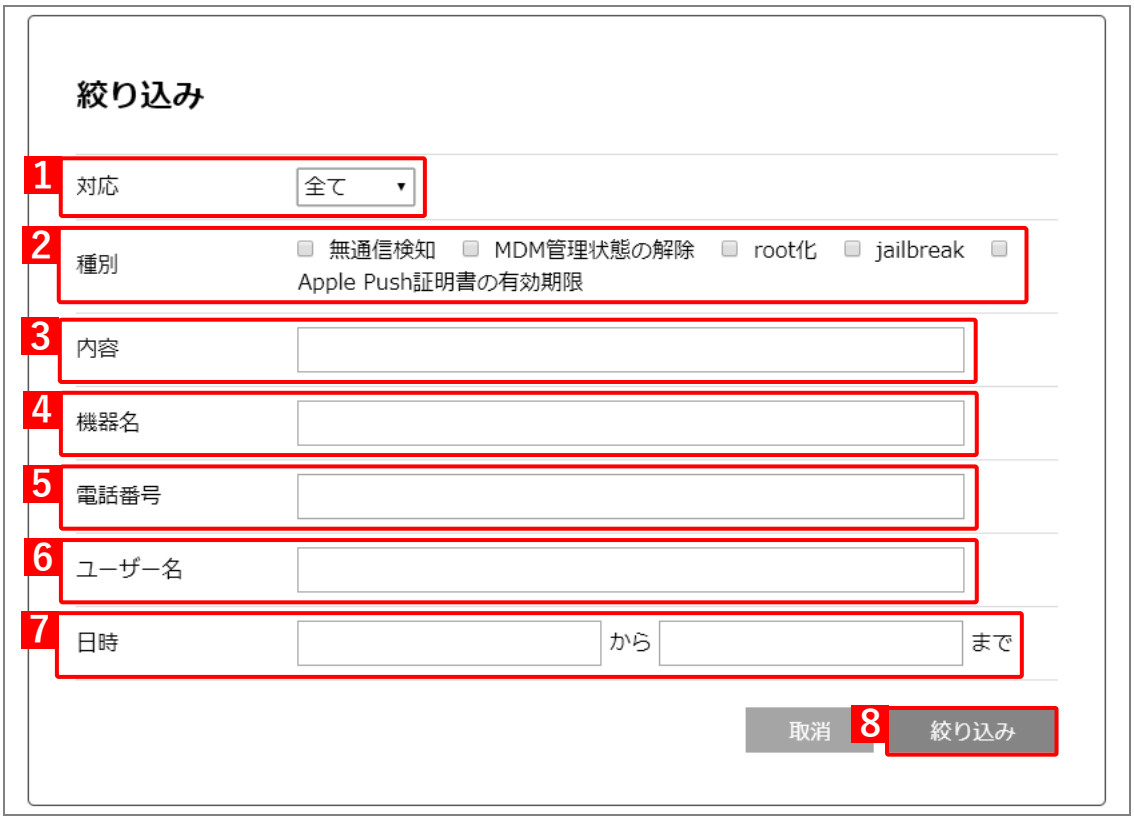


項番	項目	説明
1	［絞り込み］	クリックすると、絞り込み条件を選択する画面が表示されます。詳細については、以下を参照してください。 「画面（絞り込み）」44 ページ
2	検索条件：	現在の検索条件が表示されます。
3	インシデント設定	インシデントの対象を指定します。詳細については、以下を参照してください。 「インシデント設定」46 ページ
4	見出し項目	各項目の見出しをクリックするたびに、インシデント一覧がその項目の昇順、降順に並び変わります。 「内容」の見出し項目での、並べ替えはできません。

項番	項目	説明
5	チェックボックス	複数のインシデントの対応をまとめて変更する場合に、対象のインシデントにチェックを入れます。 チェックを入れると、一覧画面の下にインシデントの対応をまとめて変更する画面が表示されます。詳細については、以下を参照してください。 「画面（対応の変更）」45 ページ
6	インシデント一覧	以下の項目が表示されます。 ●対応 インシデントのステータスが表示されます。 ●内容 インシデントに対応するログが表示されます。 ●機器名 インシデントが発生した機器名が表示されます。クリックすると、機器画面が表示されます。 ●電話番号 インシデントが発生した機器の電話番号が表示されます。 複数の電話番号を持つ端末は、端末が保持している電話番号のうち、いずれか 1 つが「電話番号」列に表示されます。 表示されていない他の電話番号は、をクリックすると表示される詳細画面で確認することができます。 端末が保持している他の電話番号で検索した場合は、検索結果に検索した電話番号が表示されないことがあります。 ●ユーザー名 インシデントが発生した機器に紐づいているユーザー名が表示されます。 ●日時 インシデントが発生した日時が表示されます。 ●詳細 をクリックすると、各インシデントの詳細画面が表示されます。表示される画面については、以下を参照してください。 「インシデントの詳細画面」47 ページ

◆画面（絞り込み）

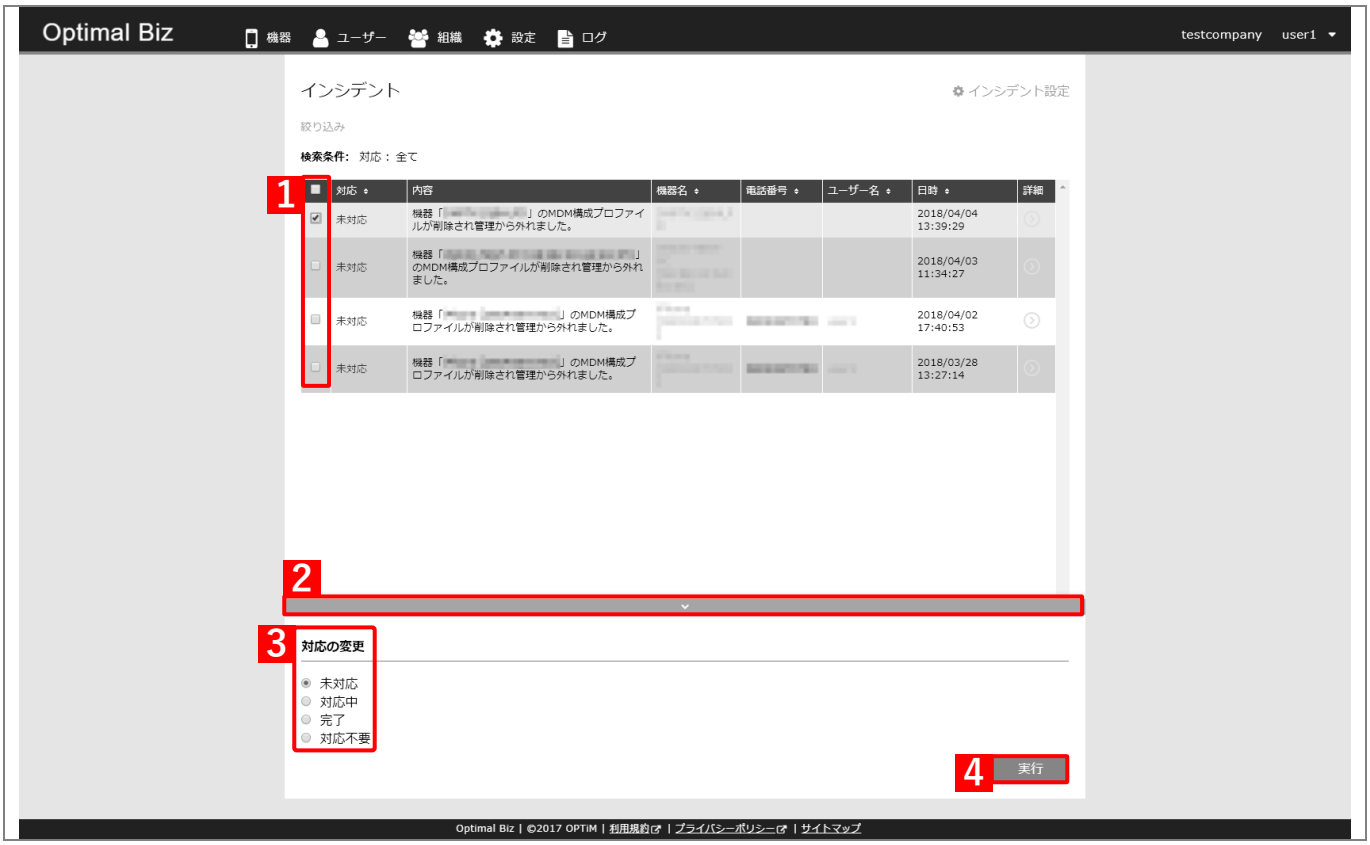
表示操作 ダッシュボードで［インシデント］→［絞り込み］



項番	項目	説明
1	対応	対応の状態で絞り込みを行う場合に、リストボックスから対応を選択します。
2	種別	インシデントの種別で絞り込みを行う場合に、対象にチェックを入れます。
3	内容	インデントの内容で絞り込みを行う場合に、テキストボックスに内容に含まれるキーワードを入力します。
4	機器名	機器名で絞り込みを行う場合に、テキストボックスに機器名に含まれるキーワードを入力します。
5	電話番号	電話番号で絞り込みを行う場合に、テキストボックスに電話番号（番号の一部分も可）を入力します。
6	ユーザー名	ユーザー名で絞り込みを行う場合に、テキストボックスにユーザー名に含まれるキーワードを入力します。
7	日時	インシデントの発生日時を範囲指定して絞り込む場合に、日時を入力します。 日時の入力欄をクリックするとカレンダーが表示され、日付、時間を設定できます。入力欄に直接入力もできます。 範囲は「から」と「まで」のいずれか日時だけでも検索できます。
8	［絞り込み］	クリックすると、条件に合ったインシデントの絞り込み検索が実行され、検索結果がインシデントの一覧に表示されます。 再度すべてのインシデントを表示するには、以下のいずれかを行う必要があります。 ・表示しているブラウザーを更新してください。 ・絞り込みの「対応」で「全て」を選択し、「種別」のすべてにチェックを入れた状態で［検索］をクリックします。

◆画面（対応の変更）

表示操作　ダッシュボードで［インシデント］→対応を変更するインシデントにチェックを入れる



項番	項目	説明
1	チェックボックス	インシデントの対応を変更する機器にチェックを入れます。チェックを入れると、一覧の下に操作メニューが表示されます。 見出し行にあるチェックボックスをクリックすると、すべての機器にチェックを入れたり、外したりできます。
2	／	クリックするたびに操作メニューを閉じたり、表示したりします。
3	対応の変更	チェックしたインシデントに設定する対応を以下から選択します。 ●未対応 対応していない場合に選択します。 インシデント機能で検知したときは、初めにこのステータスが設定されています。 ●対応中 インシデントの内容に対応中の場合に選択します。 ●完了 インシデントの内容について対応が完了した場合に選択します。 ●対応不要 確認の結果対応が不要と判断した場合に選択します。
4	［実行］	チェックを入れたインシデントの対応を一括で変更します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●個別にインシデントの対応を変更する方法については、以下を参照してください。 「インシデントの詳細画面」47 ページ

3.3.1 インシデント設定

インシデントとして検知する対象を設定します。

◆画面

表示操作　ダッシュボードで［インシデント］→［インシデント設定］

項番	項目	説明
1	無通信検知	チェックを入れると、以下のログがインシデントの対象に設定されます。 ・機器「機器名」の通信が最終通信日時から指定期間以上ありませんでした。 「期間を設定」をクリックすると、無通信検知の期間を編集する画面を表示します。 ☞「通知設定」633 ページ
2	MDM 管理状態の解除	チェックを入れると、以下のログがインシデントの対象に設定されます。 ・機器「機器名」の MDM 構成プロファイルが削除され管理から外れました。 iOS のみ対応しています。
3	root 化	チェックを入れると、以下のログがインシデントの対象に設定されます。 ・機器「機器名」のエージェントが端末の root 化を検知しました。 Android のみ対応しています。
4	Jailbreak	チェックを入れると、以下のログがインシデントの対象に設定されます。 ・ログ機器「機器名」のエージェントが端末 Jailbreak を検知しました。 iOS のみ対応
5	Apple Push 証明書の有効期限	チェックを入れると、以下のログがインシデントの対象に設定されます。 ・Apple Push 証明書の有効期限が YYYY/mm/dd HH:MM:SS に切れます。ご利用の Apple ID を使用して手順にしたがって更新してください。 有効期限の 30 日前から、インシデントに表示されます。

3.3.2 インシデントの詳細画面

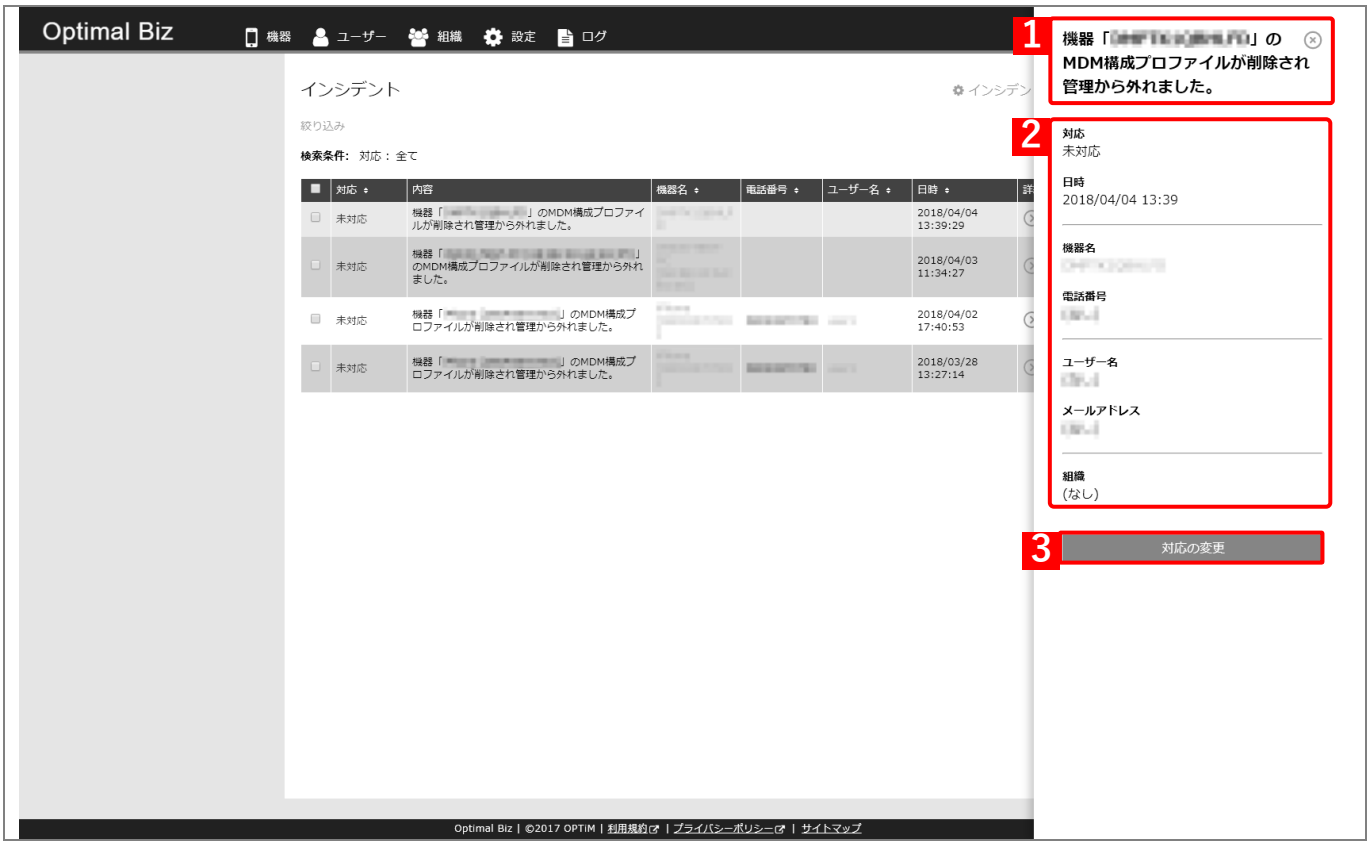
インシデントの詳細情報の表示と、対応の変更を行います。

画面

画面（対応の変更）

◆画面

表示操作 **ダッシュボードで［インシデント］→対象のインシデントの「詳細」の**

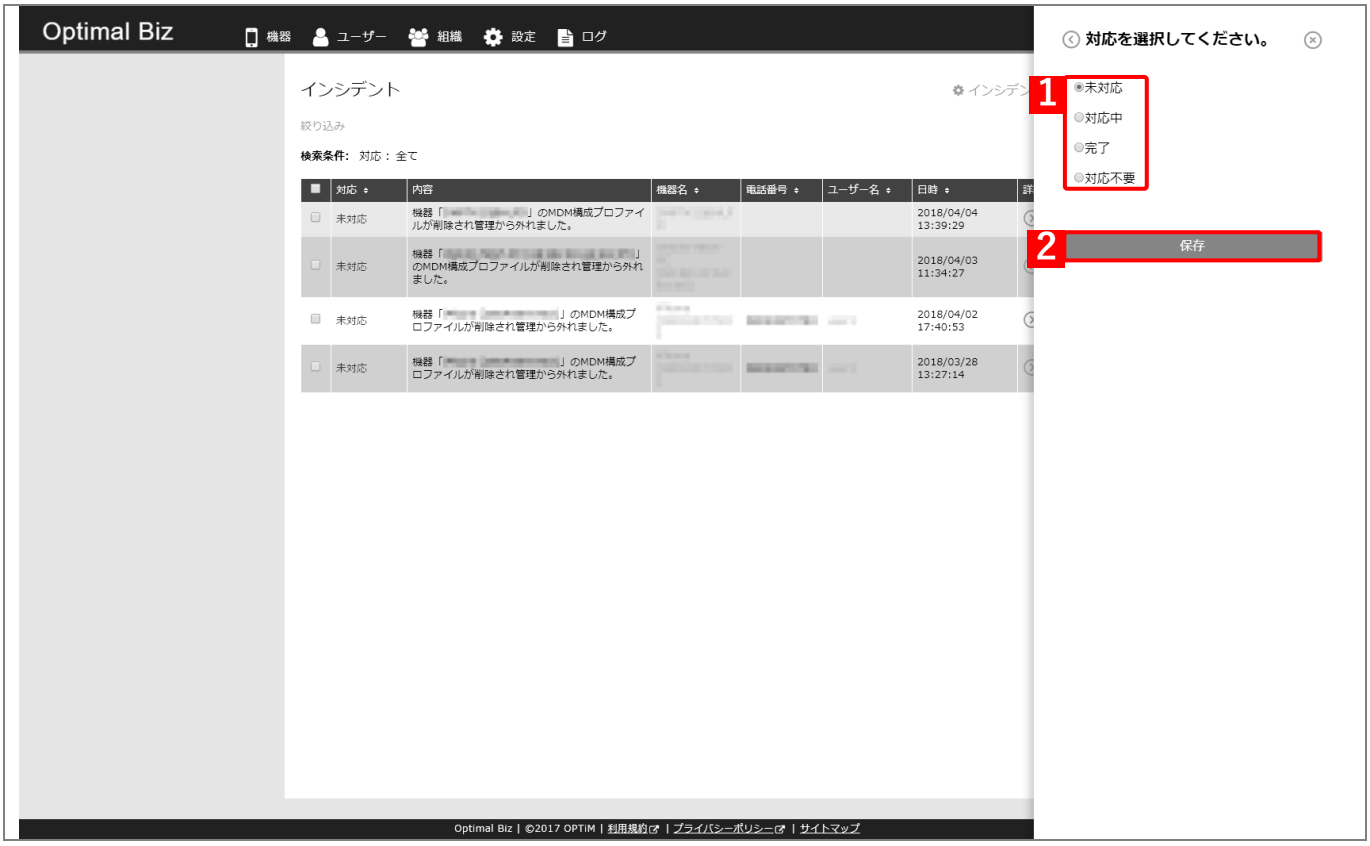


項番	項目	説明
1	ログの内容	クリックした「詳細」に対応するログが表示されます。
2	機器情報	該当の機器について各情報が表示されます。 ●対応 インシデントステータスが表示されます。ステータスは［対応の変更］で変えられます。 ●日時 ログの発生日時が表示されます。 ●機器名 該当の機器名が表示されます。クリックすると機器画面に遷移します。［機器］の詳細については、以下を参照してください。 「一覧」54 ページ ●電話番号 機器の電話番号が表示されます。 複数の SIM を搭載している端末の場合は、SIM ごとに電話番号が表示されます。 ●ユーザー名 機器に紐づいているユーザー名が表示されます。クリックすると、該当ユーザーの画面を表示します。 ●メールアドレス

項番	項目	説明
		機器に紐づいているユーザーに登録しているメールアドレスが表示されます。クリックすると、メーラーが起動し、「件名」と「本文」が適切入力されたメールが作成されます。 ●組織 機器に紐づいている組織名が表示されます。
3	対応の変更	クリックすると、「対応」のステータスを変更する画面を表示が表示されます。 「画面（対応の変更）」48 ページ

◆画面（対応の変更）

表示操作　ダッシュボードで［インシデント］→対象のインシデントの「詳細」の ＞ →［対応の変更］



項番	項目	説明
1	対応のステータス	対応のステータスを以下から選択します。 ●未対応 対応していない場合に選択します。 インシデント機能で検知したときは、初めにこのステータスが設定されています。 ●対応中 インシデントの内容に対応中の場合に選択します。 ●完了 インシデントの内容について対応が完了した場合に選択します。 ●対応不要 確認の結果対応が不要と判断した場合に選択します。
2	保存	クリックすると、選択したステータスに変更されます。

3.4 個人設定

ダッシュボード右端のユーザー名をクリックし、表示されるメニューから［個人設定］選択すると、ログインユーザーごとに以下の項目を設定することができます。

画面（個人設定の編集画面）
画面（アプリケーションメモのクリア確認画面）
画面（2 段階認証設定）
画面（2 段階認証設定削除）

●パスワード
ログインしているユーザーのパスワードを変更します。

●アプリケーションメモ
「アプリケーション」画面で各アプリのメモ欄にチェックを入れた数を、アプリケーションメモとして表示します。また、［クリア］をクリックすると、アプリケーションメモを一括で削除し、「アプリケーション」画面のメモ欄のチェックを外すことができます。
「アプリケーション」画面の詳細については、以下を参照してください。

「（情報－Android）アプリケーション」141 ページ
「アプリケーション禁止」320 ページ

●2 段階認証
ログインしているユーザーの 2 段階認証を設定、または設定を削除します。
2 段階認証で使用する端末を変更したときは、本設定を削除し、次回のログイン時に新しい端末で、2 段階認証の設定を行います。

別ユーザーでログインした場合、設定は反映されません。また、ユーザー種別が閲覧者のユーザーも設定の変更ができます。

◆画面（個人設定の編集画面）

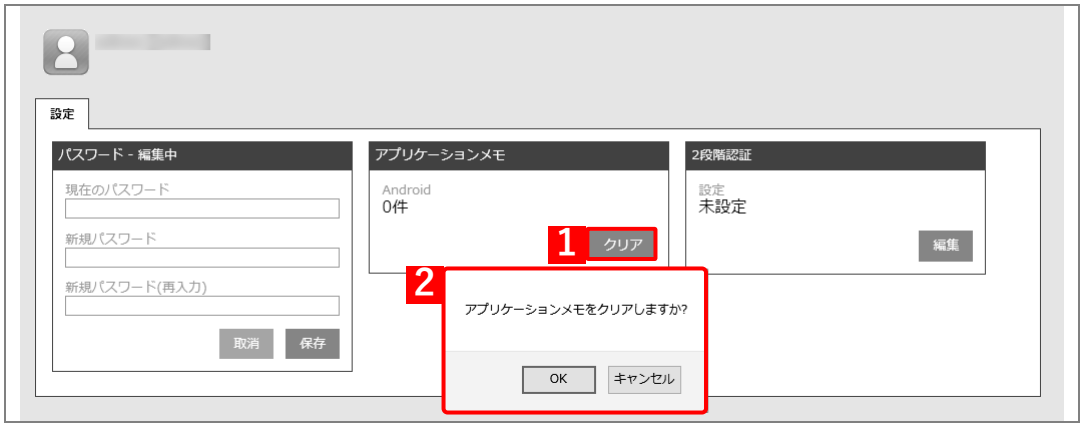
表示操作　管理サイト画面の右上の［ユーザー名］→［個人設定］→［編集］

項番	項目	説明
1	パスワード	ログイン中のユーザーのパスワードを変更します。 ●現在のパスワード 現在設定しているパスワードを 4 から 20 文字の半角英数字で入力します。 ●新規パスワード 変更後のパスワードを 4 から 20 文字の半角英数字で入力します。 ●新規パスワード(再入力) 「新規パスワード」で入力したパスワードと同じ値を入力してください。

項番	項目	説明
2	アプリケーションメモ	登録しているアプリケーションメモの数を確認できます。アプリケーションメモの詳細については、以下を参照してください。 ☞「アプリケーション禁止」320 ページ
3	2 段階認証	ログインしているユーザーの 2 段階認証の設定状況が表示されます。 ●未設定 ［編集］が表示されます。クリックして、2 段階認証の設定を行います。 ☞「画面（2 段階認証設定)」51 ページ ●設定済み ［設定削除］が表示されます。設定を削除するときにクリックします。 ☞「画面（2 段階認証設定削除)」52 ページ

◆画面（アプリケーションメモのクリア確認画面）

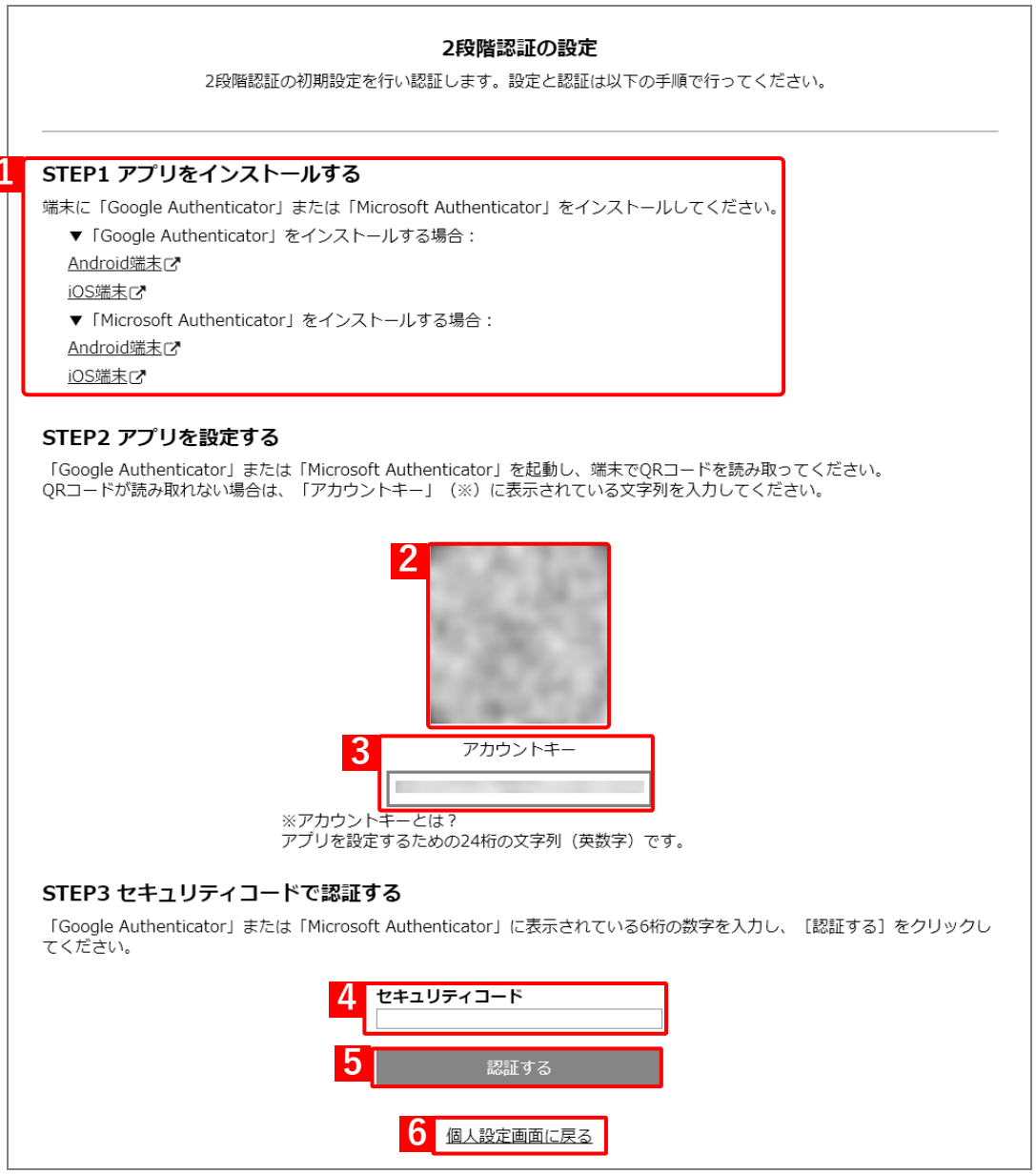
表示操作　［ダッシュボード］→［ユーザー名］→［個人設定］→［クリア］



項番	項目	説明
1	［クリア］	クリックすると、登録しているアプリケーションメモを削除します。
2	メッセージボックス	アプリケーションメモのクリアの実行確認の画面です。 ●OK アプリケーションメモのクリアを実施します。 ●キャンセル アプリケーションメモのクリアを中止します。

◆画面（2 段階認証設定）

表示操作　［ダッシュボード］→［ユーザー名］→［個人設定］→「2 段階認証」パネルの［編集］



項番	名称	説明
1	アプリをインストールする	端末に 2 段階認証で使用するアプリをインストールします。詳細は以下を参照してください。 『かんたん初期設定マニュアル』の「補足・便利な操作」－「ログイン／ログアウト」－「2 段階認証で管理サイトにログインする」
2	QR コード	項番 1 でインストールしたアプリで、表示されている QR コードを読み取ります。
3	アカウントキー	項番 2 で QR コードが読み取れなかった場合、表示されているアカウントキーを項番 1 でインストールしたアプリに入力します。
4	セキュリティコード	項番 1 でインストールしたアプリに表示された 6 桁の数字を入力します。
5	［認証する］	クリックすると、2 段階認証が完了し、個人設定が表示されます。
6	［個人設定画面に戻る］	クリックすると、個人設定が表示されます。

◆画面（2 段階認証設定削除）

表示操作　**［ダッシュボード］→［ユーザー名］→［個人設定］→「2 段階認証」パネルの［設定削除］**

項番	項目	説明
1	［設定削除］	2 段階認証の設定を削除するとき、クリックします。 実行確認画面が表示されます。 ●OK 2 段階認証の設定を削除します。 ●キャンセル 2 段階認証の設定の削除を中止します。

4 機器

この章では、ヘッダーメニューの［機器］画面に表示される、各種の設定について説明します。

4.1 一覧

サイドメニューの［一覧］画面に表示される、各種の設定について説明します。

4.1.1 機器一覧

［一覧］画面では、登録されている端末の情報を表示します。

一覧から対象の端末を選択し、各種の設定や操作、情報の確認などを行うことができます。また、検索や絞り込み、並べ替え、端末の一括削除、端末の新規登録なども行うことができます。

画面

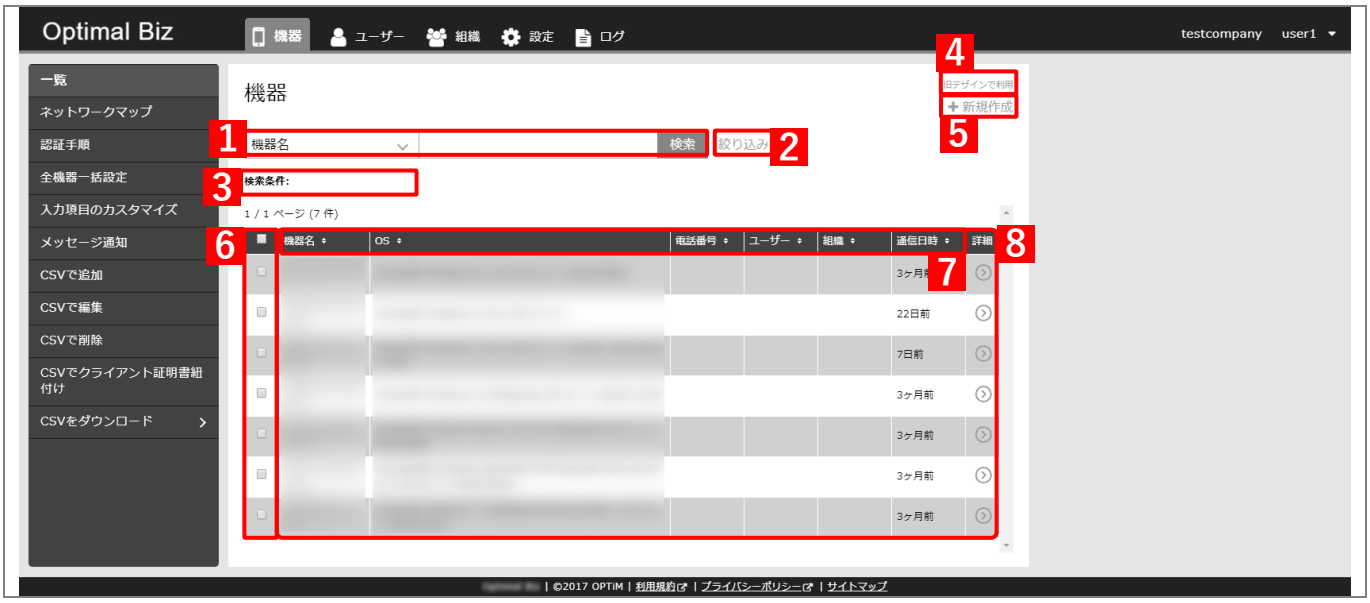
画面（絞り込み）

画面（一括削除）

機器一覧では、端末名称（機器名）が辞書順で表示されます（英字は小文字、大文字の順になります）。

◆画面

表示操作［機器］→［一覧］



項番	項目	説明
1	機器検索	をクリックして、リストボックスからカテゴリを選択し、テキストボックスに、検索するキーワードを入力して［検索］をクリックします。 検索キーワードに該当する機器のみが一覧に表示されます。 再度、すべての機器を一覧に表示するには、以下のいずれかの操作をしてください。 ・「検索条件」に表示された をクリックします。 ・テキストボックスを空欄にしてから［検索］をクリックします。 ・キーボードの［F5］キーを押します。
2	［絞り込み］	クリックすると、絞り込み条件を選択する画面が表示されます。詳細については、以下を参照してください。 「画面（絞り込み）」56 ページ
3	検索条件	機器検索や［絞り込み］をクリックして検索した場合、その条件が表示されます。 をクリックすると、再度、すべての機器が一覧に表示されます。

項番	項目	説明
4	［旧デザインで利用］	クリックすると、旧デザインの画面が表示されます。詳細については、以下を参照してください。 ☞「旧デザイン」252 ページ
5	［新規作成］	クリックすると、機器の新規作成画面が表示されます。詳細については、以下を参照してください。 ☞「機器の新規作成」61 ページ
6	チェックボックス	複数の機器をまとめて削除する場合に、対象の機器にチェックを入れます。 チェックを入れると、一覧画面の下に機器をまとめて削除する画面が表示されます。詳細については、以下を参照してください。 ☞「画面（一括削除）」57 ページ
7	見出し項目	各項目の見出しをクリックするたびに、機器の一覧がその項目の昇順、降順に並び替えられます。
8	機器一覧	以下の項目が表示されます。 ●機器名 機器の名称が表示されます。 機器名をクリックすると、機器一覧の右側に該当の機器の管理情報の表示や編集、設定、操作、各種情報を表示する詳細画面が表示されます。 ☞「機器の詳細画面」59 ページ 機器名をクリックすると、機器一覧の対象の機器情報の行の背景色の色が変わります。 ●OS 該当機器の OS 名が表示されます。 ●電話番号 登録済みの電話番号が表示されます。 複数の電話番号を持つ端末は、端末が保持している電話番号のうち、いずれか 1 つが「電話番号」列に表示されます。 表示されていないほかの電話番号は、〉をクリックすると表示される詳細画面で確認することができます。 端末が保持しているほかの電話番号で検索した場合は、検索結果に検索した電話番号が表示されないことがあります。 ●ユーザー 作成したユーザーに機器が紐づいている場合は、そのユーザー名が表示されます。 ●組織 以下の組織が表示されます。 ・機器が紐づいている組織 ・機器に紐づいているユーザーが所属している組織 ●通信日時 対象の機器と管理サーバーが最後に通信した日時（〇日前、〇分前）が表示されます。 機器の状態によって、「(管理外)」、「(認証待ち)」などが表示されます。 iOS 端末は、MDM 構成プロファイルの通信日時が表示されます。 ●詳細 〉をクリックすると、機器一覧の右側に該当の機器の管理情報の表示や編集、設定、操作、各種情報を表示する詳細画面が表示されます。 ☞「機器の詳細画面」59 ページ 機器を選択すると、背景色が変わります。

◆画面（絞り込み）

表示操作　［機器］→［一覧］→［絞り込み］

項番	項目	説明
1	OS	OS の種別、資産管理対象機器で絞り込みを行う場合に、対象にチェックを入れます。
2	OS バージョン	OS のバージョンで絞り込みを行う場合に、テキストボックスに対象のバージョンを入力します。
3	電話番号	管理情報の電話番号の登録状況で絞り込みを行う場合に、「登録済み」または「登録なし」にチェックを入れます。
4	ユーザー	管理情報の「ユーザー」の登録状況で絞り込みを行う場合に、「登録済み」または「登録なし」にチェックを入れます。
5	組織	作成した組織で絞り込みを行う場合に、対象の組織にチェックを入れます。
6	（カスタマイズ項目）	機器やユーザーの「入力項目のカスタマイズ」で登録した項目、分類がある場合、登録されているグループで絞り込みを行う場合いに、対象のグループにチェックを入れます。
7	通信状況	通信状況で絞り込みを行う場合に、「無通信検知機器」または「管理外機器」にチェックを入れます。 無通信検知については、以下を参照してください。 「通知設定」633 ページ 管理外機器については、以下を参照してください。 「機器の種類」190 ページ

項番	項目	説明
8	認証状況	認証状況で絞り込みを行う場合に、「認証待ち機器」または「認証待ち機器を含まない」にチェックを入れます。
9	［絞り込み］	クリックすると、設定した絞り込み条件に一致した機器が一覧に表示されます。

◆画面（一括削除）

削除した端末は、管理サイトからの設定や確認が一切できなくなります。ただし、既存の設定は端末にそのまま保持されます。端末を削除する場合は、十分に注意してください。

削除した端末側で、別途以下の操作を行う必要があります。

- ライセンスの解除
- エージェントおよびプロファイルのアンインストール

iOS 端末にシングル APP モードの設定を適用している場合は、必ずシングル APP モードの割り当てを解除／同期を行い、端末で解除されたことを確認してから、機器を削除してください。シングル APP モードが適用されている状態で機器を削除すると、端末が操作不能になる場合があるので、注意してください。

「シングル APP モード（監視対象のみ）」535 ページ

表示操作　［機器］→［一覧］→削除する機器にチェックを入れる

項番	項目	説明
1	チェックボックス	削除する機器にチェックを入れます。チェックを入れると、一覧の下に操作メニューが表示されます。 見出し行にあるチェックボックスをクリックすると、すべての機器にチェックを入れたり、外したりできます。
2		クリックするたびに操作メニューを閉じたり、表示したりします。
3	削除	チェックした機器を削除する場合に、「この機器を削除する」を選択します。

項番	項目	説明
4	［実行］	クリックすると確認画面が表示されます。
5	確認画面	［OK］をクリックすると、チェックが入っている機器が一覧から削除されます。 個別に削除する方法については、以下を参照してください。 ☞「機器の個別削除」73 ページ

◆エラー一覧

文言	発生契機	対処方法
⚠ シングル APP モードの設定が割り当てられているため、削除に失敗した認証済みの iOS 機器があります。	シングル APP モードが適用されている状態で機器を削除しようとしている。	シングル APP モードの割り当てを解除／同期を行い、端末で解除されたことを確認して、再度、削除してください。

4.1.2 機器の詳細画面

［一覧］画面から詳細画面を表示すると、端末への設定セットの反映や管理情報の確認／編集、各種の設定、操作、情報の確認などを行うことができます。

◆画面

表示操作　**［機器］→［一覧］→対象の機器の機器名または「詳細」の**

項番	項目	説明
1	機器名	対象の端末の名称が表示されます。 機器の管理情報、情報画面すべてに表示されています。
2	通信日時	対象の端末と管理サーバーが最後に通信した日時が表示されます。 機器の情報は、この通信日時の時点の情報が表示されます。最新の情報を表示したい場合は、項番 4 同期 をクリックしてください。 機器の管理情報、設定、操作、情報画面すべてに表示されます。 iOS 端末は、MDM 構成プロファイルの通信日時が表示されます。
3	⊗	クリックすると、機器の詳細画面が閉じます。 機器の管理情報、設定、操作、情報画面すべてに表示されます。
4	同期	クリックすると、対象の機器との同期が実行されます。 詳細については、以下を参照してください。 ☞「機器との同期」70 ページ 機器の管理情報、設定、操作、情報画面すべてに表示されます。
5	管理情報	機器の管理情報の表示、編集を行います。 詳細については、以下を参照してください。 ☞「機器の管理情報」67 ページ
6	設定／操作／情報	●設定 機器への設定セットやテンプレートの設定、その他の設定を行うためのメニューが表示されます。表示されているメニュー以外を表示するには［他の設定を見る］をクリックします。機器の OS の種別によって、設定項目が異なります。詳細については、以下を参照してください。 ☞「機器の設定」74 ページ ●操作 機器への各種操作を行うためのメニューが表示されます。表示されているメニュー以外を表示するには［他の操作を見る］をクリックします。機器の OS の種別によって、操作が異なります。詳細については、以下を参照してください。 ☞「機器の操作」109 ページ ●情報 機器の各種情報の確認を行うためのメニューが表示されます。表示されているメニュー以外を表示するには［他の情報を見る］をクリックします。機器の OS の種別によって、確認できる情報が異なります。詳細については以下を参照してください。 ☞「機器の情報」134 ページ
7	［この機器を削除する］	クリックすると、詳細画面を表示している機器を削除します。 削除については、以下を参照してください。 ☞「機器の個別削除」73 ページ ライセンス認証済みの Windows 端末は、削除を実施したあと、エージェントと同期ができたタイミングで利用ライセンス数が回復します。

4.1.3 機器の新規作成

端末側でライセンス認証を行うと、管理サイトへ端末が登録され、機器一覧に端末が表示されますが、ライセンス認証前に、端末を新規作成（手動で端末を管理サイトへ登録）することができます。端末を新規作成しておくと、端末と同期したタイミングで設定内容の反映とライセンス認証が行われるため、認証後に各種の設定を行う手間を省くことができます。

また、管理者が登録したい端末のみを新規作成し、他の端末を認証しないようにすることもできます。

「機器認証制御」641 ページ

新規作成した端末は、「通信日時」欄に「(認証待ち)」と表示されます。

画面（新規作成：OS 選択）

画面（新規作成：特定の OS 種別を選択した場合）

画面（新規作成：「資産管理対象機器」を選択した場合）

ゼロタッチ端末の場合は、この画面から端末を新規作成しないでください。ゼロタッチ端末を新規作成する方法については、以下のセクションおよびマニュアルを参照してください。

「機器一覧」380 ページ

『Android キッティングマニュアル』の「Google アカウントでゼロタッチ登録を利用して Android Enterprise 連携を行う」

『Android キッティングマニュアル』の「Google Workspace アカウントでゼロタッチ登録を利用して Android Enterprise 連携を行う」

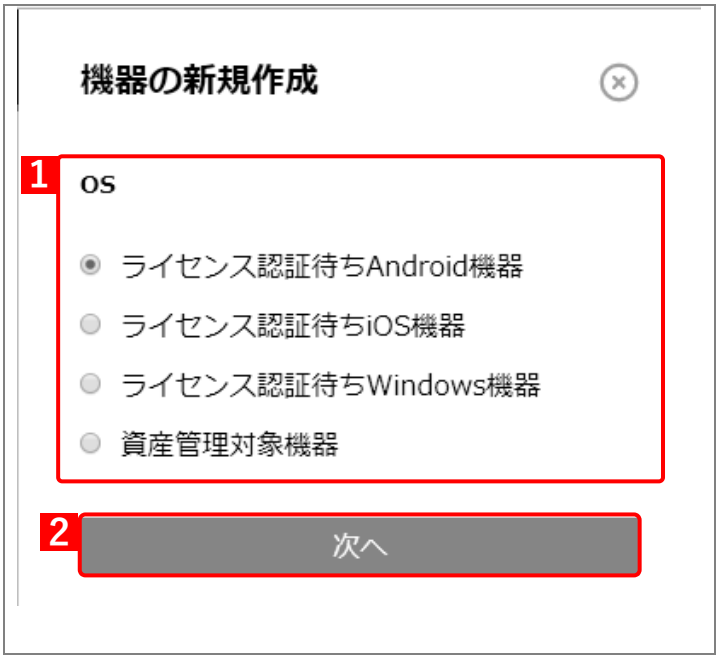
端末とユーザーの紐づけ、または端末と組織の紐づけには、あらかじめユーザーと組織を作成する必要があります。詳細については、以下を参照してください。

「［管理］タブ」257 ページ

「［管理］タブ」284 ページ

◆画面（新規作成：OS 選択）

表示操作　**［機器］→［一覧］→［新規作成］**

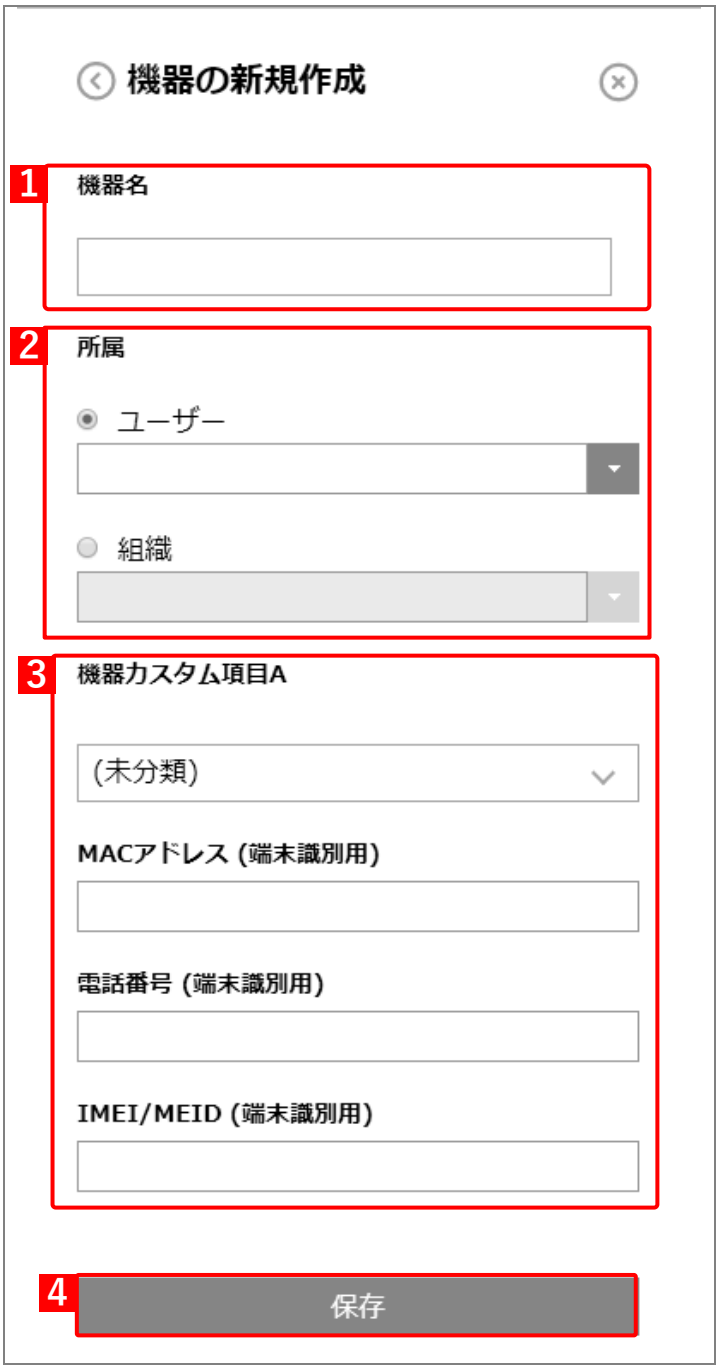


項番	項目	説明
1	OS	新規作成する機器の OS の種別または「資産管理対象機器」のいずれかを選択します。

項番	項目	説明
2	［次へ］	項番 1 の「OS」で選択した OS の種別、または「資産管理対象機器」の設定画面を表示します。

◆画面（新規作成：特定の OS 種別を選択した場合）

表示操作　**［機器］→［一覧］→［新規作成］→「OS」で特定の OS 種別を選択→［次へ］**



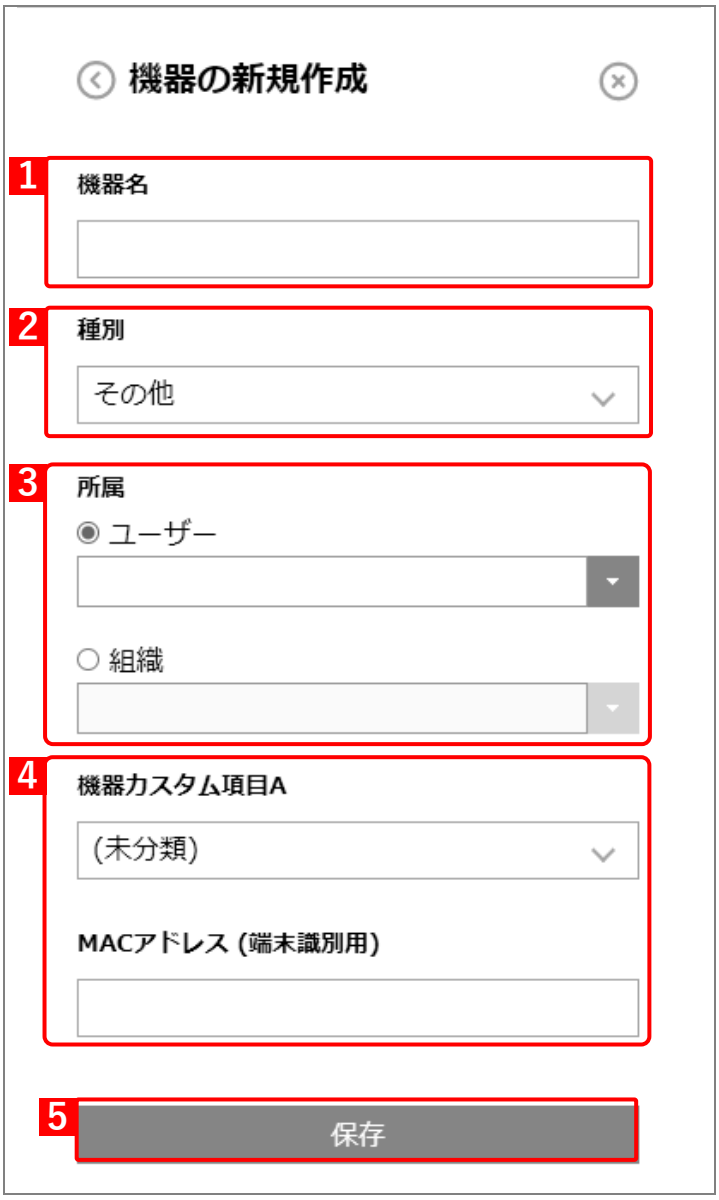
項番	項目	説明
1	機器名	機器名を 100 文字以内で入力します。必須入力項目です。 機器名は機器画面やログなど、管理サイトのさまざまな箇所で表示されます。 重複する名称は登録できません。
2	所属	この機器を所属させる対象を以下から選択します。 ●ユーザー 機器にユーザーを紐づける場合に選択し、リストボックスから登録済みのユーザーを選択します。 「ユーザー」253 ページ ●組織 機器に組織を紐づける場合に選択し、リストボックスから登録済みの組織を選択します。 「組織」281 ページ
3	（カスタム項目）	機器の「入力項目のカスタマイズ」で登録した項目名が表示されます。必要に応じて、項目を選択したり、入力したりします。登録内容によって、表示される項目が異なります。入力項目の場合は、1,000 文字以内で入力してください。 カスタム項目の作成については、以下を参照してください。 「入力項目のカスタマイズ」218 ページ
	MAC アドレス(端末識別用) （※1）	ライセンス認証した端末と本画面で作成した端末を紐づけるために、端末の MAC アドレスを入力します。 「XX:XX:XX:XX:XX:XX」（X は大文字の 16 進数）という形式で入力してください。 重複する MAC アドレスは登録できません。 MAC アドレスの確認方法については、機器に付属しているマニュアルを参照してください。 Android 端末および iOS 端末では、MAC アドレスを新規に入力することができません。すでに登録しているライセンス認証待ち機器は、MAC アドレスを入力していると、保存することができません。 Android 端末および iOS 端末で新規作成するときは、「(端末識別用)」の電話番号、IMEI/MEID、シリアル番号のいずれかを入力してください。 Windows 端末を新規で作成したときに、SIM に割り当てられている MAC アドレスは、端末識別用として使用できません。Windows 端末の「(端末識別用)」の値は、Wi-Fi や Bluetooth などに割り当てられている MAC アドレス、もしくは、電話番号、IMEI/MEID、シリアル番号のいずれかを入力してください。
	電話番号(端末識別用) （※1）	ライセンス認証した端末と本画面で作成した端末を紐づけるために、端末の電話番号を入力します。 ハイフンを除いた電話番号を入力してください。 当項目は Android 端末、iOS 端末、および Windows 端末の場合のみ入力項目として表示されます。 重複する電話番号は登録できません。 電話番号の確認方法については、機器に付属しているマニュアルを参照してください。 iOS 端末では、「+81」から始める国際電話番号が表示されていることがありますが、「0」から始まる日本の電話番号に置き換えて入力してください。 例) ・090 の場合 国際電話番号：+8190XXXXXXXX 日本の電話番号：090XXXXXXXX ・080 の場合 国際電話番号：+8180XXXXXXXX 日本の電話番号：080XXXXXXXX

項番	項目	説明
	IMEI/MEID(端末識別用) （※1）	ライセンス認証した端末と本画面で作成した端末を紐づけるために、100 文字以内で IMEI または MEID を入力します。使用できる文字は、半角英数字と記号です。 当項目は Android 端末と Windows 端末の場合のみ入力項目として表示されます。 重複する IMEI または MEID は登録できません。 IMEI/MEID の確認方法については、機器に付属しているマニュアルを参照してください。
	シリアル番号(端末識別用) （※1）	ライセンス認証した端末と本画面で作成した端末を紐づけるために、100 文字以内で端末のシリアル番号を入力します。使用できる文字は、半角英数字と記号です。 当項目は iOS 端末、および Windows 端末の場合のみ入力項目として表示されます。 シリアル番号の確認方法については、機器に付属しているマニュアルを参照してください。 重複するシリアル番号は登録できません。
4	［保存］	機器を登録します。登録した機器は、機器一覧に追加されます。

※1：機器がライセンス認証したときに、事前登録した情報と紐づくように「(端末識別用)」の項目のいずれか 1 つは必ず設定してください。

◆画面（新規作成：「資産管理対象機器」を選択した場合）

表示操作　**［機器］→［一覧］→［新規作成］→「OS」で「資産管理対象機器」を選択→［次へ］**



項番	項目	説明
1	機器名	機器名を 100 文字以内で入力します。必須入力項目です。 機器名は機器画面やログなど、管理サイトのさまざまな箇所で表示されます。 重複する名称は登録できません。
2	種別	プルダウンメニューから機器の種別を選択します。選択できる種別は以下のとおりです。 ・ネット TV 端末、レコーダー、STB、AV アンプ、デジタルカメラ、デジタルビデオカメラ、オーディオ、プレイヤー、プロジェクター、フォトフレーム、AV 系その他、デスクトップ、ノート PC、ストレージ、PDA、プリンター、タブレット、スマートフォン、PC 系その他、携帯電話、IP 電話、ルーター、FAX、スイッチングハブ、PLC モデム、無線 LAN モデム、同軸ケーブルモデム、通信系その他、エアコン、冷蔵庫、洗濯機、照明、電子レンジ、Web カメラ、ゲートウェイ、ドアホン、センサー、換気扇、ブラインド、シャッター、雨戸、散水機、給湯器、便座、電気錠、太陽光発電、床暖房、ポット、IH 調理器、炊飯器、掃除機、くらし系その他、据置ゲーム機、ポータブルゲーム機、家庭用ロボット、娯楽系その他、その他

項番	項目	説明
3	所属	この機器を所属させる対象を以下から選択します。 ●ユーザー 機器にユーザーを紐づける場合に選択し、リストボックスから登録済みのユーザーを選択します。 ☞「ユーザー」253 ページ ●組織 機器に組織を紐づける場合に選択し、リストボックスから登録済みの組織を選択します。 ☞「組織」281 ページ
4	（カスタム項目）	機器の「入力項目のカスタマイズ」で登録した項目名が表示されます。必要に応じて、項目を選択したり、入力したりします。登録内容によって、表示される項目が異なります。入力項目の場合は、1,000 文字以内で入力してください。 カスタム項目の作成については、以下を参照してください。 ☞「入力項目のカスタマイズ」218 ページ
	MAC アドレス(端末識別用)	ライセンス認証が行われた機器と、当画面で登録した機器を紐づけるための MAC アドレスを入力します。 「XX:XX:XX:XX:XX:XX」（X は大文字の 16 進数）という形式で入力してください。 本項目の入力は任意です。 重複する MAC アドレスは登録できません。 MAC アドレスの確認方法については、機器に付属しているマニュアルを参照してください。 Android 端末および iOS 端末では、MAC アドレスを新規に入力することができません。すでに登録しているライセンス認証待ち機器は、MAC アドレスを入力していると、保存することができません。 Android 端末および iOS 端末を新規作成するときは、「(端末識別用)」の電話番号、IMEI/MEID、シリアル番号のいずれかを入力してください。 Windows 端末を新規で作成したときに、SIM に割り当てられている MAC アドレスは、端末識別用として使用できません。Windows 端末の「(端末識別用)」の値は、Wi-Fi や Bluetooth などに割り当てられている MAC アドレス、もしくは、電話番号、IMEI/MEID、シリアル番号のいずれかを入力してください。
5	［保存］	機器を登録します。登録した機器は、機器一覧に追加されます。

4.1.4 機器の管理情報

端末の管理情報の確認と編集を行います。

端末とユーザーとの紐づけ、または端末と組織との紐づけも行うことができます。

画面

画面（編集）

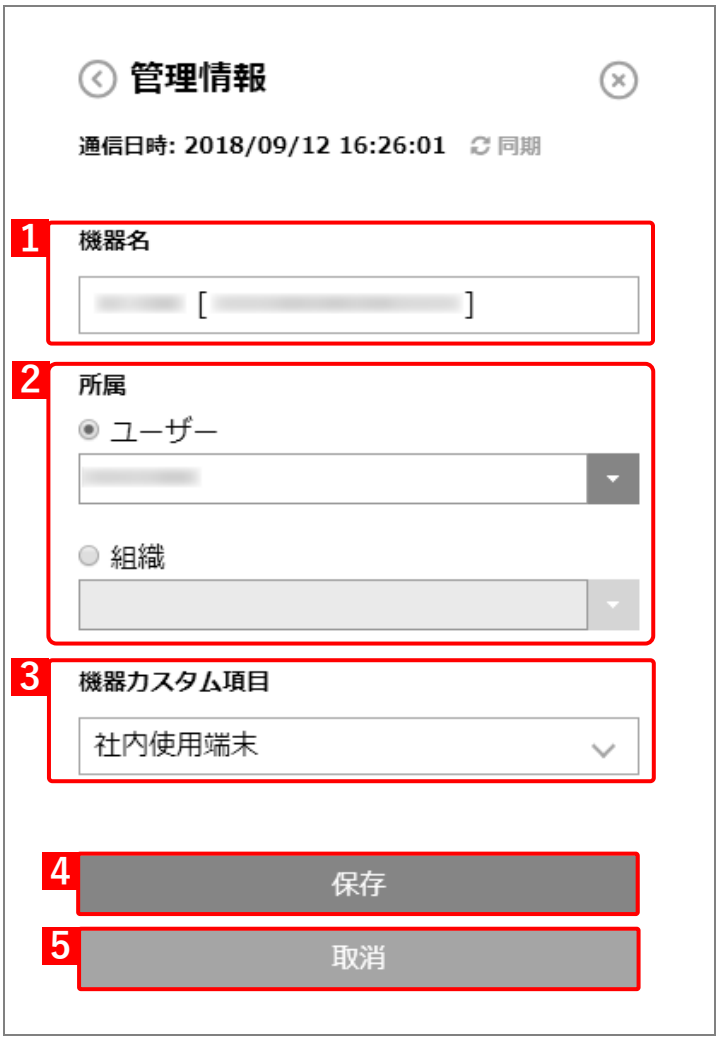
◆画面

表示操作［機器］→［一覧］→対象の機器の機器名または「詳細」の

項番	項目	説明
1	OS	対象の機器の OS バージョンが表示されます。
2	電話番号	電話番号が登録されている場合は、電話番号が表示されます。 複数の電話番号を持つ端末は、端末が保持している電話番号がすべて表示されます。
3	ユーザー	所属にユーザーが設定されている場合は、ユーザー名が表示されます。
4	組織	所属に組織が設定されている場合は、組織名が表示されます。
5	カスタマイズ項目	機器の「入力項目のカスタマイズ」で登録した項目名が表示されます。登録内容によって、表示される項目が異なります。 「入力項目のカスタマイズ」218 ページ
6	［管理情報の編集］	クリックすると、管理情報を編集できます。 「画面（編集）」68 ページ

◆画面（編集）

表示操作［機器］→［一覧］→対象の機器の機器名または「詳細」の ⓘ →［管理情報の編集］



項番	項目	説明
1	機器名	機器名を 100 文字以内で入力します。必須入力項目です。 機器名は機器画面やログなど、管理サイトのさまざまな箇所で表示されます。 他の機器名と重複はできません。 iOS 端末は端末名称変更を設定すると、編集した機器名が端末のデバイス名になります。詳細は以下を参照してください。 ☞「画面（端末名称変更）」386 ページ 端末のデバイス名は AirDrop やテザリング時の AP 名などに設定されるため、他の端末から見ることができます。電話番号などの個人情報を機器名に設定しないでください。 端末のデバイス名は、最大で 63 文字まで表示されます。 端末の状態によっては端末のデバイス名に表示されるまで、時間がかかる場合があります。 端末のデバイスは、iOS 端末の「設定」アプリ→［一般］→［情報］→「名前」です。

項番	項目	説明
2	所属	この機器を所属させる対象を以下から選択します。 ●ユーザー 機器にユーザーを紐づける場合に選択し、リストボックスから登録済みのユーザーを選択します。 「ユーザー」253 ページ ●組織 機器に組織を紐づける場合に選択し、リストボックスから登録済みの組織を選択します。 「組織」281 ページ
3	（カスタマイズ項目）	機器の「入力項目のカスタマイズ」で登録した項目名が表示されます。 必要に応じて、項目を選択したり、入力したりします。登録内容によって、表示される項目が異なります。 入力項目の場合は、1,000 文字以内で入力してください。 カスタム項目の作成については、以下を参照してください。 「入力項目のカスタマイズ」218 ページ
4	［保存］	クリックすると、編集した管理情報を保存して編集を終了します。
5	［取消］	クリックすると、編集した内容をキャンセルして編集を終了します。

◆エラー一覧

文言	発生契機	対処方法
⚠ Google Workspace 連携したメールアドレスをユーザーに登録して下さい。	管理サイトの［機器］→［一覧］で機器にユーザーを紐づける際に、Google Workspace アカウントを利用したゼロタッチ登録を行った機器で認証した機器に対して Google Workspace のメールアドレスが含まれていないユーザーを割り当てようとしている。	Google Workspace アカウントを利用したゼロタッチ登録を行った端末で認証した端末に対しては、Google Workspace のメールアドレスを含んだユーザーを紐づけてください。

4.1.5 機器との同期

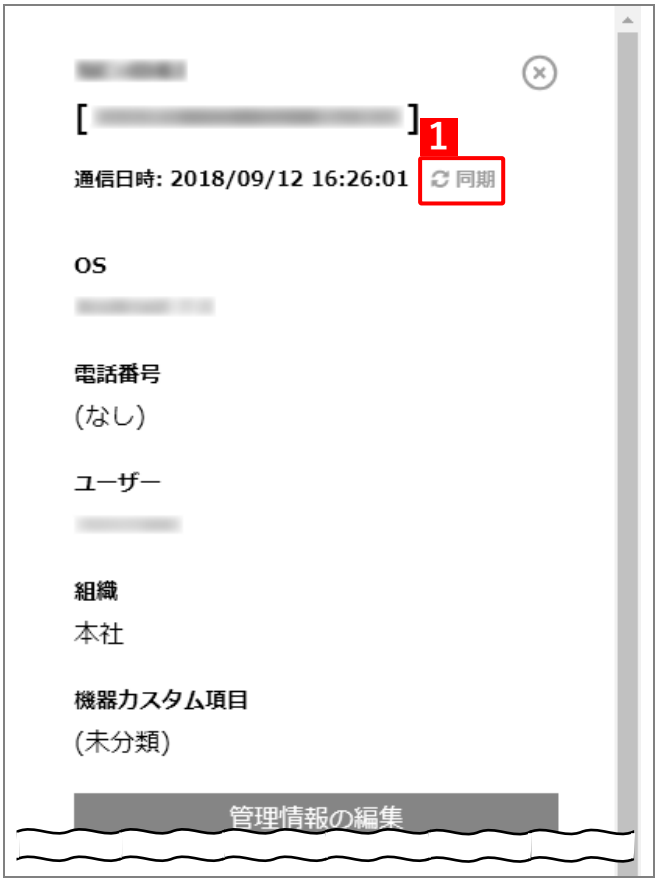
対象の端末に、管理サイトで行った各種設定を反映します。

また、位置情報など、管理サイトで保持している端末情報の更新を行うこともできます。

- 対象の端末が認証されている必要があります。
- 同期は定期的に行われますが、急ぐ場合は手動で同期を行うことができます。また、同期を行ったあと、設定の反映や端末情報が更新されるまでの時間は、サーバーの通信状況に依存します（ベストエフォート型）。
- 定期同期については、OS ごとに以下のとおりです。
  - Android 端末、Windows 端末の場合は、「管理サイトの通信と動作」の「管理サーバーとの通信間隔」で定期同期の間隔を設定できます。
    ☞ Android：「管理アプリの通信と動作」298 ページ
    ☞ Windows：「管理アプリの通信と動作」561 ページ
  - iOS 端末の場合は、前回の同期から最短 8 時間後です。
  - 定期同期の実施間隔は、サーバーの状況などによって時間間隔が変動する場合があります。
- 同期された情報を管理サイト画面に反映させるには、管理サイト画面の更新が必要です。
- 機器の管理情報、設定、操作、情報画面で、同期が必要な操作画面すべてに 同期 が表示されています。

◆画面（例：機器の管理情報画面）

表示操作 ［機器］→［一覧］→**対象の機器の機器名または「詳細」の** ›→ 同期



項番	項目	説明
1	同期	対象の端末と同期したい場合、クリックします。 確認画面で［OK］をクリックすると、同期が実行されます。取り消す場合は、［キャンセル］をクリックします。

◆エラー一覧

文言	発生契機	対処方法
⚠ エージェント個別管理で Push 通知が無効になっています。	［設定］→［Android］→［エージェント個別管理］で Push 通知を「利用しない」に選択した設定を割り当て、「同期」をクリックしている。	Push 通知を「利用しない」に選択した設定を外し、同期してください。
⚠ 証明書が無効なため通知ができませんでした。メニューの Apple Push 証明書登録から証明書を登録してください。	Apple Push 証明書が登録されていない状態で、認証済み iOS 機器の機器詳細画面で「同期」をクリックしている。	Apple Push 証明書を登録してください。

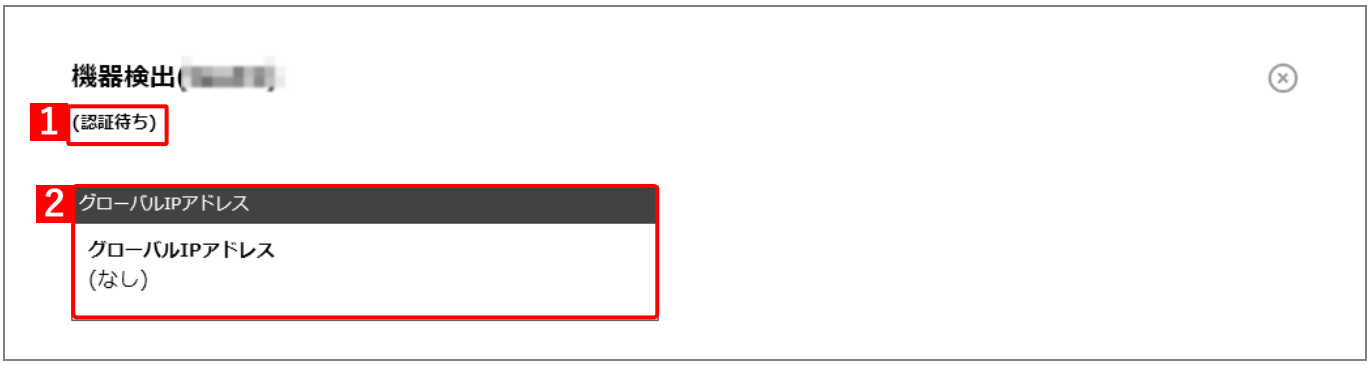
4.1.6 機器検出の情報

エージェントやポータルがインストールできず、ライセンスの認証ができない資産管理対象機器（プリンターやストレージ、ライセンス認証せずに使用する端末）や、ライセンス認証待ち端末のグローバル IP アドレスを表示します。グローバル IP アドレスを管理することで、資産管理対象機器やライセンス認証待ち端末を資産として管理することができます。

- 対象の端末が認証されている必要があります。
- 機器一覧の「OS」項目が「資産管理対象機器（xxxxx）」と表示されている機器や、「通信日時」項目が「(認証待ち)」と表示され端末のみ、情報を確認することができます。
- 表示される情報は、検出された情報の種類によって異なります。
- 「機器の新規作成」で［ライセンス認証待ち Android 機器］、［ライセンス認証待ち iOS 機器］、［ライセンス認証待ち Windows 機器］のいずれかを選んだ場合は、端末がライセンス認証されるまで「(認証待ち)」と表示されます。

◆画面

表示操作　**［機器］→［一覧］→認証待ち機器の機器名または「詳細」の→詳細画面の「情報」の［機器検出］**



項番	項目	説明
1	(認証待ち)	認証待ち機器であることが表示されます。
2	情報	検出された情報が表示されます。 検出結果に、表示される情報が異なります。

4.1.7 機器の個別削除

管理サイトに登録されている端末を削除します。

複数の端末を削除する場合は、以下を参照してください。

「画面（一括削除）」57 ページ

削除した端末は、管理サイトからの設定や確認が一切できなくなります。ただし、既存の設定は端末にそのまま保持されます。端末を削除する場合は、十分に注意してください。

削除した端末側で、別途以下の操作を行う必要があります。

- ライセンスの解除
- エージェントおよびプロファイルのアンインストール

iOS 端末にシングル APP モードの設定を適用している場合は、必ずシングル APP モードの割り当てを解除／同期を行い、端末で解除されたことを確認してから、機器を削除してください。シングル APP モードが適用されている状態で機器を削除すると、端末が操作不能になる場合があるので、注意してください。

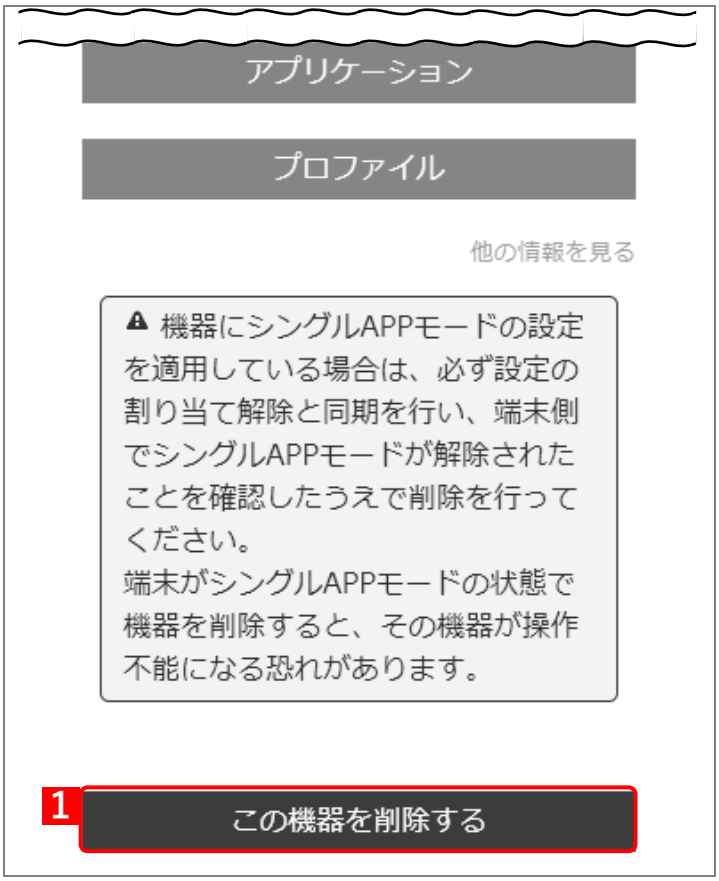
iOS 端末にシングル APP モードの設定を適用した状態で、機器を削除しようとした場合は、削除できない旨のメッセージが表示されます。

「シングル APP モード（監視対象のみ）」535 ページ

◆画面

表示操作 ［機器］→［一覧］→対象の機器の機器名または「詳細」の ›→詳細画面の末尾を表示

ここでは、iOS 端末の画像を例に使用しています。



項番	項目	説明
1	［この機器を削除する］	対象の端末を管理サイトから削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.8 機器の設定

各端末の詳細画面から、端末ごとの各種設定を行うことができます。

設定内容は OS により異なります。

また、機器の詳細画面の「機器」では OS によりさまざまな設定項目ボタンが表示されますが、各機器への設定セットに割り当てて適用する方法は、機器ごとに設定を割り当てる方法と、OS ごとの全機器に一括で設定する方法の 2 つの方法があります。

設定画面で設定が行われている場合で、基本パッケージが存在しない、および機器オプションパッケージが機器に割り当てられていないときは、警告が表示されます。

機器ライセンスパッケージの割り当て状態にかかわらず、設定セットなどの設定は、制限なく行えます。

●機器ごとに設定する場合

OS にあわせて以下を参照してください。

・Android 端末に適用する場合

「（設定－Android）設定の割り当て」75 ページ

・iOS 端末に適用する場合

「（設定－iOS）設定の割り当て」83 ページ

・Windows 端末に適用する場合

「（設定－Windows）設定セットの割り当て」103 ページ

●全機器に一括設定する場合

以下を参照してください。

「全機器一括設定」200 ページ

4.1.8.1 （設定－Android）設定の割り当て

各機能で作成した設定セットを Android 端末に反映します。

設定セットの内容は、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

画面

画面（編集）

登録されている Android 端末に一括で設定セットを反映する場合は、以下を参照してください。

「［Android 設定］タブ」202 ページ

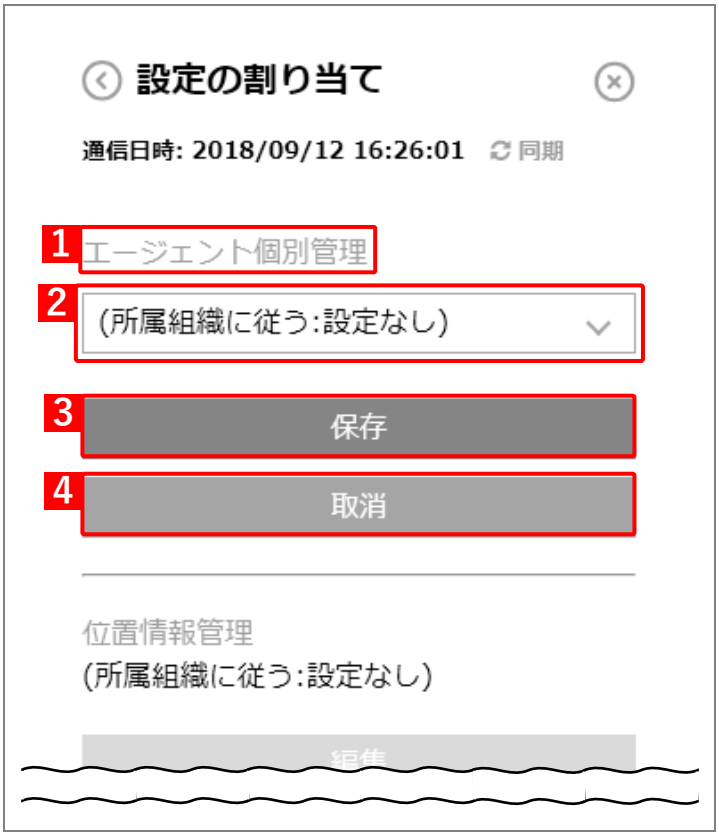
◆画面

表示操作 **［機器］→［一覧］→Android 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［設定の割り当て］**

項番	項目	説明
1	設定一覧	Android 端末への各設定機能と設定中の設定セット名などが表示されます。 設定機能名をクリックすると、該当の設定画面に遷移します。 機器個別の設定画面で設定しているにもかかわらず、機器オプションパッケージを機器に割り当てていない場合は、(A)（B）の警告が表示されます。
2	［編集］	クリックすると、設定機能ごとに、適用する設定を変更できます。 「画面（編集）」76 ページ

◆画面（編集）

表示操作 **［機器］→［一覧］→Android 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［設定の割り当て］→対象の機能の［編集］**



項番	項目	説明
1	設定機能	クリックすると、該当の機能の設定セットの一覧画面に遷移します。
2	(所属組織に従う:設定なし)	適用する設定セット名をリストボックスから選択します。 ●(所属組織に従う:設定なし) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(設定なし) 各機能の設定を外します。 ●各機能の設定名 各機能で作成済みの設定セットを適用したいときは、その設定名をリストボックスから選択して設定します。ここで設定した設定セットに対する編集および削除が行われた場合、この設定にも反映されます。
3	［保存］	クリックすると、設定内容を保存します。
4	［取消］	クリックすると、編集作業をキャンセルします。

4.1.8.2 （設定－Android）設定テンプレートの割り当て

設定テンプレート機能で作成したテンプレートを Android 端末に反映します。

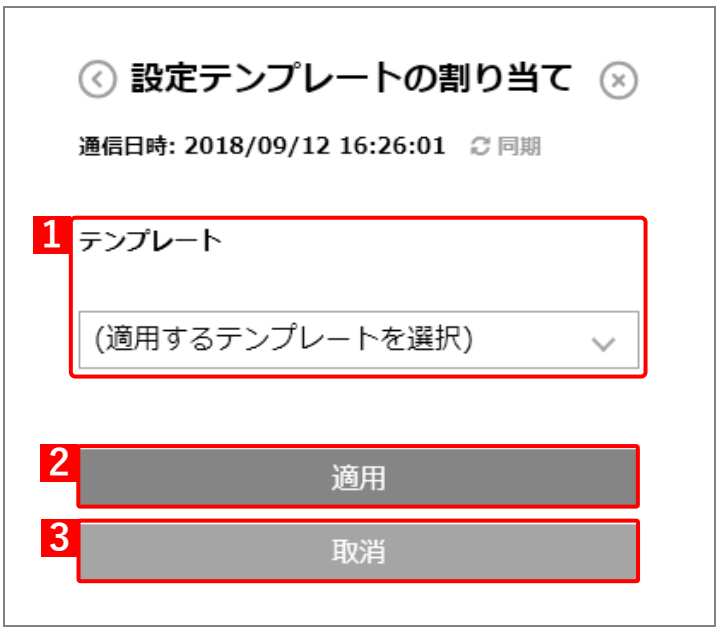
テンプレートは、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

対象の Android 端末に割り当てる設定テンプレートの作成は、以下を参照してください。

☞「設定テンプレート」300 ページ

◆画面

表示操作 ［機器］→［一覧］→Android 端末の機器名または「詳細」の ⊙ →詳細画面の「設定」の［設定テンプレートの割り当て］



項番	項目	説明
1	テンプレート	適用するテンプレートをリストボックスから選択します。
2	［適用］	クリックすると、設定したテンプレートの設定内容が対象の機器に適用されます。
3	［取消］	クリックすると、設定テンプレートの割り当てをキャンセルします。

4.1.8.3 （設定－Android）パッケージ

オプションで契約したアプリを、対象の Android 端末で使用できるようにします。

オプションパッケージは、指定した端末でのみ利用できます。

使用数が契約数に達している場合は、新たにオプションパッケージを割り当てることができません。使用数および契約数は、ダッシュボードの「利用状況」で確認してください。

「ダッシュボードの画面構成」38 ページ

◆画面

表示操作　**［機器］→［一覧］→Android 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［パッケージ］→［編集］**

項番	項目	説明
1	オプションパッケージ	利用できるオプションパッケージの一覧が表示されます。 対象の端末で利用するパッケージにチェックを入れます。 利用を解除する場合は、チェックを外します。 1 つの機器に同じパッケージを複数割り当てて［保存］をクリックすると、エラーメッセージが表示されます。
2	［保存］	クリックすると、オプションパッケージの割り当てや解除の内容が対象の端末に適用されます。
3	［取消］	クリックすると、オプションパッケージの割り当てをキャンセルします。

4.1.8.4 （設定－Android）クライアント証明書

クライアント証明書を対象の Android 端末に配信します。

画面（新規設定）

画面（編集、削除）

本機能はクライアント証明書の配信までを行います。端末内に保存されるクライアント証明書の場所やインストール方法については、端末メーカーへ問い合わせてください。

配信するクライアント証明書を、あらかじめ管理サイトへアップロードし、本機能で端末に配信するための設定セットを作成してください。クライアント証明書の設定セット作成については、以下を参照してください。

「クライアント証明書管理」348 ページ

「クライアント証明書一括アップロード」352 ページ

クライアント証明書がアップロードされていない場合は、クライアント証明書の設定画面に［クライアント証明書をアップロードする］が表示され、クリックすると［クライアント証明書管理］画面が表示されます。

「クライアント証明書管理」348 ページ

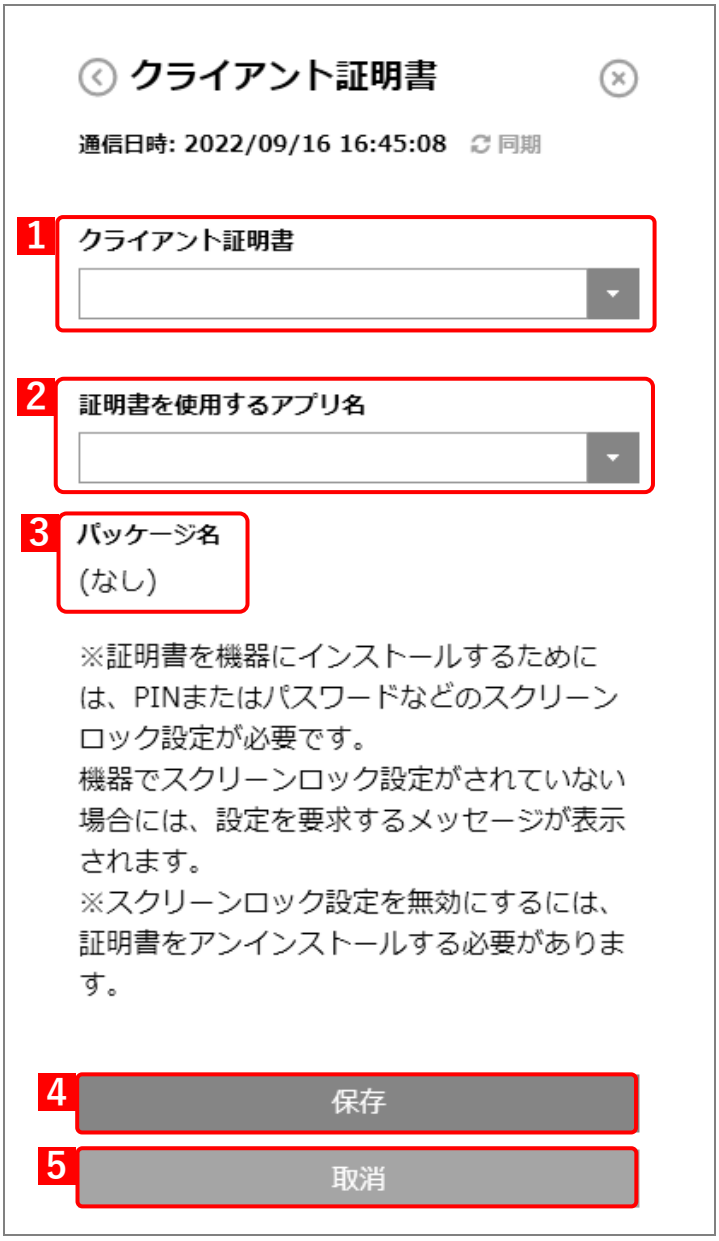
クライアント証明書を Android 端末にインストールするには、PIN またはパスワードなどのスクリーンロック設定が必要です。

管理サイトでクライアント証明書を削除した場合、Android 端末のクライアント証明書は削除されません。また、管理サイトでクライアント証明書を変更した場合は、新規のクライアント証明書として配信されます。Android 端末のクライアント証明書は、変更および削除されません。

「クライアント証明書管理」348 ページ

◆画面（新規設定）

表示操作［機器］→［一覧］→Android 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］→［編集］



項番	項目	説明
1	クライアント証明書	インストールするクライアント証明書をリストボックスから選択します。
2	証明書を使用するアプリ名	項番【1】で選択したクライアント証明書を使用するアプリをリストボックスから選択します。 リストボックスには、個別アプリケーションで登録したアプリが表示されます。使用するアプリは、個別アプリケーションに登録してください。 「Android Enterprise／個別アプリケーション」333 ページ
3	パッケージ名	項番【2】で選択したクライアント証明書を使用するアプリを選択すると、選択したアプリのパッケージ名が自動で表示されます。

項番	項目	説明
4	［保存］	クリックすると、選択したクライアント証明書が Android 端末にインストールされます。 クライアント証明書を機器にインストールするためには、PIN またはパスワードなどのスクリーンロック設定が必要です。機器でスクリーンロック設定がされていない場合は、設定を要求するメッセージが表示されます。 スクリーンロック設定を無効にするには、クライアント証明書をアンインストールする必要があります。
5	［取消］	クリックすると、クライアント証明書の設定をキャンセルします。

◆画面（編集、削除）

表示操作　**［機器］→［一覧］→Android 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］**

項番	項目	説明
1	証明書を使用するアプリ名	クライアント証明書を使用するアプリ名が表示されます。
2	パッケージ名	項番【1】のクライアント証明書を使用するアプリのパッケージ名が表示されます。
3	ファイル名	クライアント証明書のファイル名が表示されます。

項番	項目	説明
4	発行先（証明書情報）	クライアント証明書の発行先が表示されます。
5	発行者（証明書情報）	クライアント証明書の発行者が表示されます。
6	有効期限（証明書情報）	クライアント証明書の有効期限が表示されます。
7	［編集］	クリックすると、クライアント証明書の編集ができます。 画面の操作は、新規設定と同様です。
8	［削除］	クライアント証明書を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.8.5 （設定－iOS）設定の割り当て

各機能で作成した設定セットを iOS 端末に反映します。

設定セットの内容は、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

画面

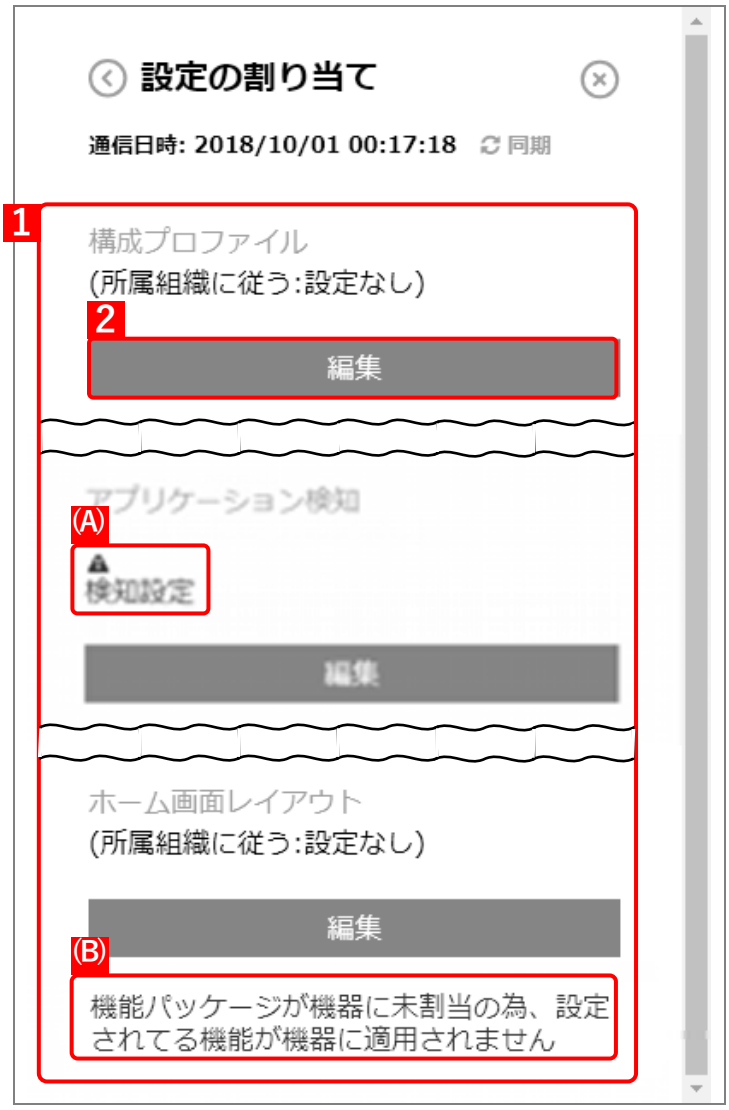
画面（編集）

登録されている iOS 端末に一括で設定セットを反映する場合は、以下を参照してください。

「［iOS 設定］タブ」204 ページ

◆画面

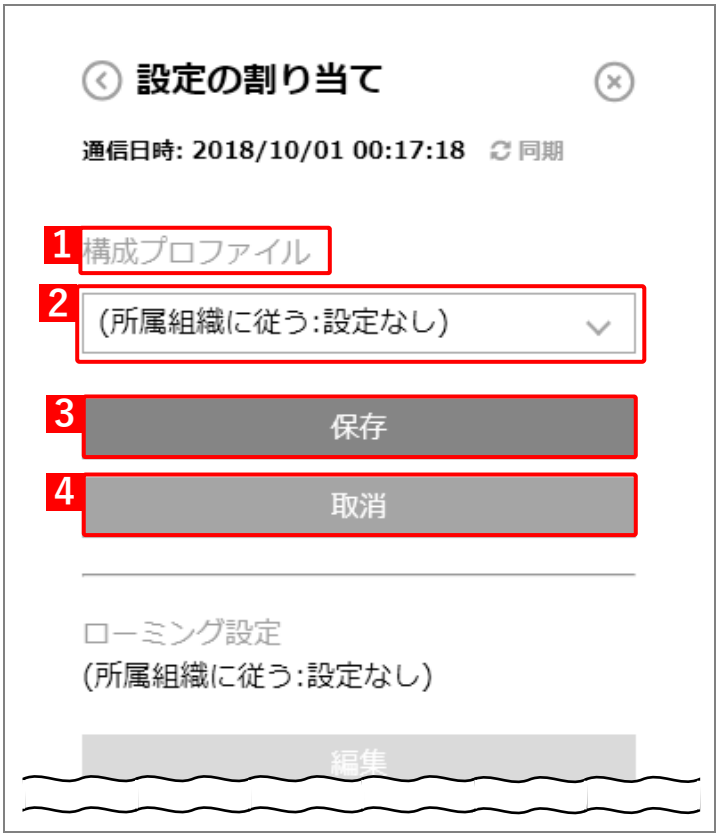
表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［設定の割り当て］**



項番	項目	説明
1	設定一覧	iOS 端末への各設定機能と設定中の設定セット名などが表示されます。 設定機能名をクリックすると、該当の設定画面に遷移します。 機器個別の設定画面で設定しているにもかかわらず、機器オプションパッケージを機器に割り当てていない場合は、（A）（B）の警告が表示されます。
2	［編集］	クリックすると、設定機能ごとに、適用する設定を変更できます。 「画面（編集）」84 ページ

◆画面（編集）

表示操作［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［設定の割り当て］→対象の機能の［編集］



項番	項目	説明
1	設定機能	クリックすると、該当の機能の設定セットの一覧画面に遷移します。
2	(所属組織に従う:設定なし)	適用する設定セット名をリストボックスから選択します。 ●(所属組織に従う:設定なし) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(設定なし) 各機能の設定を外します。 ●各機能の設定名 各機能で作成済みの設定セットを適用したいときは、その設定名をリストボックスから選択して設定します。ここで設定した設定セットに対する編集および削除が行われた場合、この設定にも反映されます。
3	［取消］	クリックすると、編集作業をキャンセルします。
4	［保存］	クリックすると、設定内容を保存します。

4.1.8.6 （設定－iOS）設定テンプレートの割り当て

設定テンプレート機能で作成したテンプレートを iOS 端末に反映します。

テンプレートは、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

対象の iOS 端末に割り当てる設定テンプレートの作成は、以下を参照してください。

☞「設定テンプレート」387 ページ

◆画面

表示操作［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「設定」の［設定テンプレートの割り当て］**

項番	項目	説明
1	テンプレート	適用するテンプレートをリストボックスから選択します。
2	［適用］	クリックすると、設定したテンプレートの設定内容が対象の機器に適用されます。
3	［取消］	クリックすると、設定テンプレートの割り当てをキャンセルします。

4.1.8.7 （設定－iOS）クライアント証明書

対象の iOS 端末にクライアント証明書を紐づけます。クライアント証明書は、各 iOS 端末に最大で 5 つ（デフォルトのクライアント証明書 1 つ、およびその他のクライアント証明書 4 つ）まで紐づけることができます。

画面（新規設定）

画面（編集、削除）

「構成プロファイルアップロード」の Wi-Fi 設定で「機器に設定されているクライアント証明書」を設定していて、端末でデフォルトのクライアント証明書が未設定の場合、証明書がインストールされません。設定した Wi-Fi の接続ができない場合があります。

［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→［iOS 制限設定］タブで、「Wi-Fi ペイロードによってインストールされた Wi-Fi ネットワークのみに接続(監視対象のみ)」にチェックを入れていて、Wi-Fi のみを利用している端末が他の Wi-Fi のアクセスポイントを 1 つも登録していない場合、同期ができなくなるので、注意してください。

「復旧方法」407 ページ

端末でデフォルトのクライアント証明書に設定して、他の環境を接続して［同期］すると、証明書がインストールされます。

各端末に紐づける 1 つ目のクライアント証明書は、その端末のデフォルトのクライアント証明書です。

機器レポートでは、「クライアント証明書」としてデフォルトのクライアント証明書のみ出力されます。

「機器レポート」237 ページ

機器に紐づいているすべてのクライアント証明書は、［CSV でクライアント証明書紐付け］からダウンロードできる CSV ファイルで確認できます。

「CSV でクライアント証明書紐付け（iOS のみ）」235 ページ

iOS 12.0 以上の端末の場合は、本機能からインストールしたクライアント証明書を VPN アプリから参照できるようにするには、VPN 設定を作成して端末に配信する必要があります。

- ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］

このとき、「資格情報」は「(機器に設定されているクライアント証明書)」に設定してください。詳細については、下記を参照してください。

「［その他▼］タブ／VPN 設定」435 ページ

デフォルトのクライアント証明書は、「構成プロファイルアップロード」の VPN 設定などで「機器に設定されたクライアント証明書」と設定されている場合に参照できます。

「構成プロファイルアップロード」393 ページ

◆画面（新規設定）

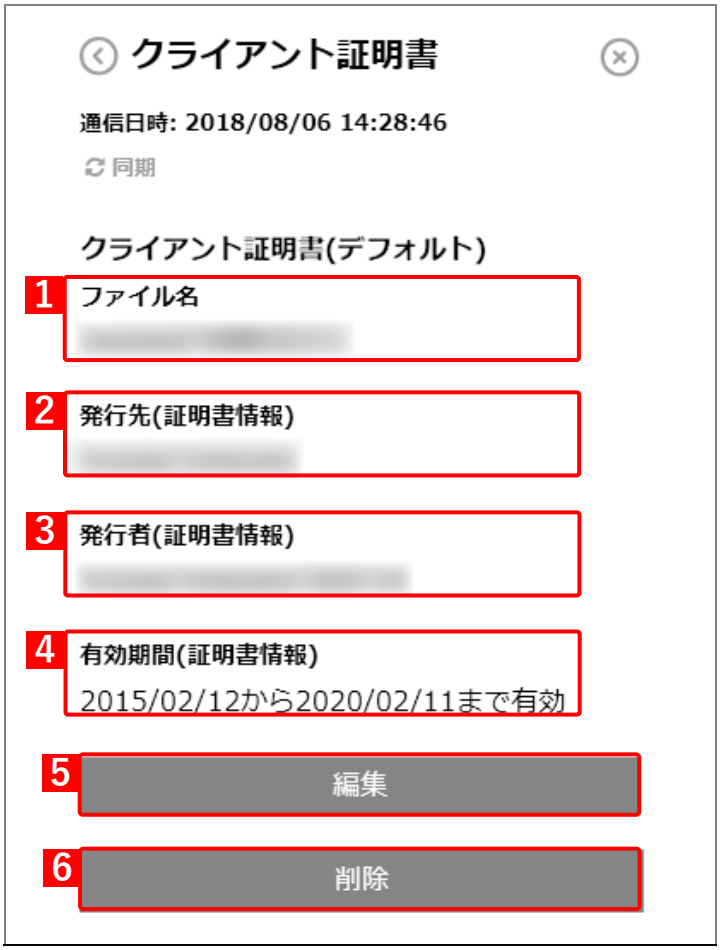
表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］→［編集］**

項番	項目	説明
1	クライアント証明書（※1）	対象の iOS 端末にインストールするクライアント証明書をリストボックスから選択します。
2	［保存］	クリックすると、選択したクライアント証明書が、iOS 端末にインストールされます。
3	［取消］	クリックすると、クライアント証明書の設定をキャンセルします。

※1：端末に紐づける最初のクライアント証明書の場合は、「クライアント証明書（デフォルト）」と表示されます。

◆画面（編集、削除）

表示操作［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］



項番	項目	説明
1	ファイル名	クライアント証明書のファイル名が表示されます。
2	発行先（証明書情報）	クライアント証明書の発行先が表示されます。
3	発行者（証明書情報）	クライアント証明書の発行者が表示されます。
4	有効期限（証明書情報）	クライアント証明書の有効期限が表示されます。
5	［編集］	クリックすると、クライアント証明書の編集ができます。 画面の操作は、新規設定と同様です。
6	［削除］	クライアント証明書を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 デフォルトのクライアント証明書を、すでに紐づけられているほかのクライアント証明書に変更できます。その場合は、デフォルトに指定したいクライアント証明書を一旦削除して、「クライアント証明書（デフォルト）」の［編集］－「クライアント証明書」で該当のクライアント証明書を選択します。

4.1.8.8 （設定－iOS）Exchange（ActiveSync）設定

Microsoft Exchange を利用する場合に、Exchange ActiveSync の設定を端末ごとに行うことができます。

本画面で行う設定は、Apple Configurator 2 の［Exchange ActiveSync］で行う設定と同様です。

画面（新規作成）

画面（編集、削除）

配信するクライアント証明書を、あらかじめ管理サイトへアップロードし、本機能で端末に配信するための設定セットを作成してください。クライアント証明書の設定セット作成については、以下を参照してください。

「クライアント証明書管理」553 ページ

「クライアント証明書一括アップロード」557 ページ

クライアント証明書がアップロードされていない場合は、クライアント証明書の設定画面に［クライアント証明書をアップロードする］が表示され、クリックすると［クライアント証明書管理］画面が表示されます。

「クライアント証明書管理」553 ページ

複数の機器に一括して Exchange（ActiveSync）設定を行う場合は、Apple Configurator 2 の［Exchange ActiveSync］で設定をしてください。または CSV ファイルを利用して一括で設定してください。

「CSV で編集」232 ページ

Apple Configurator 2 の詳細については、Apple に問い合わせてください。

Microsoft Exchange および Exchange ActiveSync の詳細については、Microsoft に問い合わせてください。

各種設定は次回の同期時に端末へ反映されます。端末への反映を急ぐ場合は、手動で同期を行ってください。

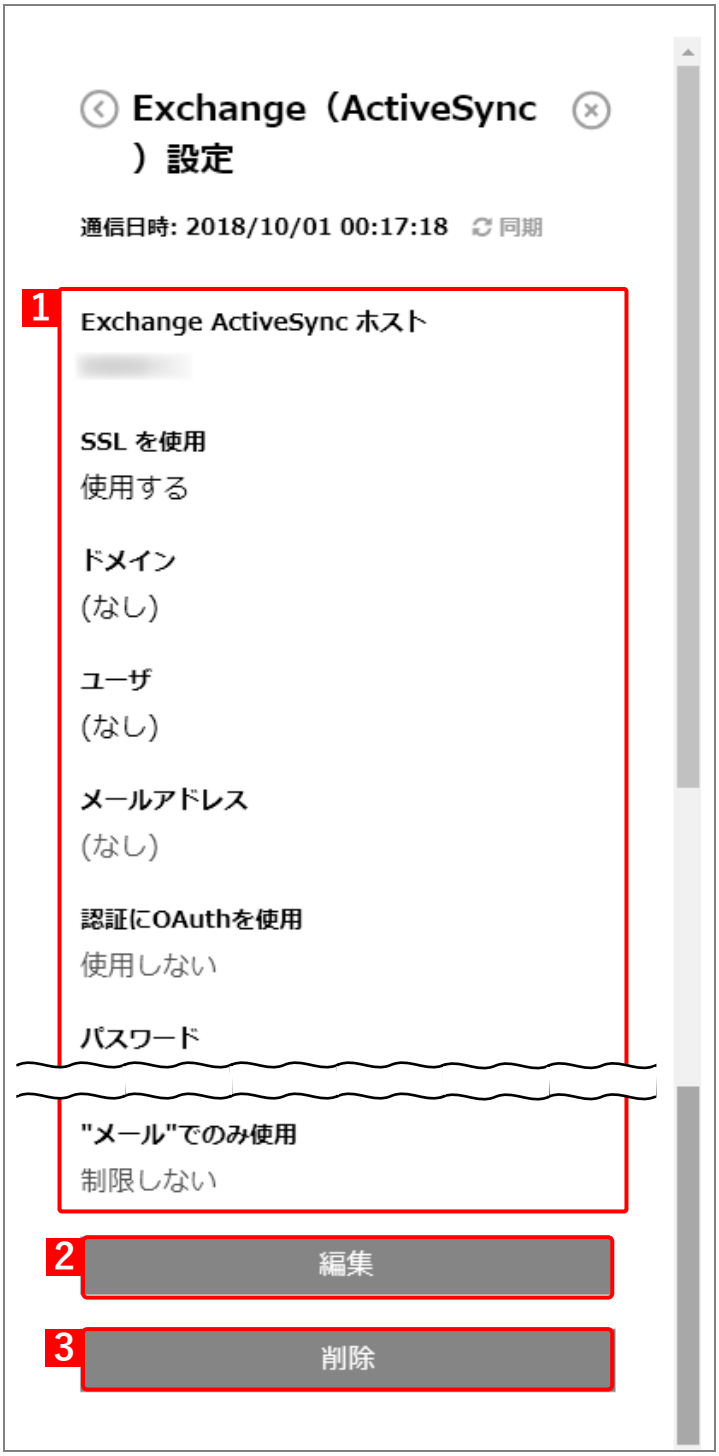
◆画面（新規作成）

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［他の設定を見る］→［Exchange（ActiveSync）設定］→［新規作成］**

項番	項目	説明
1	設定項目	以下の項目を設定します。 設定項目の詳細については、Exchange の管理者に問い合わせてください。 ●Exchange ActiveSync ホスト Exchange ActiveSync ホスト名を入力します。 Exchange ActiveSync ホスト名は、Microsoft に問い合わせてください。 ●SSL を使用 「使用する」または「使用しない」を選択します。 ●ドメイン ドメイン名を入力します。 ●ユーザー情報 ・所属ユーザーの情報を利用 利用する場合は、チェックボックスにチェックを入れてください。 ●ユーザ 「所属ユーザーの情報を利用」が無効の場合は、ユーザー名を入力します。 ●メールアドレス 「所属ユーザーの情報を利用」が無効の場合は、メールアドレスを入力します。 ●認証に OAuth 使用 「使用する」または「使用しない」を選択します。 先進認証（OAuth で認証）する場合は、「使用する」を選択します。 ・「使用する」の場合 ・OAuth サインイン URL を入力します。 ・OAuth トークンリクエスト URL を入力します。 ・「使用しない」の場合 ・パスワードを入力します。 ●認証資格情報 リストボックスからクライアント証明書を選択します。 ●過去のメールを同期（日数） 「無制限」、「1 日」、「3 日間」、「1 週間」、「2 週間」、「1 か月」から選択します。 ●メッセージの移動を許可 「許可する」または「許可しない」を選択します。 ●最近使ったアドレスの同期を許可 「許可する」または「許可しない」を選択します。 ●Mail Drop を許可 「許可する」または「許可しない」を選択します。 ●"メール"でのみ使用 「"メール"でのみ使用する」または「制限しない」を選択します。
2	［保存］	クリックすると、Exchange の設定内容が対象の機器に適用されます。
3	［取消］	クリックすると、Exchange の設定をキャンセルします。

◆画面（編集、削除）

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［他の設定を見る］→［Exchange（ActiveSync）設定］**



項番	項目	説明
1	設定内容	以下の設定内容を確認します。 ●Exchange ActiveSync ホスト ●SSL を使用 ●ドメイン ●ユーザー情報 ・所属ユーザーの情報を利用 ●ユーザ 「所属ユーザーの情報を利用」が無効の場合 ●メールアドレス 「所属ユーザーの情報を利用」が無効の場合 ●認証に OAuth 使用 ・「使用する」の場合 ・OAuth サインイン URL ・OAuth トークンリクエスト URL ・「使用しない」の場合 ・パスワード ●認証資格情報 ●過去のメールを同期（日数） ●メッセージの移動を許可 ●最近使ったアドレスの同期を許可 ●Mail Drop を許可 ●"メール"でのみ使用
2	［編集］	クリックすると、Exchange の設定内容の編集ができます。 画面の操作は、新規作成と同様です。
3	［削除］	Exchange の設定を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.8.9 （設定－iOS）VPN 設定

VPN を利用する場合の設定を、iOS 端末ごとに行います。

画面（新規作成）

画面（編集、削除）

本画面で行う設定は、Apple Configurator 2 の［VPN］で行う設定とほぼ同様ですが、接続タイプは以下に対応しています。

- IKEv2
- IPSec
- L2TP
- PPTP（iOS 10 未満と OS X 10.12 未満）
- Cisco AnyConnect
- Cisco Legacy AnyConnect（iOS12 未満）
- Juniper SSL
- Pulse Secure
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- Check Point Mobile VPN
- カスタム SSL

Apple Configurator 2 の詳細については、Apple に問い合わせてください。

存在しない識別子を入力した場合、VPN 設定が端末に反映されず構成プロファイルのインストールに失敗することがあります。識別子は VPN 装置ベンダーごとに異なるため、VPN 装置ベンダーへご確認ください。

クライアント証明書を、あらかじめ管理サイトへアップロードし、本画面の設定項目（「固有名証明書」または「資格情報」）で選択するための設定セットを作成してください。接続タイプにより、設定項目が異なりますので、以下を参照してください。

設定項目	接続タイプ
固有名証明書	●IKEv2 ●IPSec ●L2TP
資格情報	●Cisco AnyConnect ●Cisco Legacy AnyConnect（iOS12 未満） ●Juniper SSL ●Pulse Secure ●F5 SSL ●SonicWALL Mobile Connect ●Aruba VIA ●Check Point Mobile VPN ●カスタム SSL

クライアント証明書の設定セット作成については、以下を参照してください。

「クライアント証明書管理」553 ページ

「クライアント証明書一括アップロード」557 ページ

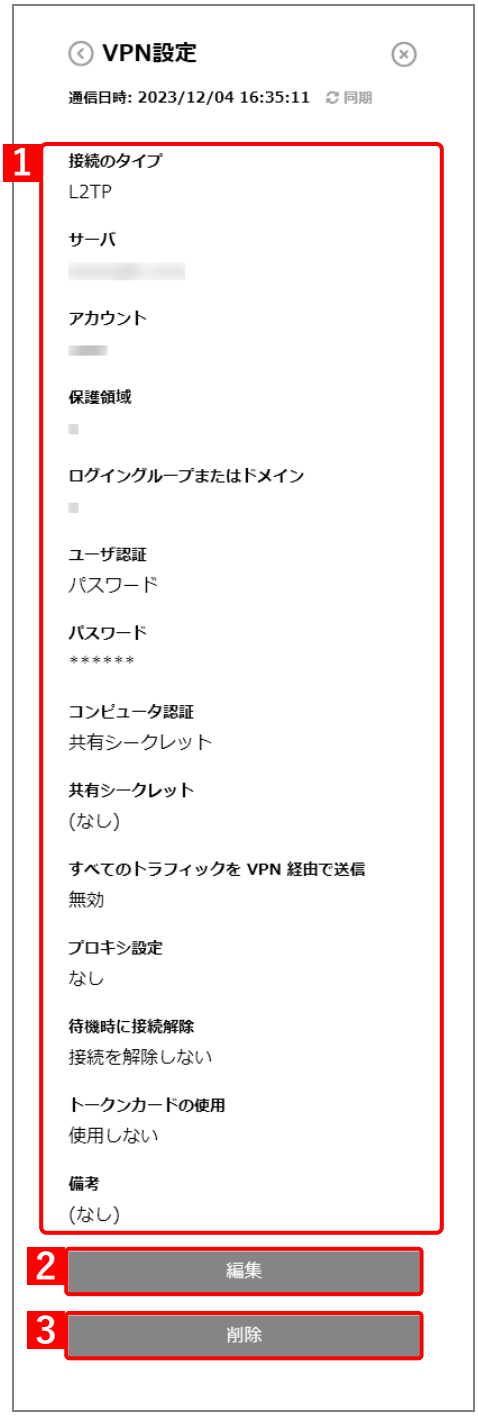
◆画面（新規作成）

表示操作　［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［他の設定を見る］→［VPN 設定］→［新規作成］

項番	項目	説明
1	接続のタイプ	接続タイプを以下から選択します。以降の入力項目は接続タイプごとに異なります。 ・IKEv2 ・IPSec ・L2TP ・PPTP（iOS 10 未満と OS X 10.12 未満） ・Cisco AnyConnect ・Cisco Legacy AnyConnect（iOS12 未満） ・Juniper SSL ・Pulse Secure ・F5 SSL ・SonicWALL Mobile Connect ・Aruba VIA ・Check Point Mobile VPN ・カスタム SSL
2	サーバ	サーバーの名称を 255 文字以内の半角英数字、記号で入力します。入力は必須です。
3	設定項目	入力項目は接続タイプごと表示項目が異なります。 設定項目については以下を参照してください。 ☞「[その他▼］タブ／VPN 設定」435 ページ
4	備考	必要に応じて、255 文字以内で入力してください。
5	［保存］	クリックすると、VPN の設定内容が対象の機器に適用されます。
6	［取消］	クリックすると、VPN の設定をキャンセルします。

◆画面（編集、削除）

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［他の設定を見る］→［VPN 設定］**



項番	項目	説明
1	設定内容	設定内容を確認します。接続のタイプによって、項目が異なります。
2	［編集］	クリックすると、VPN 設定の編集ができます。画面の操作は、新規作成と同様です。
3	［削除］	VPN の設定を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.8.10 （設定－iOS）個別構成プロファイル

Apple が提供している Apple Configurator 2 で作成した構成プロファイルを、個別にアップロードして iOS 端末にインストールします。iOS 端末で構成プロファイルをインストールすることで端末の制御や設定を行うことができます。構成プロファイルは、あらかじめ Apple Configurator 2 上で作成してください。

画面（新規作成）

画面（ダウンロード、編集、削除）

Apple Configurator 2 および構成プロファイルの詳細については、Apple に問い合わせてください。

複数の iOS 端末に一括で同じ構成プロファイルをインストールする場合は、必要な構成プロファイルをアップロードし、構成プロファイルの設定セットを作成してから、全端末に一括設定を行ってください。
詳細については、以下を参照してください。

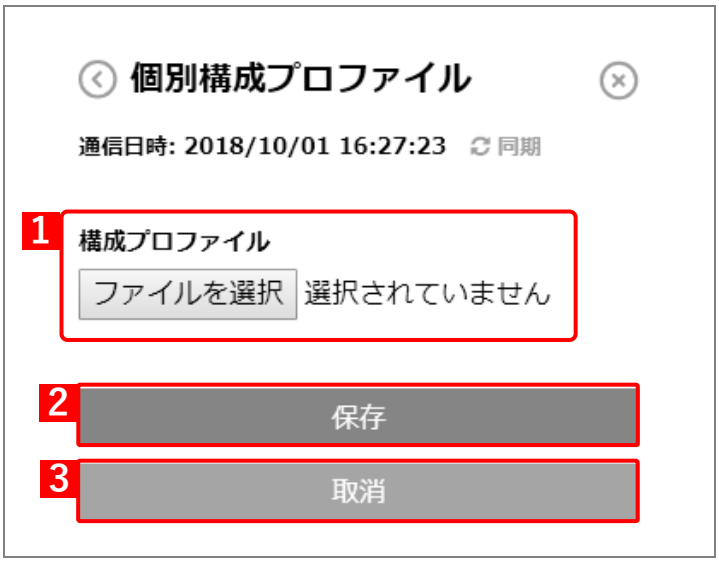
「構成プロファイルアップロード」393 ページ

「構成プロファイル」500 ページ

「全機器一括設定」200 ページ

◆画面（新規作成）

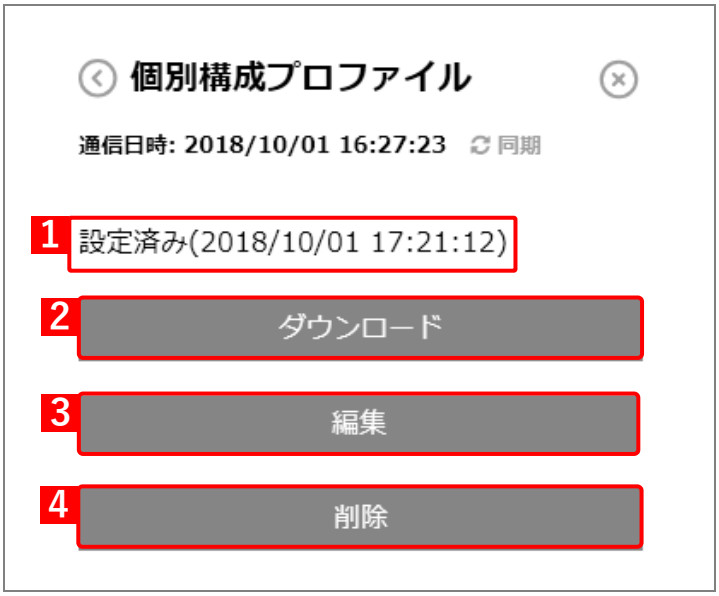
表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［個別構成プロファイル］→［新規作成］**



項番	項目	説明
1	構成プロファイル	［ファイルを選択］をクリックし、構成プロファイルのファイルを選択します。ファイルを選択すると、選択したファイル名が表示されます。
2	［保存］	クリックすると、選択したプロファイルが、対象の機器に適用されます。
3	［取消］	クリックすると、個別構成プロファイルの設定をキャンセルします。

◆画面（ダウンロード、編集、削除）

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［個別構成プロファイル］**



項番	項目	説明
1	設定済み	個別構成プロファイルが設定された日時が表示されます。
2	ダウンロード	クリックすると、設定されている構成プロファイルをダウンロードできます。
3	［編集］	クリックすると、個別構成プロファイルの編集ができます。 画面の操作は、新規作成と同様です。
4	［削除］	個別構成プロファイルを削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.8.11 （設定－iOS）「App とブック」設定

端末に対する「App とブック」ライセンスの配布状況を確認・管理します。

画面（新規作成）

画面（編集、削除）

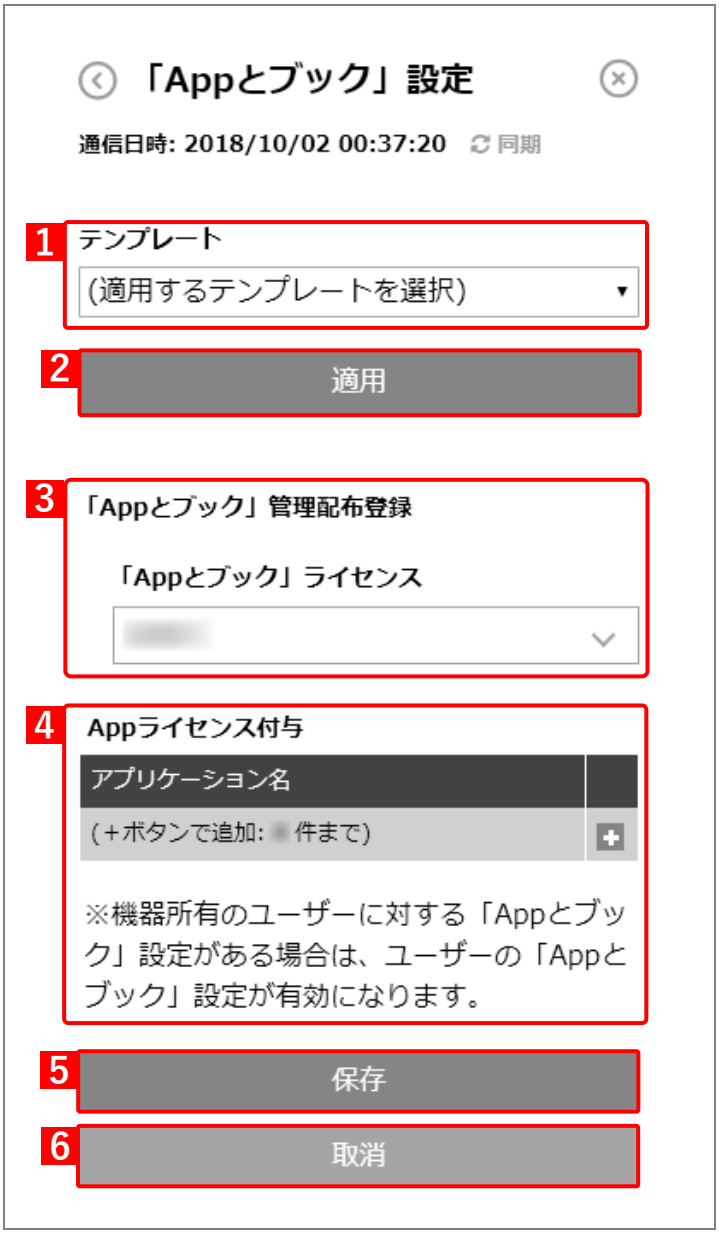
本機能で割り当てたライセンスは、「「App とブック」ライセンス」の［アプリケーション］タブで「未割当数」としてカウントされます。この状態で実際にライセンスは付与されていません。詳細については、以下を参照してください。

「［アプリケーション］タブ」518 ページ

ユーザー（または組織）画面でユーザーに「App とブック」ライセンスを付与している場合は、ユーザーの付与が優先されるため、機器に紐づいたユーザーのライセンス付与の状態が表示されます。本画面で編集できません。

◆画面（新規作成）

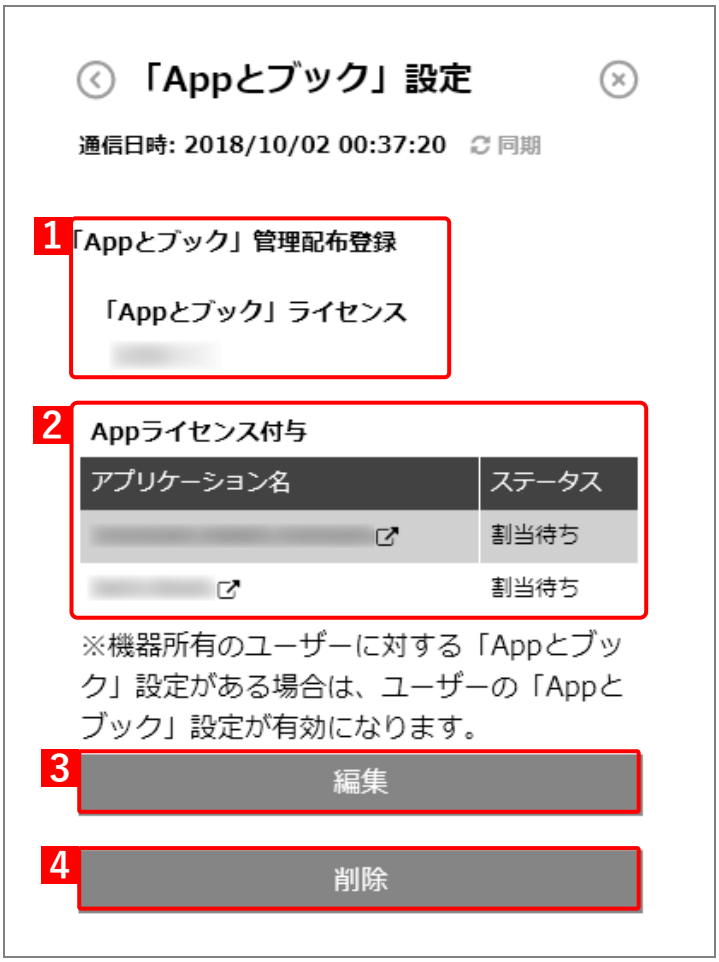
表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の → 詳細画面の「設定」の［他の設定を見る］→［「App とブック」設定］→［新規作成］**



項番	項目	説明
1	テンプレート	登録済みの「App とブック」設定テンプレートを適用して、設定する場合は、リストボックスからテンプレートを選択します。
2	［適用］	クリックすると、選択した「App とブック」設定テンプレートの内容が、【3】と【4】の設定項目に反映されます。
3	「App とブック」管理配布登録	「App とブック」ライセンスで、リストボックスから「App とブック」アカウントを選択します。
4	App ライセンス付与	●アプリケーション名 アプリをリストボックスから選択します。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。 ABM で購入したアプリの件数が表示されます。アプリは最大 300 件まで購入できます。
5	［保存］	クリックすると、「App とブック」の設定内容が対象の機器に適用されます。
6	［取消］	クリックすると、「App とブック」の設定をキャンセルします。

◆画面（編集、削除）

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の → 詳細画面の「設定」の［他の設定を見る］→［「App とブック」設定］**



項番	項目	説明
1	「App とブック」管理配布登録	「App とブック」ライセンスで、リストボックスから「App とブック」アカウントを選択します。
2	App ライセンス付与	以下の情報が表示されます。 ●アプリケーション名 対象のアプリ名が表示されます。クリックすると、アプリのサイトが表示されます。 ●ステータス 現在のライセンス付与の割り当て状況が表示されます。 ・割当済 ライセンスが割り当てられている ・割当待ち ライセンスが割り当てられていない ・ライセンス残数 0 ライセンスが割り当てられておらず、ライセンスの残数が 0 になっている ABM で「App とブック」ライセンスを購入するか、不要な「App とブック」ライセンスを機器、ユーザー、組織から外して、再度割り当てを行ってください。
3	［編集］	クリックすると、「App とブック」設定の編集ができます。画面は、新規作成と同様です。
4	［削除］	「App とブック」設定を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

◆エラー一覧

文言	発生契機	対処方法
⚠ アプリケーションは重複しないものを入力してください。	「App ライセンス付与」欄で［+］でアプリを追加するときに、アプリ名が重複している。	重複しているアプリを設定から削除し、［保存］をクリックしてください。
⚠ 書籍は重複しないものを入力してください。	「ブックライセンス付与」欄で[+]で書籍を追加するときに書籍名が重複している。	重複している書籍を設定から削除し、［保存］をクリックしてください。

4.1.8.12 （設定－Windows）設定セットの割り当て

各機能で作成した設定セットを Windows 端末に反映します。

設定セットの内容は、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

画面

画面（編集）

登録されている Windows 端末に一括で設定セットを反映する場合は、以下を参照してください。

「［Windows 設定］タブ」205 ページ

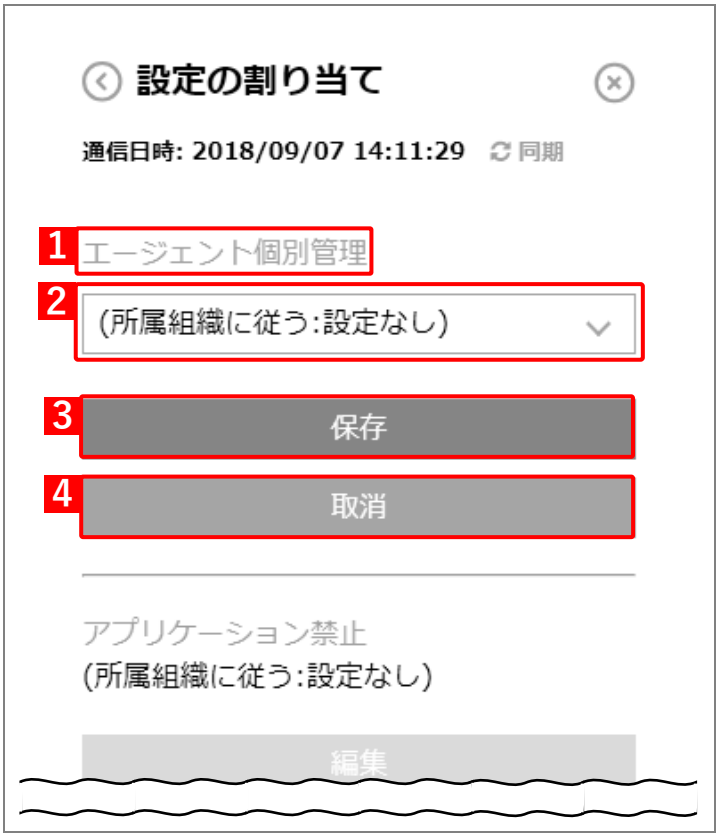
◆画面

表示操作 **［機器］→［一覧］→Windows 端末の機器名または「詳細」の → 詳細画面の「設定」の［設定の割り当て］**

項番	項目	説明
1	設定一覧	Windows 端末への各設定機能と設定中の設定セット名などが表示されます。設定機能名をクリックすると、該当の設定画面に遷移します。 機器個別の設定画面で設定しているにもかかわらず、機器オプションパッケージを機器に割り当てていない場合は、(A)（B）の警告が表示されます。
2	［編集］	クリックすると、設定機能ごとに適用する設定を変更できます。 「画面（編集）」104 ページ

◆画面（編集）

表示操作 **［機器］→［一覧］→Windows 端末の機器名または「詳細」の → 詳細画面の「設定」の［設定の割り当て］→対象の機能の［編集］**



項番	項目	説明
1	設定機能	クリックすると、該当の機能の設定セットの一覧画面に遷移します。
2	(所属組織に従う:設定なし)	適用する設定セット名をリストボックスから選択します。 ●(所属組織に従う:設定なし) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(設定なし) 各機能の設定を外します。 ●各機能の設定名 各機能で作成済みの設定セットを適用したいときは、その設定名をリストボックスから選択して設定します。ここで設定した設定セットに対する編集および削除が行われた場合、この設定にも反映されます。
3	［保存］	クリックすると、設定内容を保存します。
4	［取消］	クリックすると、編集作業をキャンセルします。

4.1.8.13 （設定－Windows）設定テンプレートの割り当て

設定テンプレート機能で作成したテンプレートを Windows 端末に反映します。

テンプレートは、管理サイトと端末が同期したタイミングで該当の端末に反映されます。

対象の Windows 端末に割り当てる設定テンプレートの作成は、以下を参照してください。

☞「設定テンプレート」564 ページ

◆画面

表示操作 **［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓘ →詳細画面の「設定」の［テンプレートの割り当て］**

項番	項目	説明
1	テンプレート	適用するテンプレートを作成済みの設定テンプレートから選択します。
2	［適用］	クリックすると、設定したテンプレートの設定内容が対象の機器に適用されます。
3	［取消］	クリックすると、設定テンプレートの割り当てをキャンセルします。

4.1.8.14 （設定－Windows）クライアント証明書

クライアント証明書を対象の Windows 端末に配信します。

画面（新規設定）

画面（編集、削除）

本機能はクライアント証明書の配信までを行います。端末内に保存されるクライアント証明書の場所やインストール方法については、端末メーカーへ問い合わせてください。

配信するクライアント証明書を、あらかじめ管理サイトへアップロードし、本機能で端末に配信するための設定セットを作成してください。クライアント証明書の設定セット作成については、以下を参照してください。

「クライアント証明書管理」616 ページ

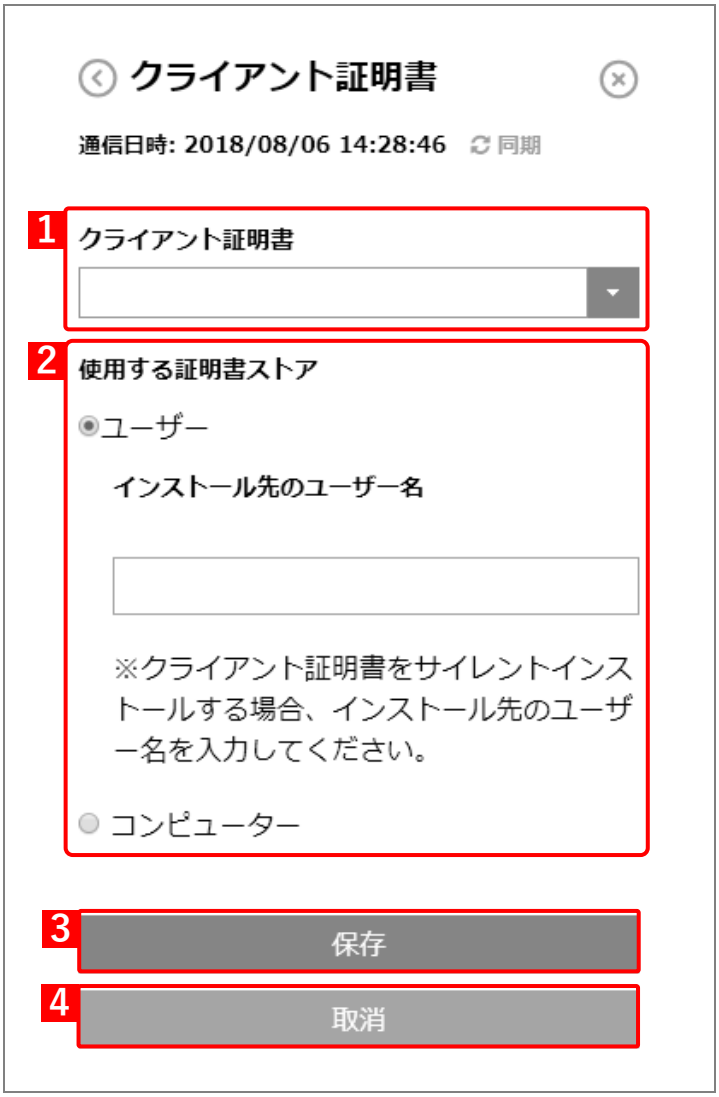
「クライアント証明書一括アップロード」620 ページ

クライアント証明書がアップロードされていない場合は、クライアント証明書の設定画面に［クライアント証明書をアップロードする］が表示され、クリックすると［クライアント証明書管理］画面が表示されます。

「クライアント証明書管理」616 ページ

◆画面（新規設定）

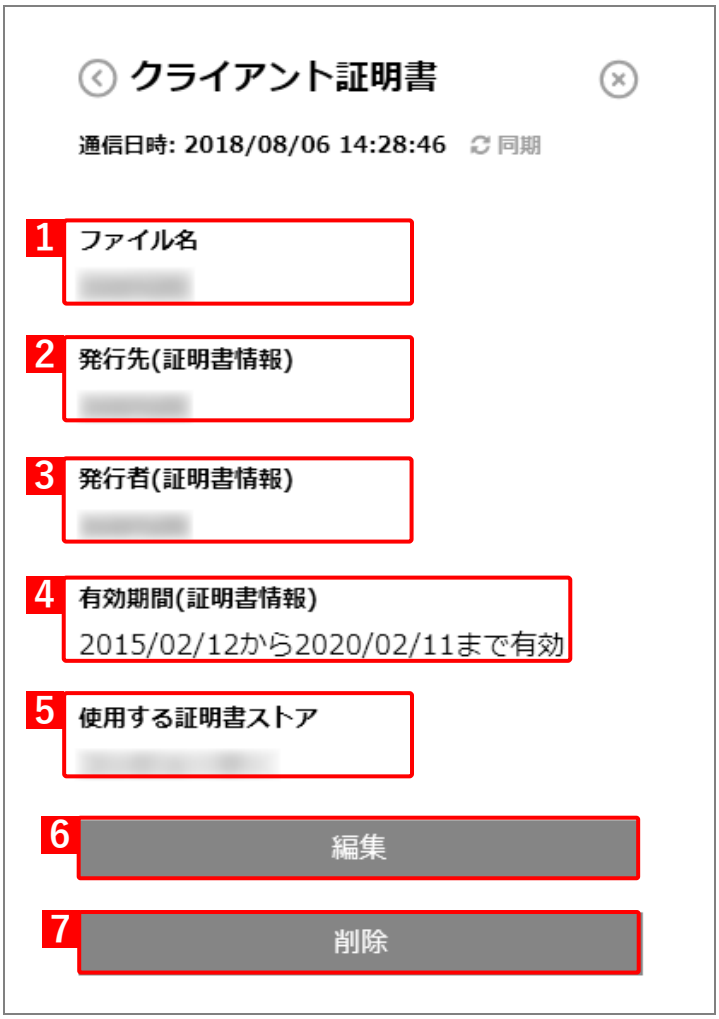
表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］→［編集］**



項番	項目	説明
1	クライアント証明書	対象の Windows 端末にインストールするクライアント証明書をリストボックスから選択します。
2	使用する証明書ストア	クライアント証明書のインストール先を以下から選択します。 ●ユーザー ユーザーを選択した場合、「インストール先のユーザー名」としてクライアント証明書を配布するユーザーを指定します。「ユーザー」が空欄の場合、機器のユーザーはクライアント証明書をインストールするときにインストール先のユーザーを選択できます。 この設定は意図しないユーザーにクライアント証明書を付与してしまう原因となりますので、十分に注意して設定してください。 ●コンピューター クライアント証明書のインストール先をコンピューターにする場合に選択します。
3	［保存］	クリックすると、選択したクライアント証明書が、Windows 端末にインストールされます。
4	［取消］	クリックすると、クライアント証明書の設定をキャンセルします。

◆画面（編集、削除）

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ＞ →詳細画面の「設定」の［他の設定を見る］→［クライアント証明書］**



項番	項目	説明
1	ファイル名	クライアント証明書のファイル名が表示されます。
2	発行先(証明書情報)	クライアント証明書の発行先が表示されます。
3	発行者(証明書情報)	クライアント証明書の発行者が表示されます。
4	有効期間(証明書情報)	クライアント証明書の有効期間が表示されます。
5	使用する証明書ストア	クライアント証明書の使用する証明書ストアが表示されます。
6	［編集］	クリックすると、クライアント証明書の編集ができます。画面の操作は新規設定と同様です。
7	［削除］	クライアント証明書を削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9 機器の操作

各端末の詳細画面から、リモートロックやリモートワイプなど、端末に対する各種操作を行います。

操作可能な機能は OS により異なります。

「操作」の設定内容は、各項目で［実行］をクリックしたタイミングで端末に反映されます。

4.1.9.1 （操作－Android）スクリーンロックパスワード変更

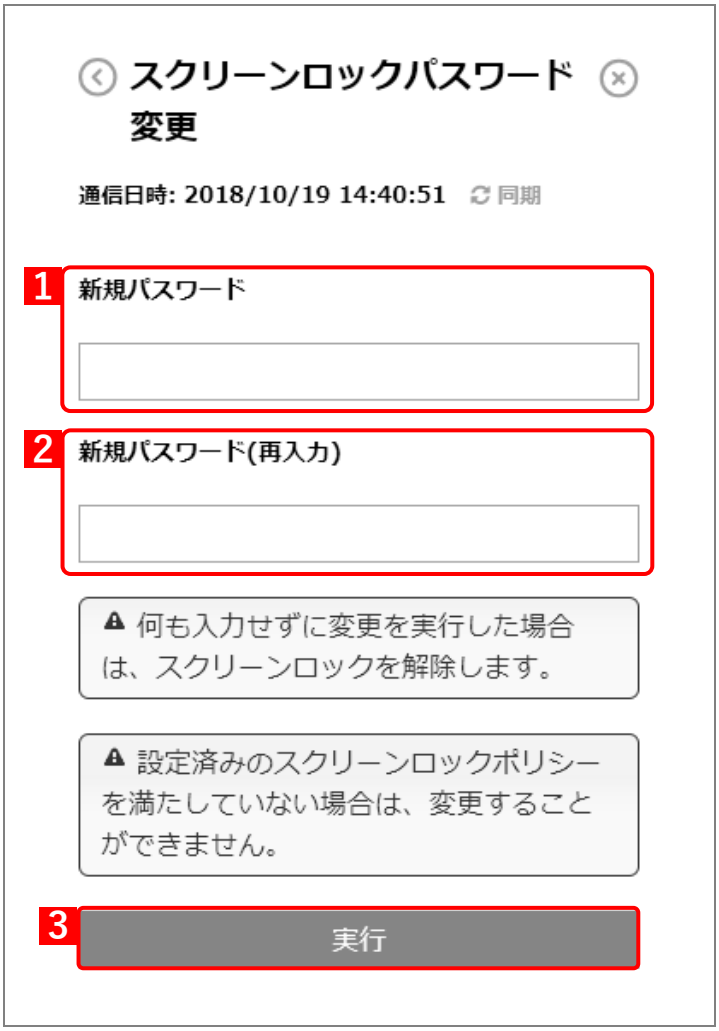
対象の端末に Android 標準のスクリーンロック画面のパスワードを設定します。「新規パスワード」を入力せずに本機能を実行した場合は、スクリーンロックが解除されます。

画面ロック機能で設定したパスワードポリシーを満たしていない場合は、スクリーンロックのパスワードを変更することはできません。画面ロックの詳細については、以下を参照してください。

「画面ロック」304 ページ

◆画面

表示操作　**［機器］→［一覧］→Android 端末の機器名または「詳細」の ⊙ →詳細画面の「操作」の［スクリーンロックパスワード変更］**



項番	項目	説明
1	新規パスワード	パスワードを 16 文字以内の半角英数字、記号で入力します。
2	新規パスワード(再入力)	「新規パスワード」で入力したパスワードを再度入力します。
3	［実行］	端末にスクリーンロックパスワード変更の内容を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.2 （操作－Android）リモートロック

対象の Android 端末をリモートロックします。

リモートロックを行うとロック画面が表示され、端末を操作できなくなります。

また、ロック画面に表示させるメッセージや、警告音の有無なども設定できます。

対象の端末が Android 6.0 以上で、エージェントバージョン 9.3 以上の場合は、Android OS 標準のスクリーンロック画面を表示できます。

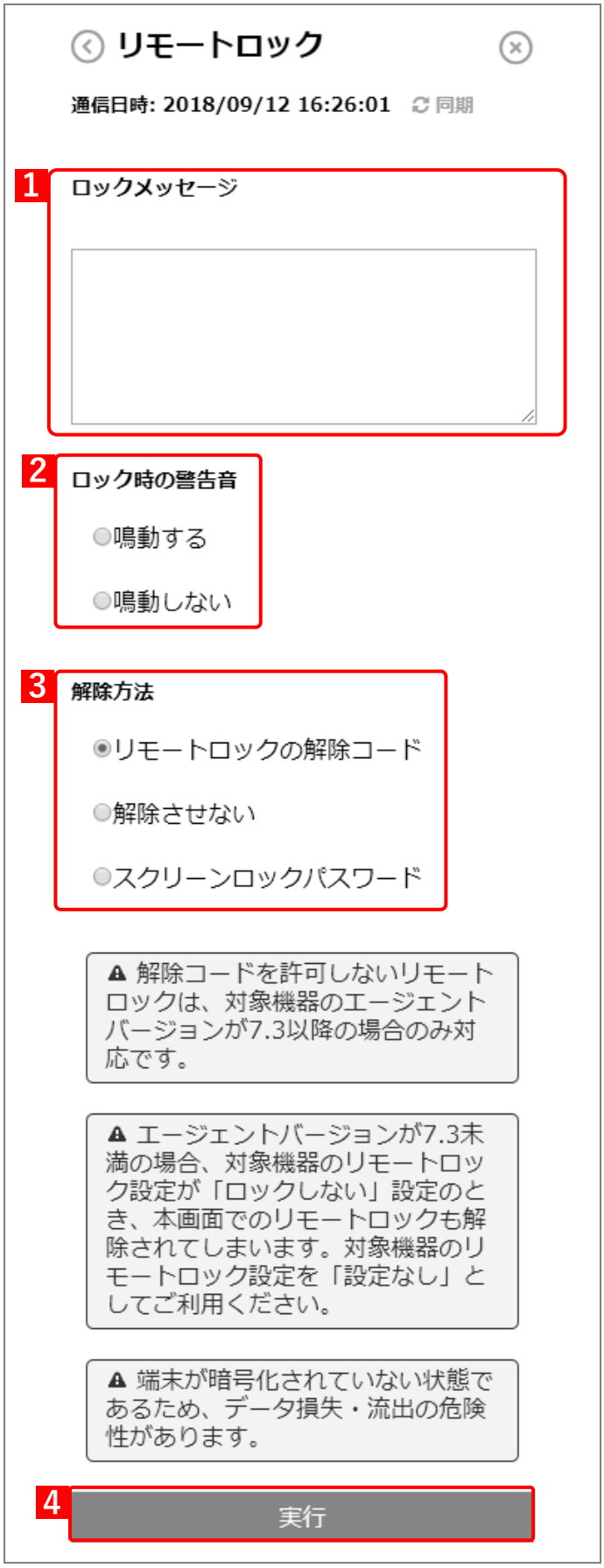
「リモートロック」の設定セットを割り当てて、端末をロックすることもできます。ただし、本機能によるロックが優先されるため、「リモートロック」の設定セットで端末をロック中に本機能でリモートロックを行うと、本機能のロック内容に変更されます。また、本機能でロック中に「リモートロック」の設定セットでロックを行っても、設定セットのロック内容は反映されません。
リモートロックの設定セットの作成については、以下を参照してください。

☞「Android リモートロック」659 ページ

Android 5.0～6.0 の場合、Device Owner Mode 化せずにマルチユーザー機能を使用している端末では、本機能を利用できません。

◆画面

表示操作　**［機器］→［一覧］→Android 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［リモートロック］**



項番	項目	説明
1	ロックメッセージ	ロック画面に表示するメッセージを入力します。入力できる文字数は 200 文字以内です。空白類（タブ、改行など）も入力できます。 解除方法で「スクリーンロックパスワード」を選択した場合は、入力したメッセージの文字数にかかわらず、端末側に表示されるのは、最大で全角 18 文字までです。
2	ロック時の警告音	リモートロックした端末から警告音を鳴らすかどうかを、以下から選択します。 本機能は Android 4.0 以上に対応しています。 ●鳴動する リモートロックされた端末で、警告音を鳴らします。 ロック画面が表示されている間、警告音として端末に設定されている通知音が最大音量で鳴り続けます。本設定にする場合は、十分に注意してください。 イヤホン利用時の動作は機種によって異なります。 ハードウェアスイッチによりサイレントモードになっている端末は鳴動しませんのでご注意ください。 項番【3】「解除方法」を「スクリーンロックパスワード」に選択した場合は、鳴動しません。 ●鳴動しない リモートロックされた端末で、警告音を鳴らしません。
3	解除方法	リモートロックの解除方法を以下から選択します。 エージェントバージョン 7.3 未満の場合、対象機器のリモートロック設定が「ロックしない」設定のとき、本画面でのリモートロックも解除されてしまいます。対象機器のリモートロック設定を「設定なし」として利用してください。 ●リモートロックの解除コード 本製品独自のロック画面を表示してロックします。「リモートロックの解除コード」を端末から入力する、もしくは管理サイトからリモートロック解除を行うことでロック画面を解除できます。 ●解除させない 本製品独自のロック画面を表示してロックします。解除コードの入力で解除できません。管理サイトからリモートロック解除を行うことでロック画面を解除できます。 「解除させない」の設定は、対象機器のエージェントバージョン 7.3 以上の場合にのみ対応しています。 ●スクリーンロックパスワード Android OS 標準のスクリーンロック画面が表示されます。事前に設定したスクリーンロックパスワードによってリモートロックを解除します。管理サイトからリモートロックを解除することはできません。 本設定を選択すると、端末にスクリーンロックパスワードを設定していない場合は、端末がロックされていない状態になります。第三者が端末のデータにアクセスするのを防ぐには、必ず「リモートロックの解除コード」または「解除させない」を選択してください。 端末側に表示できるロックメッセージは、最大で全角 18 文字までです。 端末の通知の設定が「すべての通知内容を表示する」になっていない場合は、メッセージは表示されません。 「スクリーンロックパスワード」の設定項目は、対象の端末が Android 6.0 以上で、エージェントバージョン 9.3 以上の場合にのみ表示されます。
4	［実行］	端末にリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.3 （操作－Android）ロック解除

対象の Android 端末のリモートロックを解除します。

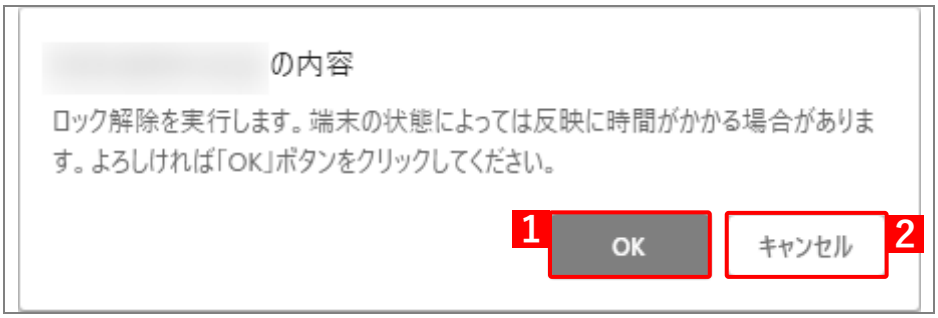
設定セットを利用して行ったリモートロックや、「管理アプリの通信と動作」で設定されたリモートロックを解除します。

「リモートロック」機能で端末をロックしている場合は、「リモートロック」項目で［ロックしない］を選択した設定セットを作成し、端末に同期しても、ロックは解除されません。

☞「Android リモートロック」659 ページ

◆画面

表示操作［機器］→［一覧］→Android 端末の機器名または「詳細」の ›› →詳細画面の「操作」の［他の操作を見る］→［ロック解除］



項番	項目	説明
1	［OK］	クリックすると、対象の端末のリモートロックが解除されます。
2	［キャンセル］	クリックすると、ロック解除の操作をキャンセルします。

4.1.9.4 （操作－Android）リモートワイプ

対象の Android 端末にリモートワイプを行います。

本機能を実行すると対象の端末が初期化されます。

本機能を実行すると操作を取り消すことはできません。十分に注意してください。

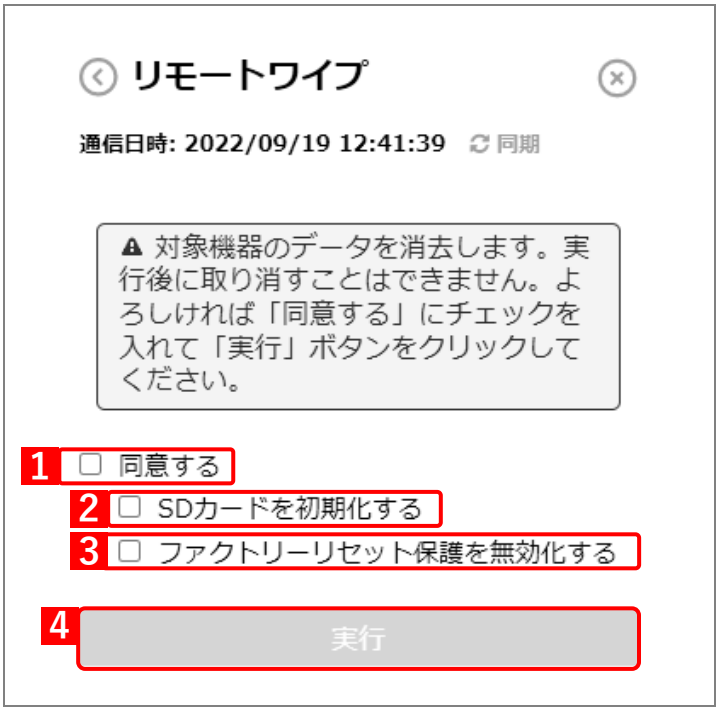
リモートワイプで端末を初期化した場合、端末の OS は初期化したときと同じバージョンになります。
ただし、アップデートの方法や仕様により、初期化する直前の OS バージョンにならない場合もあります。

設定セットを利用しても、リモートワイプができます。
リモートワイプの設定セットの作成については、以下を参照してください。

「Android リモートワイプ」662 ページ

◆画面

表示操作 ［機器］→［一覧］→**Android 端末の機器名または「詳細」の** ⓘ **→詳細画面の「操作」の［他の操作を見る］→［リモートワイプ］**



項番	項目	説明
1	同意する	リモートワイプを実行するには、チェックを入れます。チェックを入れると、項番 4 の［実行］がクリックできるようになります。
2	SD カードを初期化する	ワイプの実行のときに、SD カードも初期化したい場合に、チェックを入れます。
3	ファクトリーリセット保護を無効化する	ワイプを実行する場合に、ファクトリーリセット保護を無効化したいときにチェックを入れます。 ファクトリーリセット保護とは、Android 端末を初期化したとき、Google アカウントの認証が必要になることで、キッティングが完了できないようにすることです。Android 端末の盗難防止になります。
4	［実行］	端末にリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.5 （操作ーAndroid）Google Play ストアのキャッシュ削除

対象の Android 端末の Google Play ストアのキャッシュを削除します。

Android Enterprise で配信したアプリが、Google Play ストア上で「保留中」の状態からインストールされない場合に、本操作を行ってください。

エージェントバージョン 9.14.1 以上かつ Android 9 以上の端末が対象です。

本操作により、「Google Play ストア」アプリ内で変更したすべての設定が初期値に戻ります。設定を初期値から変更している場合は、本操作終了後に端末から再設定してください。「アプリの自動更新」を［アプリを自動更新しない］に設定している場合や、企業で Wi-Fi の使用を制限している場合は、初期値の［Wi-Fi 接続時のみ］に設定されるため、特に注意してください。

アプリ配信設定を設定後に本操作を実施すると、端末側に表示されるアプリ配信設定の内容が一時的に変更前の表示になる場合があります。本操作を行うときは、注意してください。端末やインストールされたアプリに影響はありません。

◆画面

表示操作　**［機器］→［一覧］→Android 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［他の操作を見る］→［Google Play ストアのキャッシュ削除］**

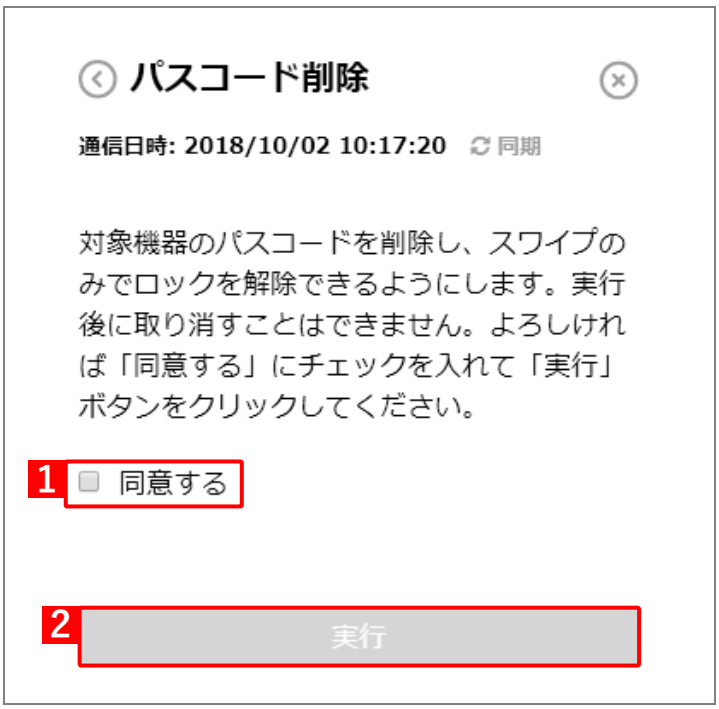
項番	項目	説明
1	［実行］	端末の Google Play ストアのキャッシュを削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.6 （操作－iOS）パスコード削除

対象の iOS 端末に設定されているパスコードを削除します。また、端末のパスコードロックの設定も解除されます。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［パスコード削除］**



項番	項目	説明
1	同意する	パスコードを削除するには、チェックを入れます。チェックを入れると、項番 2 の［実行］がクリックできるようになります。
2	［実行］	端末のパスコードを削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.7 （操作－iOS）リモートロック

対象の iOS 端末をリモートロックします。

リモートロックを行うとロック画面が表示され、端末を操作できなくなります。

また、ロック画面に表示させるメッセージも設定できます。

端末の設定により、ロックから復帰するときにパスコードの入力を求められることがあります。

iOS 端末にパスコードが設定されていない場合、デフォルトのロック解除画面のみが表示されます。このため、「ロックメッセージ」、「電話番号」で設定された連絡情報をユーザーは確認できません。リモートロックを行う前に、詳細画面の「情報」の［デバイス］で「スクリーンロック」の「パスコード保護」が「保護されています」になっているか確認してください。

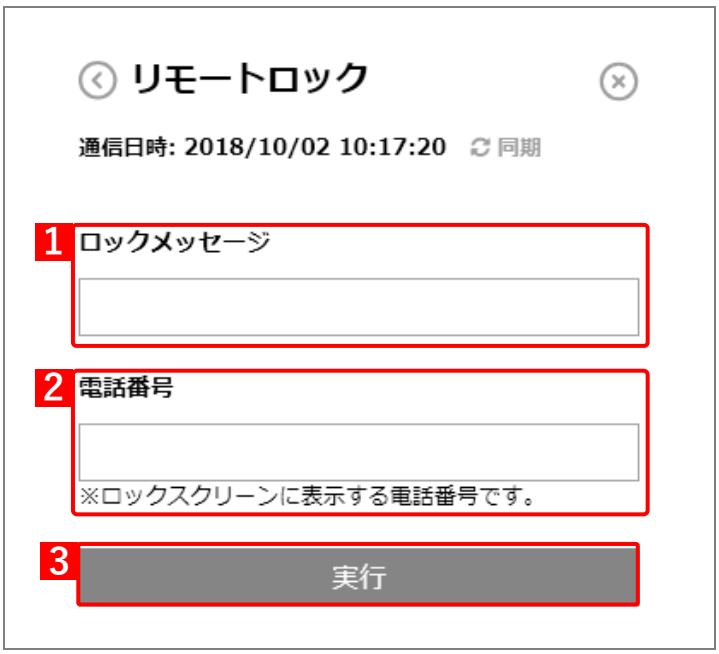
「（情報－iOS）デバイス」151 ページ

iOS 7.0 以下の OS では、「ロックメッセージ」と「電話番号」は表示されません。

管理サイトで、ロックを解除することはできません。ロックを解除するときは、端末にパスワードを入力します。

◆画面

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［リモートロック］**



項番	項目	説明
1	ロックメッセージ	ロック画面に表示するメッセージを入力します。入力できる文字数は 200 文字以内です。空白類（タブ、改行など）も入力できます。
2	電話番号	ロックスクリーンに表示する電話番号を 20 文字以内の半角数字、「-」、「+」、「*」、「#」、「,」で入力します。
3	［実行］	端末にリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.8 （操作－iOS）リモートワイプ

対象の iOS 端末にリモートワイプを行います。

本機能を実行すると対象の端末が初期化されます。

iOS 17 以上の監視対象端末では、リモートワイプ時に Wi-Fi 設定が含まれる構成プロファイルを適用することで、端末を初期化したあと、手動で Wi-Fi 設定をする必要がなくなります。本機能で適用した構成プロファイルは、本機能で削除できます。

本機能を実行すると操作を取り消すことはできません。十分に注意してください。

リモートワイプで端末を初期化した場合、端末の OS は初期化したときと同じバージョンになります。ただし、アップデートの方法や仕様により、初期化する直前の OS バージョンにならない場合もあります。

適用した Wi-Fi 設定が含まれる構成プロファイルを削除するときは、以下に注意してください。

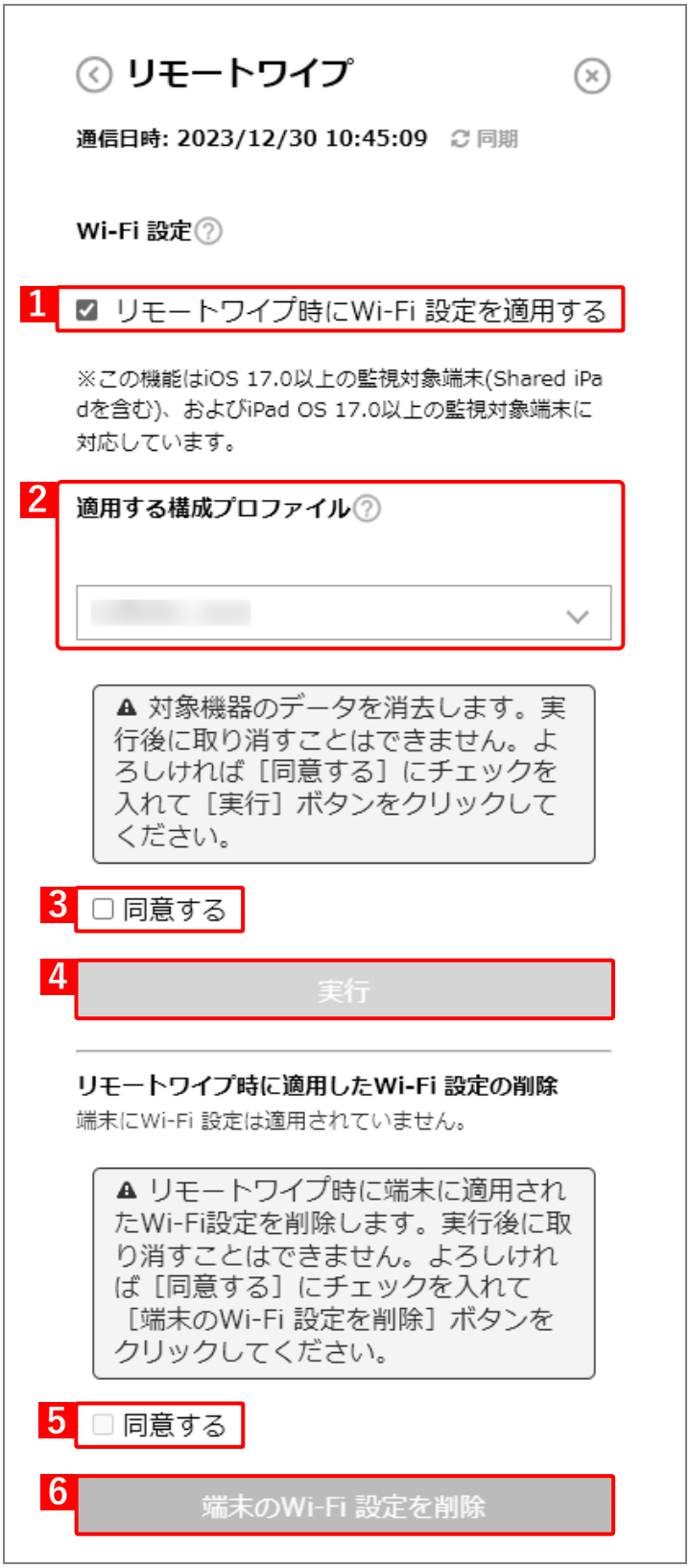
- ほかの構成プロファイルに通信可能な接続情報が端末に存在する場合のみ、削除してください。
- 適用した構成プロファイルで Wi-Fi 接続している場合は、削除すると通信が切断されます。
- 適用した構成プロファイルで Wi-Fi 接続していて、シングル APP モード設定中の場合は、通信が切断され、設定の変更や MDM プロファイルのアンインストールが、Apple Configurator 2 以外では行えません。
- 通常で利用する Wi-Fi 設定は、本機能を実行後に以下で構成プロファイルを適用してください。

☞「（設定－iOS）設定の割り当て」83 ページ

Wi-Fi 設定が含まれる構成プロファイルを適用して端末を初期化した場合、端末の初期設定時「Wi-Fi ネットワークを選択」画面以外はスキップされます。

◆画面

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［他の操作を見る］→［リモートワイプ］**



項番	項目	説明
1	［リモートワイプ時に Wi-Fi 設定を適用する］	リモートワイプ時に Wi-Fi 設定を適用するには、チェックを入れます。チェックを入れると、項番 2「適用する構成プロファイル」が表示されます。 iOS 17 以上の監視対象端末に対応します。
2	適用する構成プロファイル	Wi-Fi 設定が含まれる構成プロファイルが、リストボックスに表示されます。適用する構成プロファイルを選択します。 Wi-Fi 設定が含まれる構成プロファイルがない場合は、項番 3［同意する］が無効になります。構成プロファイルについては、以下を参照してください。 「構成プロファイル」392 ページ ユーザー種別が「ロック・ワイプ」のユーザーは、構成プロファイルの設定内容を確認できないので、確認できるユーザーに問い合わせてください。
3	［同意する］	リモートワイプを実行するには、チェックを入れます。チェックを入れると、項番 4 の［実行］がクリックできるようになります。
4	［実行］	端末にリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。
5	［同意する］	リモートワイプ時に端末に適用された Wi-Fi 設定を削除します。 項番 2「適用する構成プロファイル」で選択した構成プロファイルの削除を実行するには、チェックを入れます。チェックを入れると、項番 6［端末の Wi-Fi 設定を削除］がクリックできるようになります。 リモートワイプ時に Wi-Fi 設定を適用していない場合は、無効になります。
6	［端末の Wi-Fi 設定を削除］	端末のリモートワイプ時に適用した構成プロファイルの削除を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.9 （操作－iOS）リモートワイプ（管理領域）

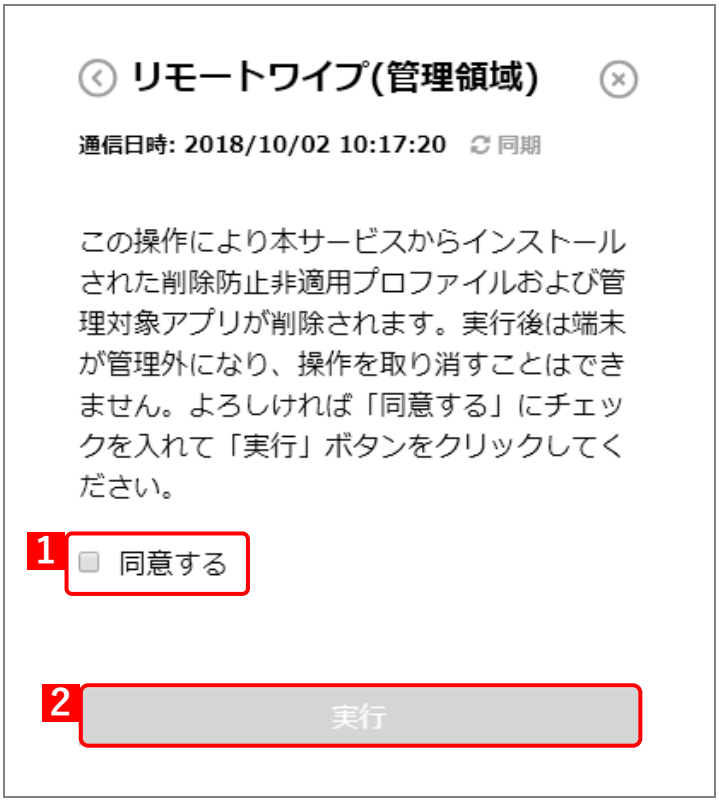
対象の iOS 端末に管理領域を含むリモートワイプを行います。

インストールされている構成プロファイル、および管理対象のアプリを削除します。本機能を実行すると端末が管理外になり、管理サイトで管理できなくなります。

- 本機能を実行すると操作を取り消すことはできません。十分に注意してください。
- 本機能を実行しても、「削除防止」を適用している構成プロファイルは端末から削除されません。「削除防止」を適用している構成プロファイルを削除するには、別途 Apple Configurator 2 を使用するか、端末を初期化する必要があります。
  構成プロファイルと管理対象アプリについては、以下を参照してください。
  ☞「構成プロファイル」392 ページ
  ☞「アプリケーション配信」530 ページ
- 監視対象端末を初期化せずに監視対象を解除したい場合は、本設定で構成プロファイルおよび管理対象アプリなどを削除すると、監視対象が解除されます。
- 端末に表示される「この iPad は～によって監視および管理されています」などのメッセージは、表示されたままになります。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［他の操作を見る］→［リモートワイプ（管理領域）］**



項番	項目	説明
1	同意する	リモートワイプ（管理領域）を実行するには、チェックを入れます。チェックを入れると、項番 2 の［実行］がクリックできるようになります。
2	［実行］	端末にリモートワイプ（管理領域）を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.10 （操作－iOS）紛失モード

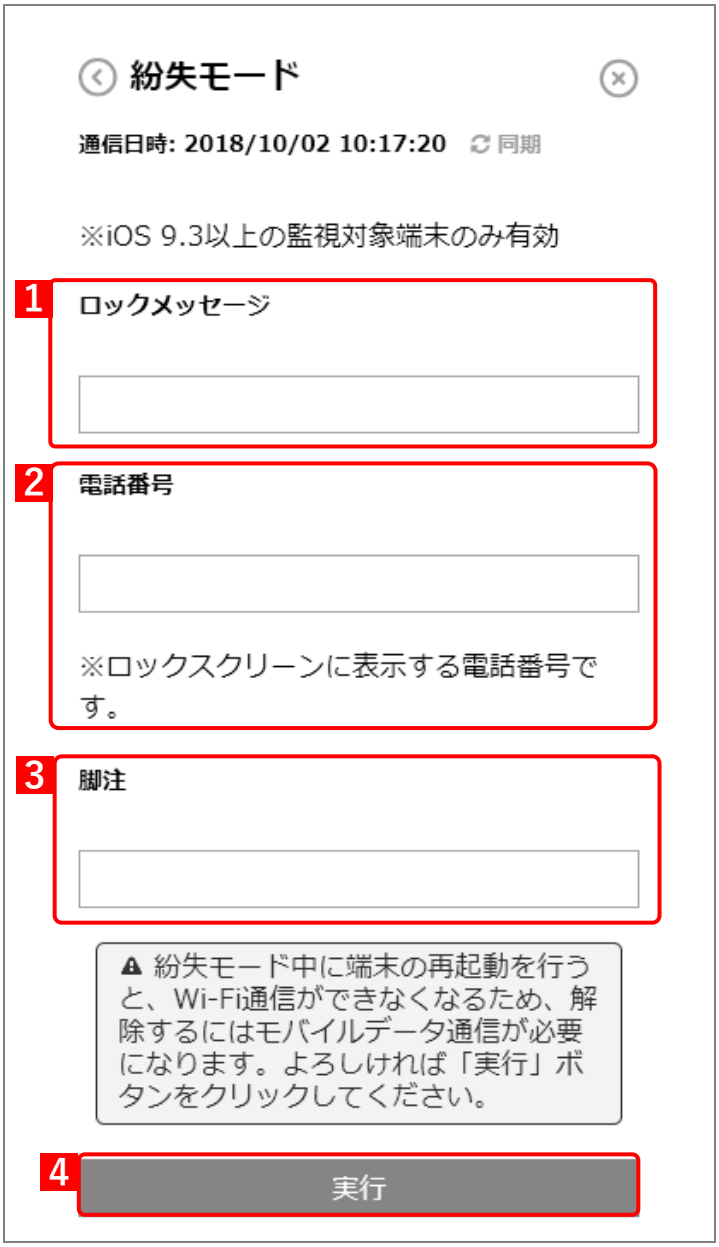
Apple が提供している iOS 端末の紛失モードを実行します。

紛失、盗難にあった場合、遠隔ロックをかけることやメッセージを表示できるようになります。また、紛失モードの解除は、管理サイトのみで行えるため、紛失によるデバイスの廃棄リスク、デバイスの不正利用による情報漏洩のリスクを低減できます。

iOS 9.3 以上の監視対象端末で有効です。

◆画面

表示操作 ［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「操作」の［他の操作を見る］→［紛失モード］**



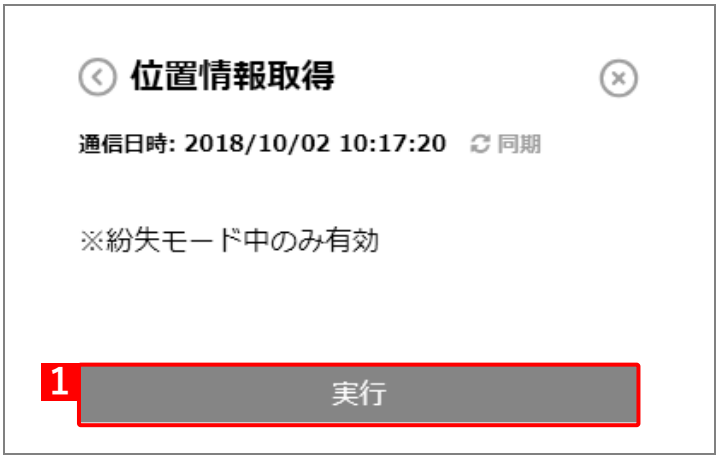
項番	項目	説明
1	ロックメッセージ	ロック画面に表示するメッセージを 200 文字以内で入力します。 ロックメッセージを入力しない場合は、電話番号の入力が必要です。
2	電話番号	ロックスクリーンに表示する電話番号を 20 文字以内の半角数字、「-」、「+」、「*」、「#」、「,」で入力します。 電話番号を入力しない場合は、ロックメッセージの入力が必要です。
3	脚注	必要に応じて、脚注を入力します。最大で全角 30 文字まで入力できます。
4	［実行］	端末に紛失モードの設定を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.11 （操作－iOS）位置情報取得

紛失モード中の iOS 端末から位置情報を取得します。エージェント認証していない端末の場合でも、紛失モードを使用すると、端末の位置情報を取得し、端末の場所を特定できます。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［他の操作を見る］→［位置情報取得］**



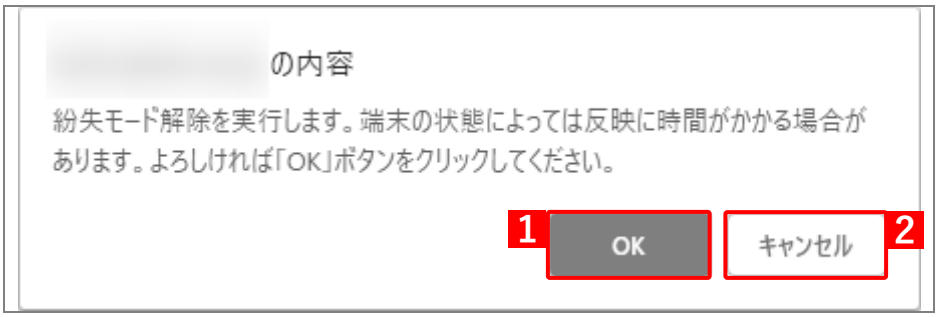
項番	項目	説明
1	［実行］	端末の位置情報を取得します。また、位置情報の取得を端末に通知します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.12 （操作－iOS）紛失モード解除

紛失モードの設定を解除します。紛失モード中に位置情報取得を行った場合は、紛失モードを解除したときに、位置情報取得を行ったことを伝えるメッセージが端末の画面に表示されます。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［他の操作を見る］→［紛失モード解除］**



項番	項目	説明
1	［OK］	クリックすると、対象の端末の紛失モードが解除されます。
2	［キャンセル］	クリックすると、紛失モードの解除の操作をキャンセルします。

4.1.9.13 （操作－iOS）アクティベーションロック解除

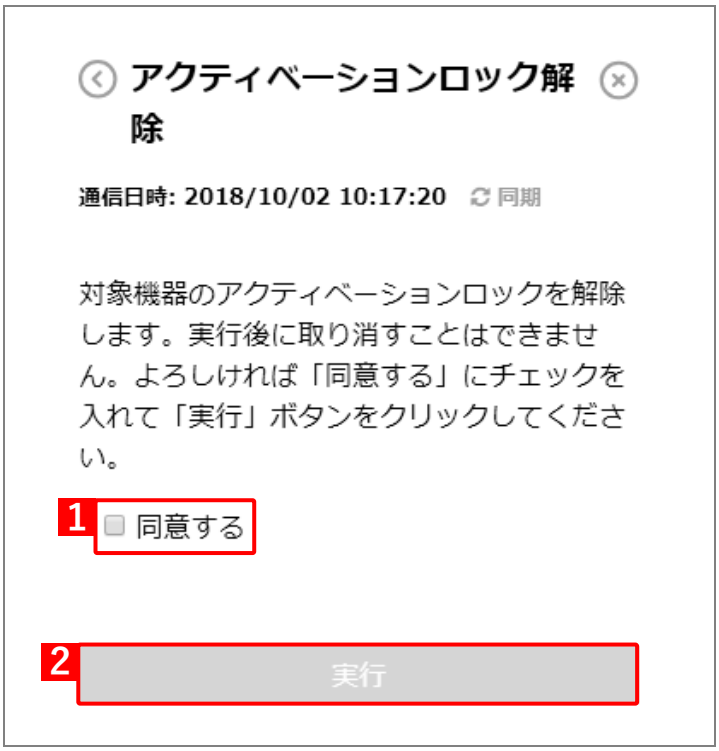
アクティベーションロックの設定を解除します。

本機能は、以下の条件を満たしている場合に操作できます。

- 監視対象端末である。
- 端末のアクティベーションロックの状態が「有効」になっている。
  アクティベーションロックの状態は、詳細画面の「情報」の［デバイス］→「その他の情報」で確認できます。
  「（情報－iOS）デバイス」151 ページ
- 「管理アプリの通信と動作」の「MDM 構成プロファイル共通管理」でアクティベーションロックの設定が「許可する」になっている。
  「画面（MDM 構成プロファイル共通管理）」384 ページ
- 端末の Bypass Code が取得できている。
  Bypass Code は、詳細画面の「情報」の［デバイス］→「その他の情報」で確認できます。
  「（情報－iOS）デバイス」151 ページ

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［他の操作を見る］→［アクティベーションロック解除］**



項番	項目	説明
1	同意する	アクティベーションロックを解除するには、チェックを入れます。チェックを入れると、項番 2 の［実行］がクリックできるようになります。
2	［実行］	端末のアクティベーションロックを解除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.14 （操作－iOS）OS アップデート

対象の iOS 端末の OS をアップデートします。

iOS 12.3 以上の監視対象端末でアップデートができます。

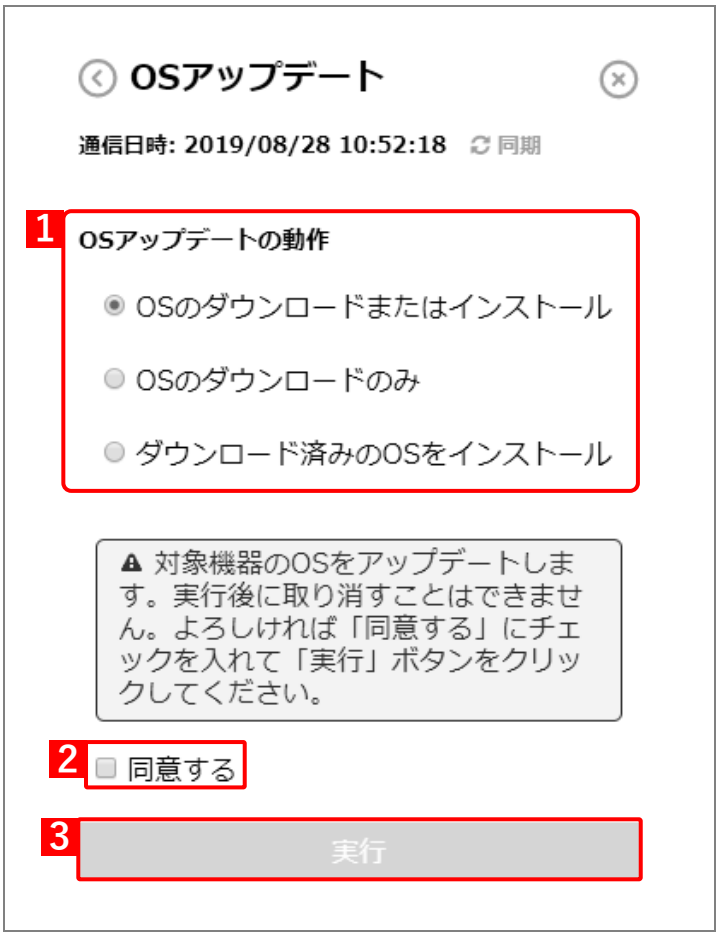
端末の状態が以下のとき、OS をアップデートできない場合があります。

- ディスク容量が不足している。
- バッテリー残量が少ない。
- Wi-Fi ネットワークが接続できない。
- パスコードが設定されている場合は、端末のロックが解除されていない。

◆画面

表示操作 ［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ＞ **→詳細画面の「操作」の［他の操作を見る］→［OS アップデート］**

最新の OS アップデートが存在しない場合は、表示されません。



項番	項目	説明
1	OS アップデートの動作	OS アップデートの動作方法を以下から選択します。 ●OS のダウンロードまたはインストール iOS 端末の状態に応じて、ダウンロードまたはインストールが行われます。 ●OS のダウンロードのみ ●ダウンロード済みの OS をインストール
2	同意する	端末に OS をダウンロード、または端末の OS をアップデートするには、チェックを入れます。チェックを入れると、項番 3 の［実行］がクリックできるようになります。

項番	項目	説明
3	［実行］	端末に OS をダウンロード、または端末の OS をアップデートします。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 OS アップデートができなかった場合は、原因のログが表示されます。詳細については、以下を参照してください。 『FAQ 一覧』の「管理サイト」－「Q30」、「iOS」－「Q35」「Q37」

4.1.9.15 （操作－iOS）リモート再起動

対象の iOS 端末を再起動します。

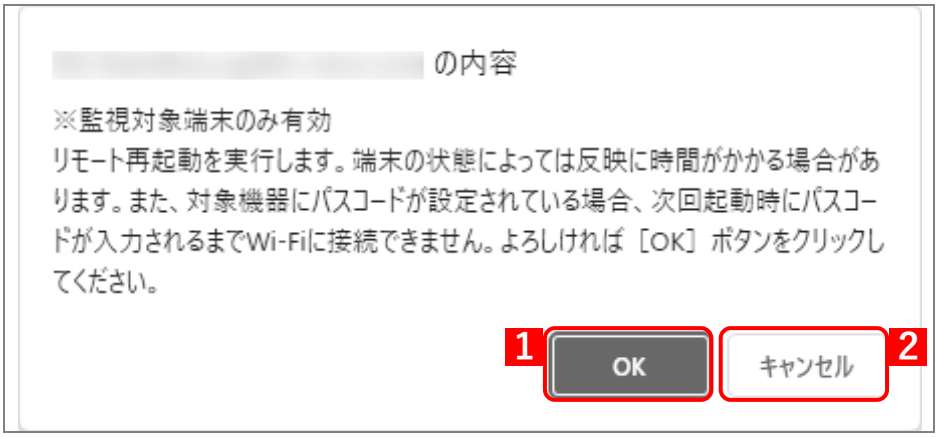
本機能を実行すると操作を取り消すことはできません。十分に注意してください。

監視対象端末で有効です。

端末にパスコードが設定されている場合は、再起動後、パスコードを入力しないと Wi-Fi に接続することができません。

◆画面

表示操作［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「操作」の［他の操作を見る］→［リモート再起動］**



項番	項目	説明
1	［OK］	クリックすると、対象の端末が再起動します。
2	［キャンセル］	クリックすると、再起動の操作をキャンセルします。

4.1.9.16 （操作－iOS）リモートシャットダウン

対象の iOS 端末をシャットダウンします。

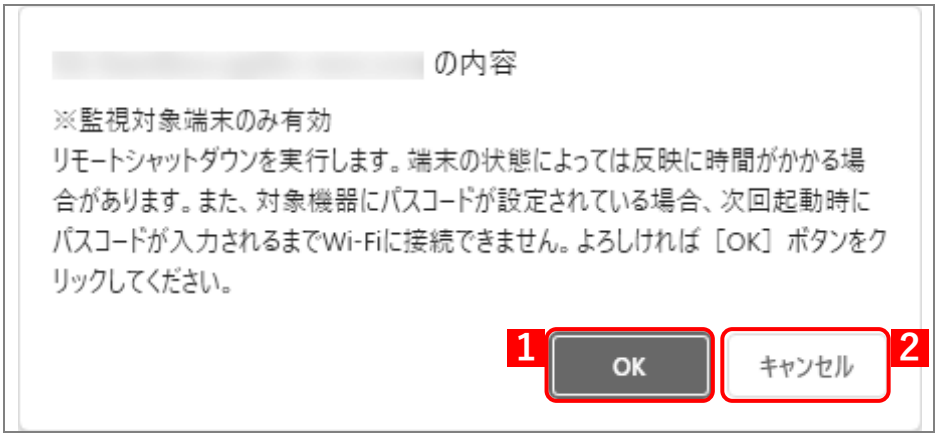
本機能を実行すると操作を取り消すことはできません。十分に注意してください。

監視対象端末で有効です。

端末にパスコードが設定されている場合は、再起動後、パスコードを入力しないと Wi-Fi に接続することができません。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［他の操作を見る］→［リモートシャットダウン］**



項番	項目	説明
1	［OK］	クリックすると、対象の端末がシャットダウンします。
2	［キャンセル］	クリックすると、シャットダウンの操作をキャンセルします。

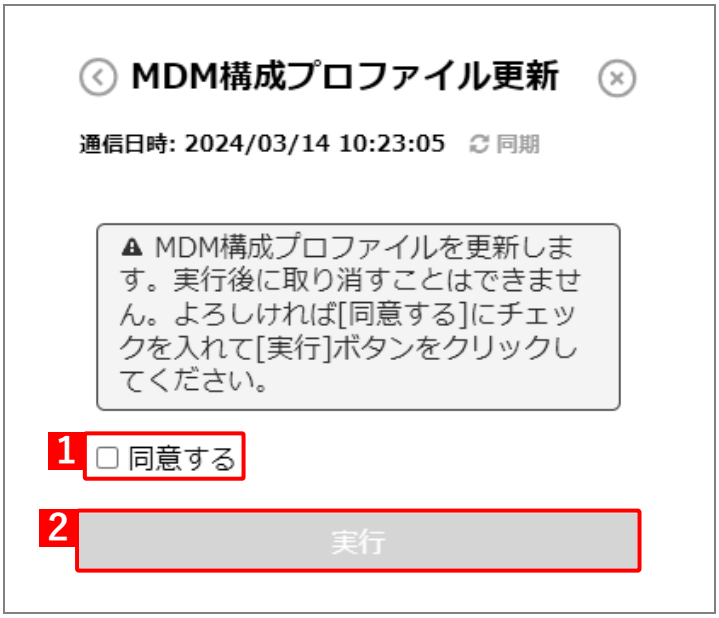
4.1.9.17 （操作－iOS）MDM 構成プロファイル更新

対象の iOS 端末の MDM 構成プロファイルを更新します。

本機能を実行すると操作を取り消すことはできません。十分に注意してください。

◆画面

表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「操作」の［他の操作を見る］→［MDM 構成プロファイル更新］**



項番	項目	説明
1	同意する	端末に MDM 構成プロファイルを更新するには、チェックを入れます。チェックを入れると、項番 2 の［実行］がクリックできるようになります。
2	［実行］	端末に MDM 構成プロファイルを更新します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.18 （操作－Windows）リモートロック

対象の Windows 端末をリモートロックします。

リモートロックを行うとロック画面が表示され、端末を操作できなくなります。

端末の状態は、詳細画面の「情報」の［デバイス］で確認できます。

詳細については、以下を参照してください。

「（情報－Windows）デバイス」173 ページ

リモート操作が Windows 端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。

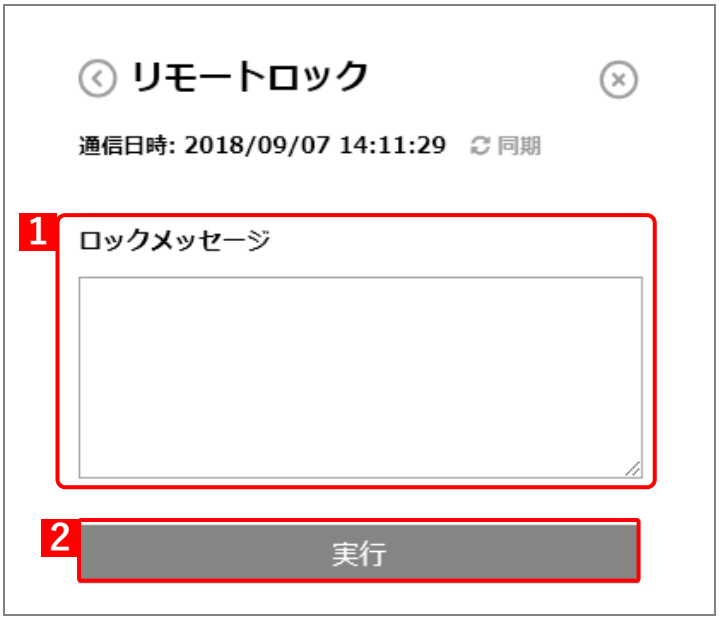
システムでグループポリシーが設定されている場合は、グループポリシーが優先され、リモートロックを解除できないことがあります。

本画面では単一の端末を対象としています。複数の端末に一括で操作を行う場合は、以下を参照してください。

「［その他▼］タブ／Windows リモート操作」215 ページ

◆画面

表示操作 **［機器］→［一覧］→Windows 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［リモートロック］**



項番	項目	説明
1	ロックメッセージ	ロック画面に表示するロックメッセージを 200 文字以内で入力してください。
2	［実行］	端末にリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.9.19 （操作－Windows）ロック解除

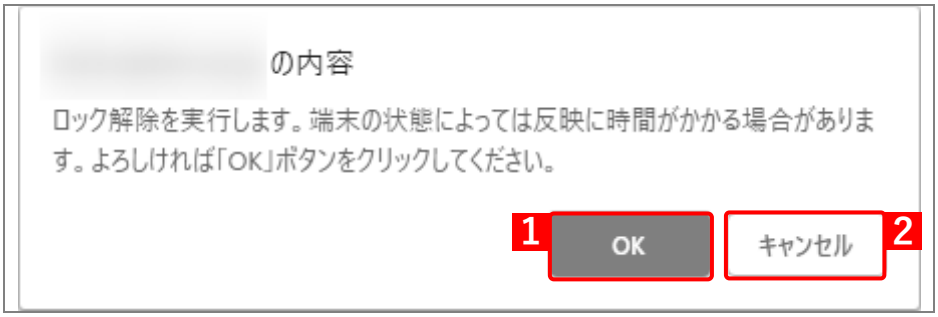
対象の Windows 端末のリモートロックを解除します。

- リモート操作が Windows 端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。
- システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本機能が利用できない場合があります。グループポリシーについては、システム管理者に問い合わせてください。
- 本画面では単一の端末を対象としています。複数の端末に一括で操作を行う場合は、以下を参照してください。

「［その他▼］タブ／Windows リモート操作」215 ページ

◆画面

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ＞ →詳細画面の「操作」の［他の操作を見る］→［ロック解除］**



項番	項目	説明
1	［OK］	端末のロックを解除します。
2	［キャンセル］	端末のロック解除の操作を取り消します。

4.1.9.20 （操作－Windows）リモートワイプ

対象の Windows 端末のリモートワイプを行います。リモートワイプには、「PC 初期化」、「BitLocker」、および「データ削除」の 3 種類の方法があります。

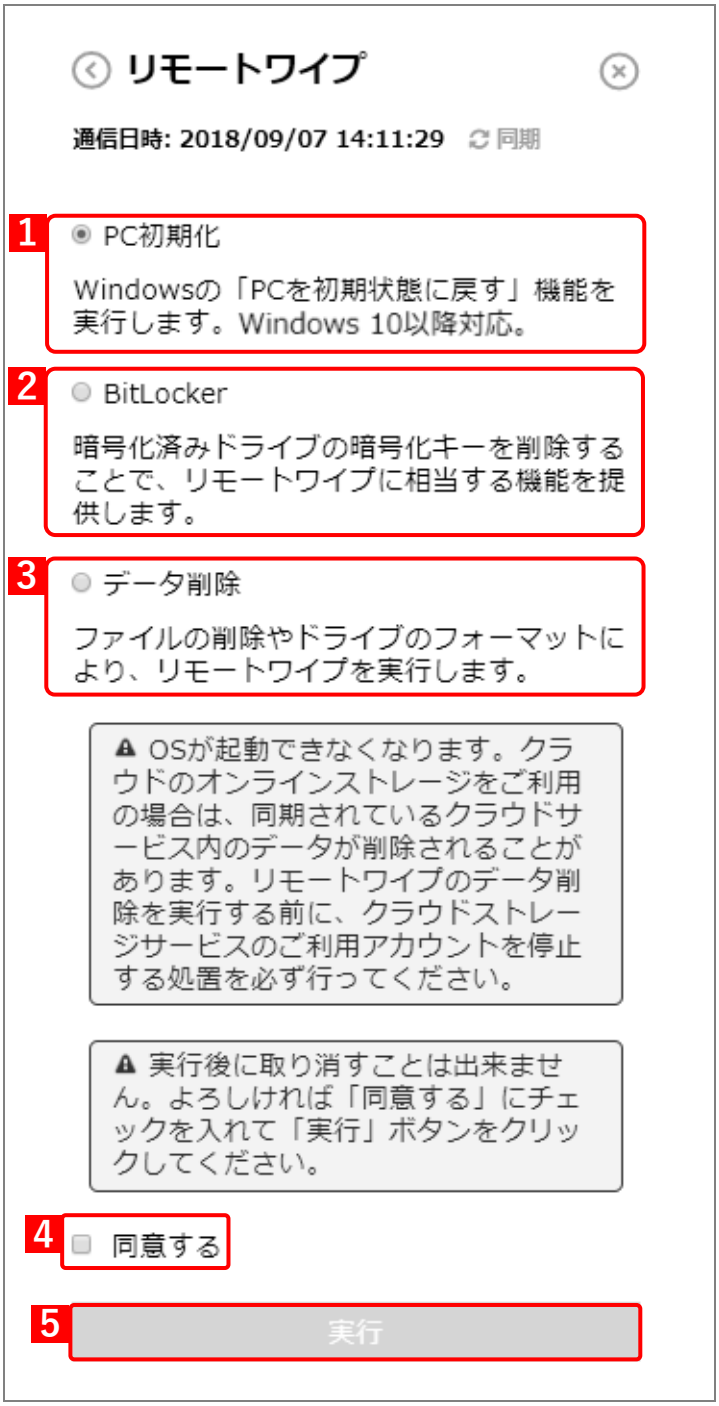
本機能を実行すると、端末の初期化や端末データへの接続を不能にしたり、ドライブをフォーマットすることができます。

- 本機能を実行すると操作を取り消すことはできません。十分に注意してください。
- リモートワイプで端末を初期化した場合、端末の OS は初期化したときと同じバージョンになります。ただし、アップデートの方法や仕様により、初期化する直前の OS バージョンにならない場合もあります。
- システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本機能が利用できない場合があります。グループポリシーについては、システム管理者に問い合わせてください。
- 本画面では単一の端末を対象としています。複数の端末に一括で操作を行う場合は、以下を参照してください。

「［その他▼］タブ／Windows リモート操作」215 ページ

◆画面

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓒ →詳細画面の「操作」の［他の操作を見る］→［リモートワイプ］**



項番	項目	説明
1	PC 初期化	Windows の「PC を初期状態に戻す」機能を実行します。 工場出荷時のリカバリー領域が必要です。リカバリ領域がないと、リモートワイプに失敗します。
2	BitLocker	BitLocker で暗号化済みドライブの回復キー以外のキープロテクターを削除します。 BitLocker でのワイプを実行したあとは、端末を起動したときに BitLocker の回復キー入力画面が表示されます。回復キーを入力するまでドライブのデータにアクセスできません。 回復キーのキープロテクターがないドライブは、BitLocker でのワイプができません。 削除した回復キーを新規で作成するには、以下の URL で「構文」と「パラメーター」を参照してください。回復キーの作成方法については、システム管理者に問い合わせてください。 https://learn.microsoft.com/ja-jp/windows-server/administration/windows-commands/manage-bde-protectors 本製品の暗号化機能を利用している場合は、暗号化機能の設定セットを無効、有効の順で割り当てて同期すると、回復キーを遠隔で新規作成することができます。 BitLocker 以外の暗号化ツールを使用している場合は、本機能は使用できません。 Windows 11 Pro/Enterprise/Education の端末に対応しています。詳細については、以下を参照してください。 「暗号化」573 ページ BitLocker については、Microsoft の Web サイトを参照してください。 https://learn.microsoft.com/ja-jp/windows/security/operating-system-security/data-protection/bitlocker/ 回復キーとは、48 桁の文字列です。回復パスワードという場合もあります。詳細については、以下を参照してください。 「（情報－Windows）セキュリティ」181 ページ
3	データ削除	ファイルを削除し、ドライブをフォーマットすることにより、リモートワイプを行います。 本機能を実行すると、OS が起動しなくなることがあります。操作を取り消すことはできません。実行時は、十分に注意してください。 以下のドライブが本機能でのリモートワイプの対象になります。 ・A:から Z:までの割り当て済みドライブ ・ドライブの種類が固定ドライブまたはリムーバブルドライブ（USB メモリなど） ・バスの種類が iSCSI と仮想ドライブ以外
4	同意する	リモートワイプを実行するには、チェックを入れます。チェックを入れると、項番 5 の［実行］がクリックできるようになります。
5	［実行］	端末にリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

4.1.10 機器の情報

各端末の詳細画面から、端末ごとの各種情報（ログ情報、デバイス情報、エージェント情報、アプリ情報、位置情報）を表示します。

4.1.10.1 （情報－Android）ログ

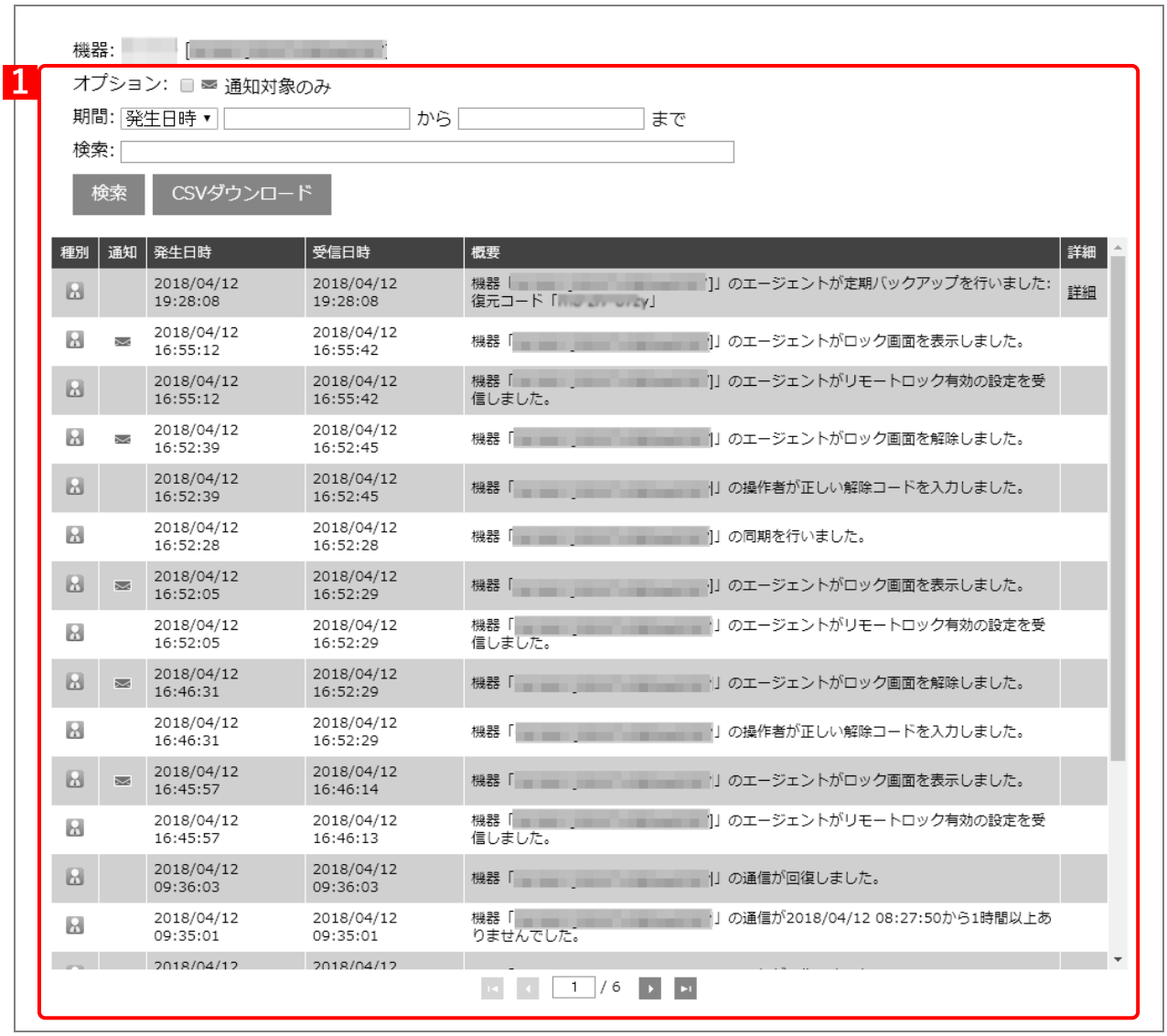
対象の Android 端末のログをログ画面に表示します。

ログ画面の詳細については、以下を参照してください。

☞「ログ画面の見かた」646 ページ

◆画面

表示操作　［機器］→［一覧］→**Android 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［ログ］**



項番	項目	説明
1	ログ画面	ログ画面に、対象の端末のログだけが表示されます。ログ画面の詳細については、以下を参照してください。 ☞「ログ画面の見かた」646 ページ

4.1.10.2 （情報－Android）デバイス

対象の Android 端末の現在の状態を表示します。

情報を取得できない場合は、「(Unknown)」と表示されます。

◆画面

表示操作　［機器］→［一覧］→Android 端末の機器名または「詳細」の ›　→詳細画面の「情報」の［デバイス］

項番	項目	説明
1	基本	以下の情報が表示されます。 ●モデル名 ●ネットワークモード 接続しているネットワーク方式が表示されます。 ●ファームウェアバージョン ●ビルド番号 ●シリアル番号
2	SIM 情報	端末に搭載されている SIM の情報が表示されます。 複数の SIM が搭載されている端末では、パネル名の末尾に番号が付いた SIM 情報パネルが、SIM ごとに表示されます。 ●電話番号 SIM に割り振られている電話番号が表示されます。 ●ネットワークオペレーター ネットワークオペレーター（ネットワーク事業者）が表示されます。 ●IMEI/MEID ●ICCID ●SIM 種別 以下のいずれかが表示されます。 ・「(Unknown)」 ・「物理 SIM」 ・「eSIM」
3	OS	以下の情報が表示されます。 ●OS バージョン
4	グローバル IP アドレス	以下の情報が表示されます。 ●グローバル IP アドレス 「NNN.NNN.NNN.NNN」形式の IP アドレスが表示されます。
5	ネットワーク	検知されたネットワークごとにパネルが表示され、ネットワークの情報が表示されます。パネルタイトルにネットワーク表示名が「ネットワーク - 表示名」の形式で表示されます。 ●SSID ネットワーク - wlan0 の場合のみ、SSID が表示されます。 ●MAC アドレス 「XX:XX:XX:XX:XX:XX」形式の MAC アドレスが表示されます。 ●IP アドレス IP アドレスが以下のいずれかの形式で表示されます。 ・形式（IPv4）：「NNN.NNN.NNN.NNN/NNN」 ・形式（IPv6）：「XX:XX:...:XX」 ・IP アドレスが 0 個の場合は空欄。 Android 8.1 以上の端末の位置情報設定が OFF の場合やエージェントの位置情報権限が無効になっている場合は、SSID が<unknown ssid>と表示されます。 Android 10 以上の端末は、デフォルト設定で Wi-Fi の MAC アドレスがランダム値で表示されます。 Android 11 以上の端末は、Wi-Fi 以外の MAC アドレスが「(Unknown)」と表示されます。また、位置情報設定が OFF の場合やエージェントの位置情報権限が無効に設定されている場合は、Wi-Fi の MAC アドレスが「(Unknown)」と表示されます。
6	Bluetooth	以下の情報が表示されます。 ●状態 Bluetooth の状態が「有効」または「無効」で表示されます。

項番	項目	説明
7	位置情報	以下の情報が表示されます。 ●無線ネットワーク ワイヤレスネットワークから位置情報の測位ができるかどうかの状態を「有効」または「無効」で表示します。 ワイヤレスネットワークとは、基地局測位（モバイルネットワーク）と、Wi-Fi ネットワークのことです。 ●GPS 機能 GPS から位置情報の測位ができるかどうかの状態を「有効」または「無効」で表示します。 ●正確な位置情報を使用 エージェントのアプリ権限「正確な位置情報を使用」の ON／OFF 状態を「有効」または「無効」で表示します。 以下の場合は、「(Unknown)」と表示されます。 ・Android 12 未満 ・Android 12 以上かつ端末の位置情報設定が OFF
8	Device Owner Mode	以下の情報が表示されます。 ●状態 Device Owner Mode の状態が、「有効」または「無効」で表示されます。 Device Owner Mode がサポートされていない場合は、「非対応」と表示されます。
9	Android Enterprise	以下の情報が表示されます。 ●Android Enterprise ユーザー Android Enterprise のユーザー情報が表示されます。 ユーザーが Android Enterprise と連携されていても、ユーザー情報の表示が「(Unknown)」から「連携済」に変わるまでしばらく時間がかかることがあります。
10	デバイス管理者権限	以下の情報が表示されます。 ●デバイス管理者権限 Android エージェントへのデバイス管理者権限付与状態が、「有効」または「無効」で表示されます。 無効の場合は、以下の機能が動作しません。 ・エージェントアンインストール抑止 ・リモートロック（Android 6.0 以上の場合） Android 標準ロック画面のみ動作しません。本製品独自のリモートロック画面は無効化されても動作します。 ・リモートワイプ ・スクリーンロックのパスワードポリシー強制 ・管理サイトからのスクリーンロックのパスワード変更/リセット ・カメラ禁止（Android 4.0 以上の場合） デバイス管理者権限が無効化された後、端末上でエージェントを起動すると管理外通知画面が表示されます。画面に従い、デバイス管理者権限を有効化してください。
11	バッテリー	以下の情報が表示されます。 ●バッテリー残量 バッテリーの残量が%で表示されます。 ●バッテリー状態 以下のいずれかが表示されます。 ・「不明」、「充電中」、「放電中」、「充電していません」、「満タン」

項番	項目	説明
12	スクリーンロック	「スクリーンロック」項目については、画面ロック（スクリーンロック）の設定セットの設定内容（スクリーンロックポリシー）と設定内容（スクリーンロックポリシー）に違反していないかどうかが表示されます。 対象の機器に画面ロック（スクリーンロック）の設定セットが適用されていない場合は、いずれの項目も「制限なし」と表示されます。 画面ロック（スクリーンロック）の設定セットの設定内容（スクリーンロックポリシー）については以下を参照してください。 「画面ロック」304 ページ ●パスワードのポリシー 以下のいずれかが表示されます。 ・不特定の場合 「制限なし」 ・ポリシーを満たしている場合 「端末は以下のポリシーを満たしています 解除方法：(ポリシーで設定した解除方法) 文字数：(ポリシーで設定した文字数)」 ・ポリシーを満たしていない場合 「端末は以下のポリシーを満たしていません 解除方法：(ポリシーで設定した解除方法) 文字数：(ポリシーで設定した文字数)」 ●パスワードの再利用 ○回前までのパスワード、または「制限なし」が表示されます。 ●パスワードの有効期限 「○日」または「制限なし」が表示されます。 ●自動ロックまでの時間 「○分」または「自動ロックしない」が表示されます。 ●ロック解除失敗時の設定 以下のいずれかが表示されます。 ・「○回失敗でリモートロック」 ・「○回失敗でワイプ」 ・「リモートロック／ワイプを行わない」 「○回失敗でリモートロック」が設定されており、ロックメッセージが設定されている場合は、ロックメッセージも合わせて表示されます。 ●ロック画面の制限 以下のいずれかが表示されます。 ・「制限しない」 ・「全て制限する」 ・「制限機能を指定する」 ・「(Unknown)」 最新バージョンにアップされたエージェントの端末では「制限しない」が表示されます。 端末で権限が許可されていないと正しい表示になりません。権限許可の詳細については、以下のマニュアルを参照してください。 『Android クライアント リファレンスマニュアル』の「管理サイトからの指示による動作」ー「管理外通知画面が表示された場合」

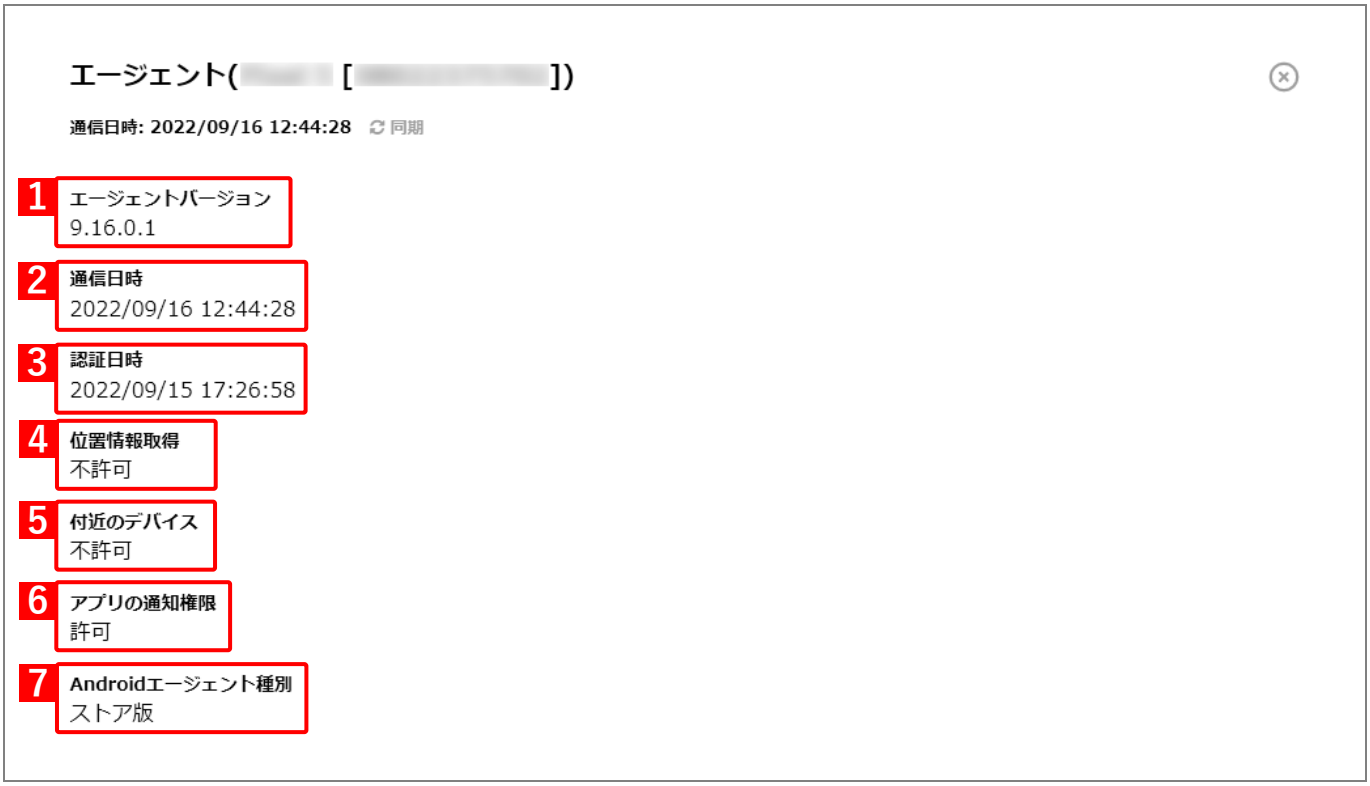
項番	項目	説明
13	スクリーンロックパスワード変更の事前設定	●状態 スクリーンロックパスワード変更用のトークンを端末に配信している場合は、端末の対応状況について、以下のいずれかが表示されます。 ・管理サイトからスクリーンロックパスワードを変更できる状態 「完了」 ・管理サイトからスクリーンロックパスワードを変更できない状態 「未完了」 ・不明の状態 「(Unknown)」
14	リモートロック	以下の情報が表示されます。 ●状態 「ロックされています」または「解除されています」が表示されます。
15	root 化	以下の情報が表示されます。 ●状態 「root 化状態」または「問題なし」が表示されます。 ●検知内容 ・状態が「root 化状態」の場合 以下のいずれかが表示されます。 ・「su コマンドが存在します」 ・「setuid されたコマンドが存在します」 ・「root 化アプリケーション（アプリケーション名）がインストールされています」 ・状態が「問題なし」の場合 「問題なし」と表示されます。
16	ファクトリーリセット保護	以下の情報が表示されます。 ●状態 以下のいずれかが表示されます。 ・「無効」 ・「有効（端末に登録済みの Google アカウントを使用する)」 ・「有効（Google アカウントを指定する)」 ・「(Unknown)」 ●Google アカウントのメールアドレス 状態が「有効（端末に登録済みの Google アカウントを使用する)」、「有効（Google アカウントを指定する)」の場合に表示されます。 ファクトリーリセット保護の設定セットの設定内容については、以下を参照してください。 「ファクトリーリセット保護（DOM)」374 ページ

4.1.10.3 （情報－Android）エージェント

対象の Android 端末のエージェント情報を表示します。

◆画面

表示操作 ［機器］→［一覧］→Android 端末の機器名または「詳細」の ›› →詳細画面の「情報」の［エージェント］



項番	項目	説明
1	エージェントバージョン	対象の Android 端末のエージェントバージョンが表示されます。
2	通信日時	対象の Android 端末と管理サーバーが最後に通信した日時が表示されます。
3	認証日時	対象の Android 端末が認証された時刻が表示されます。
4	位置情報取得	位置情報取得の許可／不許可の設定状況が表示されます。
5	付近のデバイス	付近のデバイスの許可／不許可の設定状況が表示されます。 Android 12 未満、エージェントバージョン 9.14.0 未満の場合は、「(Unknown)」と表示されます。
6	アプリの通知権限	アプリの通知権限の許可／不許可の設定状況が表示されます。 Android 13 未満、エージェントバージョン 9.16.0 未満の場合は、「(Unknown)」と表示されます。
7	Android エージェント種別	対象の Android 端末のエージェント種別として以下のいずれかが表示されます。 ●ストア版 ●(Unknown) 古いバージョンのエージェントの場合、「(Unknown)」と表示されます。

4.1.10.4 （情報－Android）アプリケーション

対象の Android 端末にインストールされているアプリの一覧を表示します。また、詳細画面を表示して、アプリの詳細情報を確認することもできます。

画面

画面（アプリの詳細）

◆画面

表示操作 ［機器］→［一覧］→Android 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［アプリケーション］

項番	項目	説明
1	［絞り込み］	項番【2】に表示する情報を以下の項目を条件にして絞り込めます。 ●「アプリケーション名」、「パッケージ名」
2	絞り込み条件	［絞り込み］をクリックして検索した場合、その条件が表示されます。 をクリックすると、再度すべてのアプリが一覧に表示されます。
3	アプリ一覧	対象の機器にインストールされているアプリの一覧に以下の情報が表示されます。 ・「アプリケーション名」、「パッケージ名」、「バージョン名」、「アプリケーションサイズ」、「インストール日時」
4	メモ	をクリックして にすると、アプリケーション禁止で「メモから追加」で追加する対象のアプリに設定されます。クリックするたびに と が切り替わります。 ［メモから追加］の機能については、以下を参照してください。 ☞「アプリケーション禁止」320 ページ
5	詳細	をクリックすると、アプリ一覧の右側に対象のアプリの詳細情報が表示されます。 ☞「画面（アプリの詳細）」143 ページ

◆画面（アプリの詳細）

アプリの詳細を確認できます。表示される各項目の詳細については、メーカーまたは開発・提供元へご確認ください。

表示操作　［機器］→［一覧］→Android 端末の機器名または「詳細」の ›　→詳細画面の「情報」の［アプリケーション］→一覧から対象のアプリの ›

項番	項目	説明
1	アプリケーション名	アプリ名が表示されます。
2	パッケージ名	アプリのパッケージ名が表示されます。
3	バージョン番号	アプリのバージョン番号が表示されます。
4	バージョン名	アプリのバージョン名が表示されます。
5	アプリケーションサイズ	アプリのファイルサイズが表示されます。 「0 Byte」と表示されることがありますが、アプリの使用には問題ありません。 端末により同じアプリでも値が異なることがあります。
6	メモリサイズ	アプリのメモリサイズが表示されます。
7	データサイズ	アプリのデータサイズが表示されます。
8	キャッシュサイズ	アプリのキャッシュサイズが表示されます。
9	インストール日時	アプリがインストールされた日時が表示されます。
10	アップデート日時	アプリがアップデートされた日時が表示されます。

4.1.10.5 （情報－Android）アプリ構成

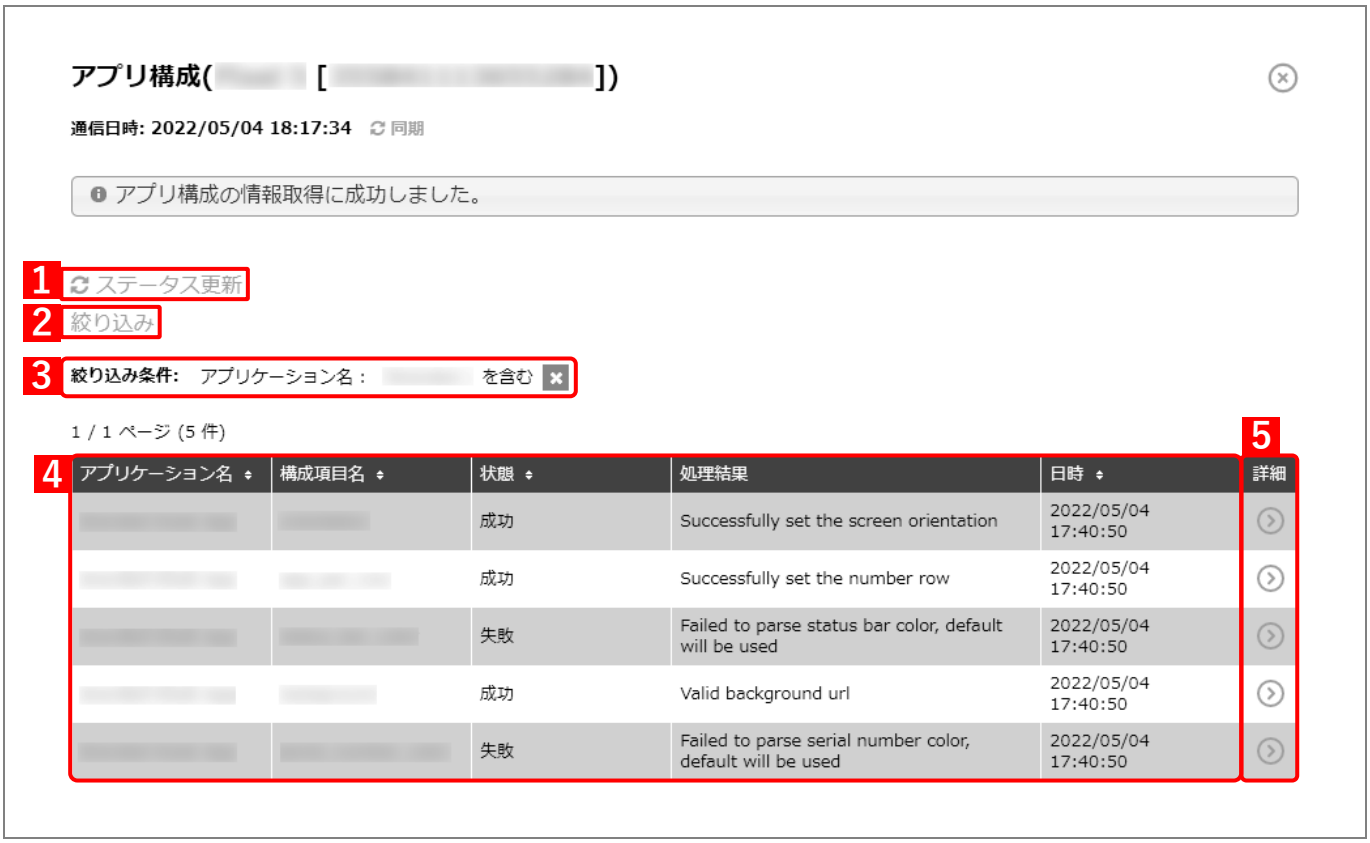
対象の Android 端末に Android Enterprise で配信したアプリのアプリ構成一覧を表示します。また、詳細画面を表示して、アプリ構成の詳細情報を確認することもできます。

画面

画面（アプリ構成の詳細）

◆画面

表示操作 ［機器］→［一覧］→**Android 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［アプリ構成］**

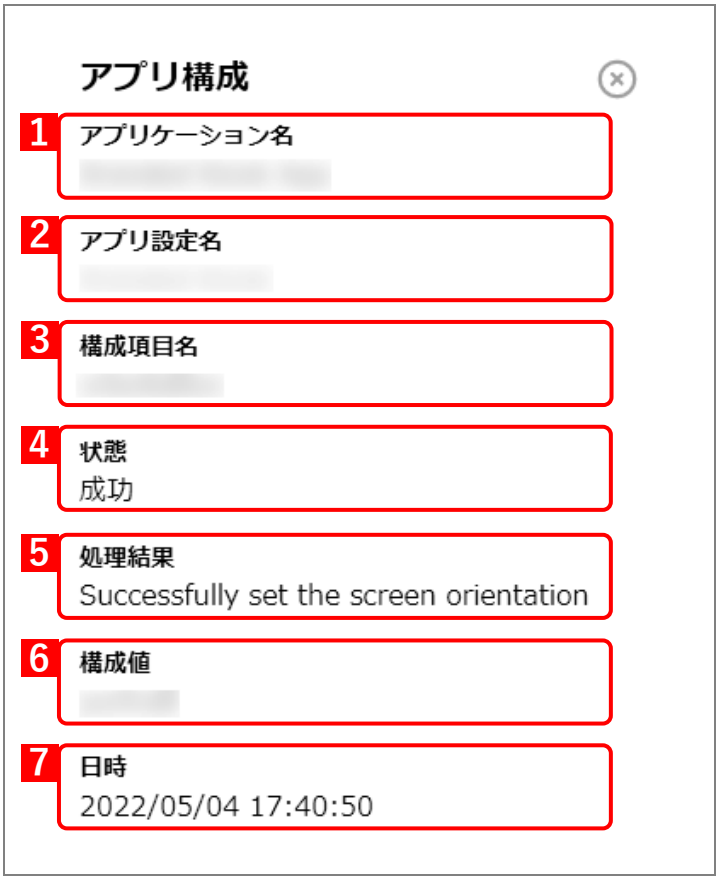


項番	項目	説明
1	［ステータス更新］	アプリ構成の一覧を更新します。実行するには、確認画面で［OK］をクリックします。 端末の状態によっては反映に時間がかかる場合があります。
2	［絞り込み］	項番【3】に表示する情報を絞り込めます。 絞り込める条件は、以下のとおりです。 ・「アプリケーション名」 ・「構成項目名」 ・「状態」
3	絞り込み条件	［絞り込み］をクリックして検索した場合、その条件が表示されます。 をクリックすると、再度すべてのアプリが一覧に表示されます。
4	アプリ構成一覧	対象の機器にインストールされているアプリの一覧に以下の情報が表示されます。 ・「アプリケーション名」、「構成項目名」、「状態」、「処理結果」、「日時」

項番	項目	説明
5	詳細	ⓘ をクリックすると、アプリ構成一覧の右側に対象のアプリ構成の詳細情報を表示する画面が表示されます。 ☞「画面（アプリ構成の詳細）」145 ページ

◆画面（アプリ構成の詳細）

表示操作［機器］→［一覧］→**Android 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［アプリ構成］→一覧から対象のアプリ構成の ⓘ**



項番	項目	説明
1	アプリケーション名	アプリ名が表示されます。
2	アプリ設定名	アプリ構成を設定する設定名が表示されます。 ［(設定名)］をクリックすると、アプリ構成を設定する画面が表示されます。
3	構成項目名	アプリ構成のユニーク ID または構成項目名が表示されます。
4	状態	状態が「成功」または「失敗」で表示されます。
5	処理結果	対象の Android 端末にアプリ構成を適用した結果が表示されます。
6	構成値	アプリ構成を設定する構成値が表示されます。
7	日時	対象の Android 端末にアプリ構成を適用した日時が表示されます。

4.1.10.6 （情報－Android）位置

Android 端末から送られた位置情報を表示します。

位置情報取得の条件については、以下を参照してください。

「Android 端末の位置情報の諸条件」147 ページ

- 位置情報送信を一度も行っていない端末は、［位置］メニューが表示されません。
- 本製品から端末の GPS を ON にすることはできません。
- 取得した位置情報の精度が低いと情報が破棄されるため、管理サイトに反映されません。
- Android 8.x の場合は、位置情報の取得が 1 時間に 1 回程度へ制限されます。
- Android 端末に「位置情報管理」の設定セットを適用してください。

「位置情報管理」309 ページ

◆画面

表示操作［機器］→［一覧］→Android 端末の機器名または「詳細」の ＞ →詳細画面の「情報」の［位置］

項番	項目	説明
1	測位情報	以下の情報が表示されます。 ●受信日時 管理サイトが端末の位置情報を取得した日時が表示されます。 ●測位日時 端末が保持している位置情報を測位した日時が表示されます。 ●北緯 測位した位置の北緯が表示されます。 ●東経 測位した位置の東経が表示されます。 ●測位プロバイダ 以下のいずれかで表示されます。 ストア版エージェントのみ表示されます。 ・GPS ・Network ・(Unknown) エージェントバージョン 9.11.100.0 未満の場合は、「(Unknown)」と表示されます
2	位置情報履歴	対象の端末が取得した位置情報の履歴を確認できます。位置情報の履歴は最大 100 件まで表示されます。例えば、「1/38」と表示されている場合は、履歴が 38 件あるうちの、最新の履歴が表示されていることを示しています。 をクリックして、履歴の表示を切り替えることができます。
3	地図	位置情報が地図で表示されます。 が表示されている位置が、地図上の端末の位置です。
4	［Google マップで表示］	クリックすると、新しいウインドウで Google マップとして表示されます。

◆Android 端末の位置情報の諸条件

Android 端末から位置情報を受信するための動作条件、位置情報測位契機、位置情報送信契機は以下のとおりです。内容を確認し、位置情報の受信を行ってください。

測位結果の情報は確実性を保証できる情報ではありません。

測位条件は端末の仕様に準じます。

項番	項目	条件
1	動作条件	以下の動作条件が満たされている必要があります。 ●端末が管理サイトと通信できる状態である。 ●エージェントの設定で位置情報の取得を許可している。 各機器の状況は、デバイス画面の「位置情報取得」から確認できます。 ☞「(情報－Android) デバイス」135 ページ 許可されていない場合は、位置情報画面の最上部にエラーが表示されます。 Android 12 以上は、正確な位置情報を取得するために、端末の設定で「正確な位置情報を使用」を有効にしてください。 ●端末で以下のいずれかによる測位をできるようにしている。 ・GPS による位置測位 以下の両方に該当する場合のみできます。 ・GPS が有効 ・3G、4G/LTE、5G、Wi-Fi いずれかのネットワークでの通信が有効 ・ネットワークによる位置測位 以下の両方に該当する場合のみできます。 ・ネットワーク位置情報（端末で［位置情報サービス］または［位置情報アクセス］などの表記がある設定）が有効 ・3G、4G/LTE、5G、Wi-Fi いずれかのネットワークでの通信が有効

項番	項目	条件
2	位置情報測位契機	以下のいずれかの契機で測位します。 ●位置情報管理の「エージェントによる測位」で設定した契機 ☞「位置情報管理」309 ページ ●他アプリ利用による測位 他アプリが位置情報を測位していた場合、利用条件に合致しなくても位置情報が管理サイトに表示されます。
3	位置情報送信契機	管理サイトと同期時に位置情報を送信します。 同期処理自体にかかる時間は、負荷状態や通信状態に依存します。

4.1.10.7 （情報－Android）Zone Management

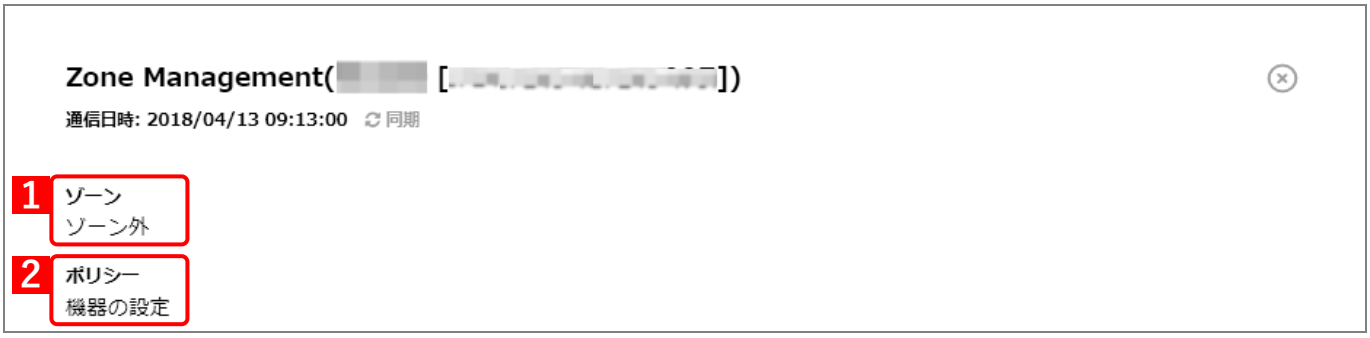
対象の Android 端末に反映されている「ゾーンポリシー構成」の設定セットの登録内容を表示します。登録されている「ゾーン」と「ポリシー」の名称から、「ゾーンポリシー構成」の内容を把握することができます。

詳細については、以下を参照してください。

☞「Zone Management」357 ページ

◆画面

表示操作 ［機器］→［一覧］→**Android 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［他の情報を見る］→［Zone Management］**



項番	項目	説明
1	ゾーン	対象の Android 端末に適用されているゾーン名が表示されます。 表示されているゾーン名をクリックすると、該当のゾーンの設定内容を確認できます。 ☞「ゾーン」357 ページ ゾーンが適用されていない場合は、「ゾーン外」と表示されます。
2	ポリシー	対象の Android 端末に適用されているポリシー名が表示されます。 表示されているポリシー名をクリックすると、該当のポリシーの設定内容を確認できます。 ☞「ポリシー」360 ページ ポリシーが適用されていない場合は、「機器の設定」と表示されます。

4.1.10.8 （情報－Android）メッセージ

対象の Android 端末に配信されるメッセージの予定と、配信済みのメッセージを表示します。

配信するメッセージの詳細については、以下を参照してください。

☞「メッセージ通知」223 ページ

◆画面

表示操作［機器］→［一覧］→**Android 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［他の情報を見る］→［メッセージ］**

項番	項目	説明
1	配信されるメッセージ	メッセージについて以下の情報が表示されます。 ●タイトル メッセージのタイトルが表示されます。 タイトルをクリックすると、メッセージ通知画面が表示されます。メッセージの設定の確認や変更ができます。 ☞「メッセージ通知」223 ページ ●スケジュール スケジュールの設定内容が表示されます。 ●次回配信予定 次回の配信日時を表示します。
2	メッセージボックス	対象の Android 端末に配信したメッセージ通知の一覧が表示されます。 ●ステータス 機器側でメッセージ通知が開封済みの場合は が、未開封の場合は が表示されます。 ●メッセージ 配信したメッセージ通知の配信日時、タイトル、本文が表示されます。

4.1.10.9 （情報－iOS）ログ

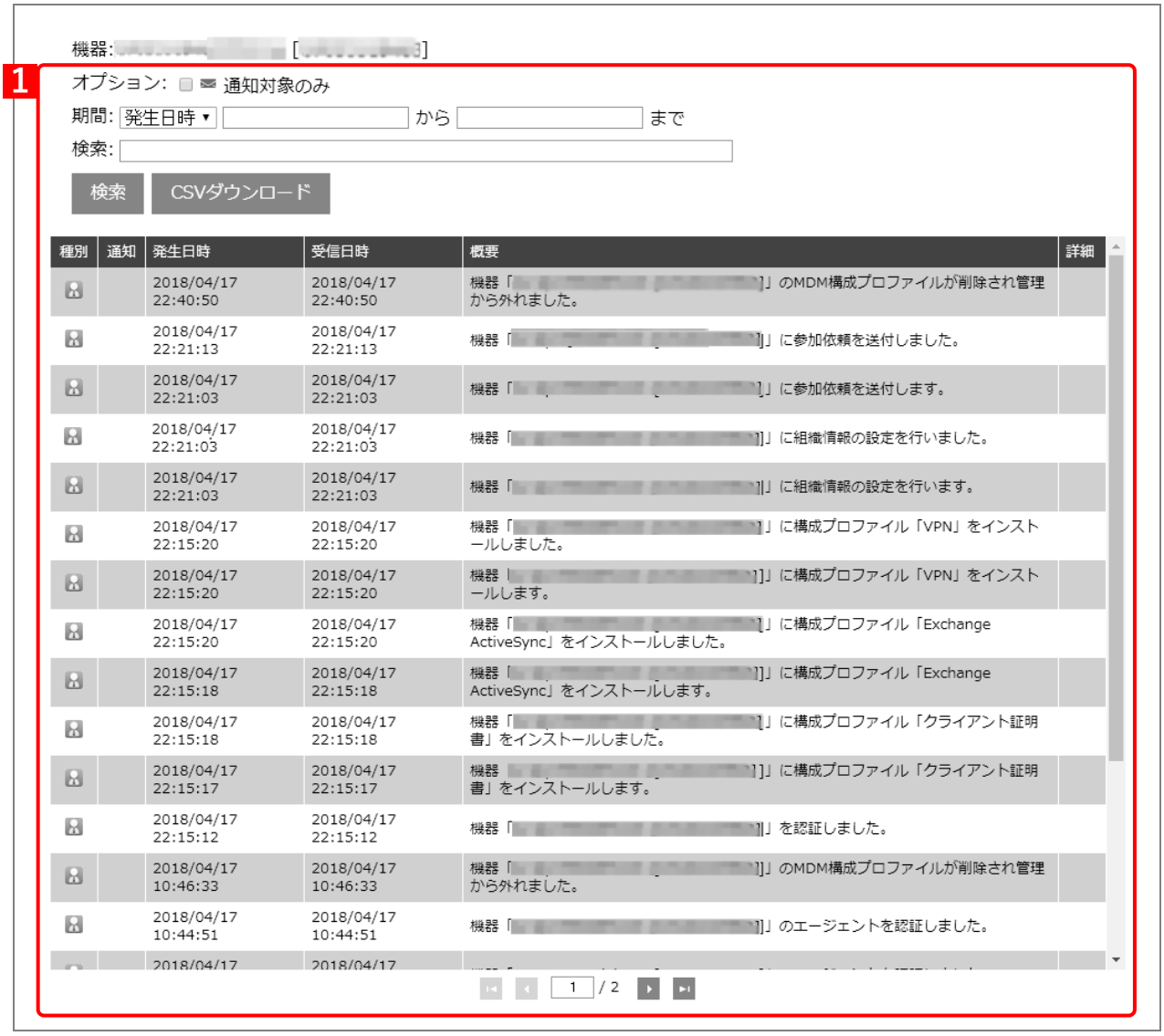
対象の iOS 端末のログをログ画面に表示します。

ログ画面の詳細については、以下を参照してください。

「ログ画面の見かた」646 ページ

◆画面

表示操作　［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ›　**→詳細画面の「情報」の［ログ］**



項番	項目	説明
1	ログ画面	ログ画面に、対象の端末のログだけが表示されます。ログ画面の詳細については、以下を参照してください。 「ログ画面の見かた」646 ページ

4.1.10.10 （情報－iOS）デバイス

対象の iOS 端末の現在の状態を表示します。

◆画面

表示操作 ［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［デバイス］

項番	項目	説明
1	基本	以下の項目が表示されます ●デバイス名 端末名称を変更するに設定すると、機器の管理情報画面で編集した機器名が端末のデバイス名になります。詳細については、以下を参照してください。 「機器の管理情報」67 ページ 「画面（端末名称変更）」386 ページ ●OS バージョン ●ビルドバージョン ●モデル名 ●モデル番号 ●モデムファームウェアバージョン ●シリアル番号 ●ExchangeActiveSync デバイス ID ●MDM プロファイルトピック ●UDID iOS 16.0 以上の端末の場合、宣言型デバイス管理機能が自動で有効になります。その場合「OS バージョン」、「シリアル番号」の値は宣言型デバイス管理によって受信した値が表示されます。
2	SIM 情報	端末に搭載されている SIM の情報が表示されます。 複数の SIM が搭載さている端末では、パネル名の末尾に番号が付いた SIM 情報パネルが、SIM ごとに表示されます。 ●電話番号 SIM に割り振られている電話番号が表示されます。 ●現在のキャリアネットワーク名 端末や iOS のバージョン、キャリアの組み合わせによっては、「現在のキャリアネットワーク名」が「(Unknown)」と表示される場合があります。 仮想移動体通信事業者が表示される場合があります。 ●契約者のキャリアネットワーク名 端末や iOS のバージョン、キャリアの組み合わせによっては、「契約者のキャリアネットワーク名」が「(Unknown)」と表示される場合があります。 仮想移動体通信事業者が表示される場合があります。 ●IMEI ●MEID ●ICCID ●EID ●ローミング状態 「ローミング中です」または「ローミングしていません」が表示されます。 エージェントのバージョン 9.16.0 未満で認証、または 9.16.0 リリース後、一度も同期していない iOS 端末の場合は、項番 11「ローミング」に「状態」として表示されます。
3	OS	以下の情報が表示されます。 ●OS バージョン 対象の iOS 端末の OS バージョンが表示されます。
4	グローバル IP アドレス	対象の iOS 端末が接続しているネットワークのインターネットサービスプロバイダ、またはモバイルデータ通信の場合は、通信事業者の情報が表示されます。 ●グローバル IP アドレス 「NNN.NNN.NNN.NNN」形式の IP アドレスが表示されます。
5	ネットワーク	以下のネットワークの情報が表示されます。 ●Bluetooth MAC アドレス 「XX:XX:XX:XX:XX:XX」形式の MAC アドレスが表示されます。 ●Wi-Fi MAC アドレス

項番	項目	説明
		「XX:XX:XX:XX:XX:XX」形式の端末固有の MAC アドレスが表示されます。 「プライベートアドレス（ランダム MAC アドレス）」は、取得および表示することはできません。 ●インターネット共有(テザリング) インターネット共有（テザリング）が、「有効」または「無効」で表示されます。
6	監視対象	以下の情報が表示されます。 ●監視対象 Apple Configurator 2、または Automated Device Enrollment（ADE）で iOS 端末を監視対象に設定している場合は「有効」と表示されます。また、監視対象に設定されていない場合は「無効」と表示されます。
7	バッテリー	以下の情報が表示されます。 ●バッテリー残量 端末のバッテリー残量が「%」で表示されます。
8	ストレージ	以下の情報が表示されます。 ●デバイス容量 デバイス容量がギガバイト単位で表示されます。 ●利用可能なデバイス容量 利用できるデバイス容量がギガバイト単位で表示されます。 ●iCloud バックアップ iCloud のバックアップが有効の場合は「有効」、無効の場合は「無効」と表示されます。 ●前回の iCloud バックアップ日時 前回の iCloud バックアップ日時が「HH:MM:SS」形式で表示されます。
9	スクリーンロック	以下の情報が表示されます。 ●パスコード保護 端末にパスコードが設定されている場合は「保護されています」と表示され、設定されていない場合は「保護されていません」と表示されます。 ●パスコード準拠（デバイス） 構成プロファイルを含むすべてのパスコードポリシー設定（Apple が定めたものを含む）と、実際のパスコード設定が合致している場合は「準拠しています」と表示され、異なっている場合は「準拠していません」と表示されます。 ●パスコード準拠（プロファイル） 構成プロファイルのパスコードポリシー設定と、実際のパスコード設定が合致している場合は「準拠しています」と表示され、異なっている場合は「準拠していません」と表示されます。
10	OS アップデート情報	以下の情報が表示されます。 ●アップデートの名前 「アップデートの名前」または「(Unknown)」が表示されます。 ●アップデートのバージョン 「アップデートのバージョン」または「(Unknown)」が表示されます。 ●アップデートのビルド番号 「アップデートのビルド番号」または「(Unknown)」が表示されます。 ●アップデートのステータス 以下のいずれかが表示されます。 ・「未ダウンロード」 ・「ダウンロード中」 ・「ダウンロード済」 ・「(Unknown)」
11	ローミング	以下の情報が表示されます。 ●音声ローミング設定 「有効」または「無効」が表示されます。 ●データローミング設定 「有効」または「無効」が表示されます。

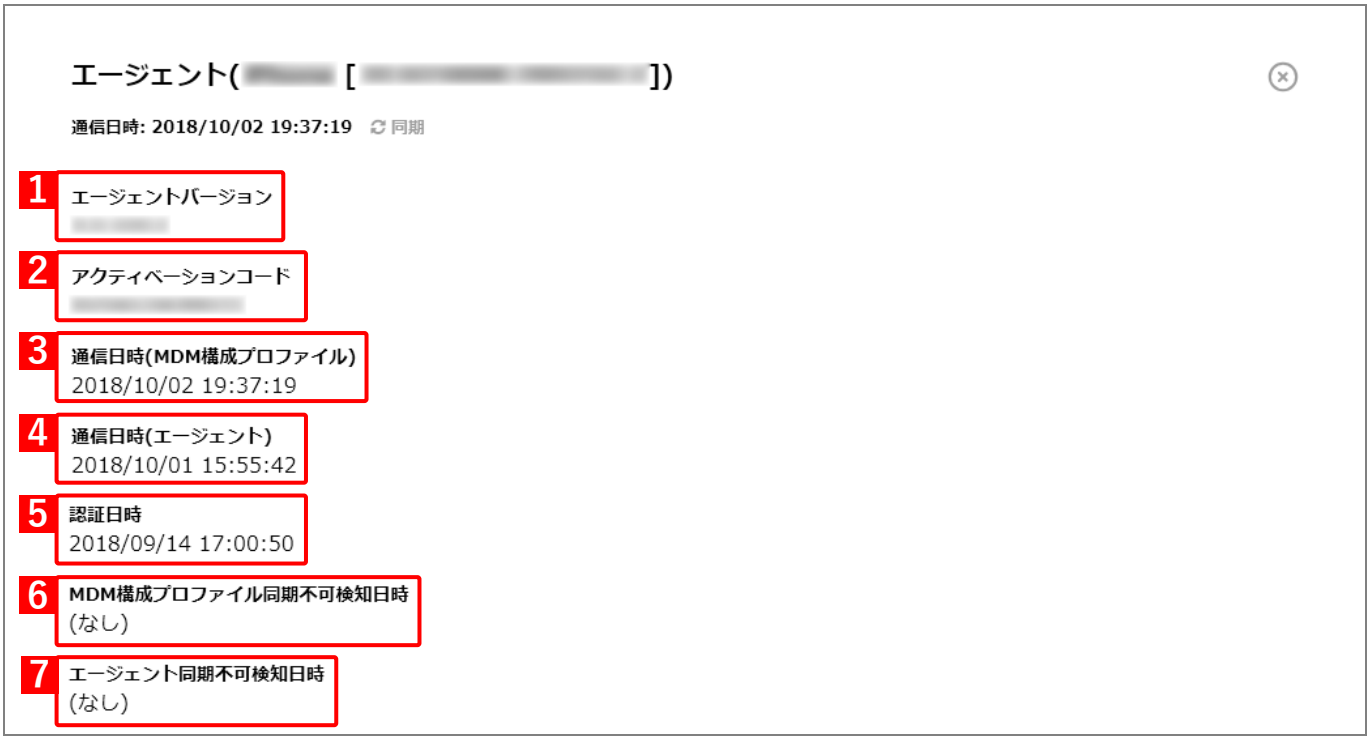
項番	項目	説明
12	暗号化	以下の情報が表示されます。 ●ハードウェア暗号化レベル パスコードが設定されている場合は「データ保護は有効です」と表示され、設定されていない場合は「データ保護は無効です」と表示されます。
13	Jailbreak	以下の情報が表示されます。 ●状態 「Jailbreak 状態」、「問題なし」、「(Unknown)」のいずれかが表示されます。 エージェントが認証されていない場合、「(Unknown)」と表示されます。
14	その他の情報	以下の情報が表示されます。 ●iTunesStore アカウント 「サインイン済み」または「未設定」が表示されます。 ●iTunesStore アカウントハッシュ iTunesStore アカウントハッシュが表示されます。 ●アクティベーションロック アプリ「iPhone を探す」のアクティベーションロックの状態を「有効」または「無効」で表示します。 ●Bypass Code 監視対象端末の場合、Bypass Code が表示されます。 ●「探す」設定 位置情報を使ったサービスの設定状況を示します。「有効」または「無効」が表示されます。 「iPhone を探す」などの位置情報を使用するサービスです。 ●おやすみモード 「有効」または「無効」が表示されます。 ●紛失モード 「有効」または「無効」が表示されます。 ●Shared iPad 設定 「有効」または「無効」が表示されます。 ●Shared iPad ユーザー最大数 Shared iPad（共有 iPad）設定が「有効」の場合、ユーザー最大数が表示されます。 ●Shared iPad オンライン認証の猶予日数 Shared iPad（共有 iPad）設定が「有効」の場合、ユーザーが Apple ID サーバーとの認証をせずにログインできる日数、または「毎回オンライン認証する」が表示されます。 iPad OS 16.0 未満の場合、「(Unknown)」と表示されます。 ●Shared iPad 自動スリープまでの時間 Shared iPad（共有 iPad）設定が「有効」の場合、端末がアイドル状態からスリープに移行するまでの秒数が表示されます。 iPad OS 17.0 未満の場合、「(Unknown)」と表示されます。 ●Shared iPad パスワード入力までの時間 Shared iPad（共有 iPad）設定が「有効」の場合、端末がスリープ状態からパスワードの入力が必要になるまでの秒数、または「毎回パスワードを入力する」が表示されます。 iPad OS 17.0 未満の場合、「(Unknown)」と表示されます。 ●自動ログアウトまでの時間 Shared iPad（共有 iPad）設定が「有効」の場合、ユーザーログイン後、端末が非アクティブ状態から自動ログアウトするまでの秒数、または「自動でログアウトしない」を表示します。 iPad OS 14.5 未満の場合、「(Unknown)」と表示されます。 ●Get Token エンドポイントのサポート 「有効」または「無効」が表示されます。

4.1.10.11 （情報－iOS）エージェント

対象の iOS 端末のエージェント情報を表示します。

◆画面

表示操作 ［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［エージェント］**



項番	項目	説明
1	エージェントバージョン	機器を管理、運用するためのアプリのバージョンです。 iOS エージェントがインストールされていないとエージェントバージョンは表示されません。
2	アクティベーションコード	本製品のエージェント認証時に必要な英数字のコードです。 ライセンス認証後にエージェント認証を行う場合や、ポータル画面からエージェント認証を行う場合はアクティベーションコードの入力は不要です。
3	通信日時(MDM 構成プロファイル)	MDM 構成プロファイルの通信日時が表示されます。 通信日時が赤字で表示されている場合、無通信検知されています。 通信日時が赤字で表示かつ、末尾に「(管理外)」または「(同期不可)」と表示されている機器は、管理外検知されています。資産管理対象で機器一覧に表示されている場合は、機器オプションパッケージが割り当てられていれば、ライセンスは割り当てられた状態のままになります。管理外検知された機器については、以下のとおりです。 ・管理外 端末から構成プロファイルが手動で削除された場合に表示されます。 ・同期不可 端末の MDM 構成プロファイルまたはエージェントが継続的に管理サイトとの通信ができない場合に表示されます。

項番	項目	説明
4	通信日時(エージェント)	iOS エージェントの通信日時が表示されます。iOS エージェントがインストールされていない場合は「(なし)」と表示されます。 管理外検知されても赤字で表示されません。
5	認証日時	iOS 端末を認証した日時が表示されています。
6	MDM 構成プロファイル同期不可検知日時	管理サイトと MDM 構成プロファイルが同期できない状態と検知された場合に、検知した日時が表示されます。管理サイトと同期ができている場合は「(なし)」と表示されます。 同期不可検知日時が表示された場合は、同期不可検知の種類によって対応が異なります。(※1)
7	エージェント同期不可検知日時	管理サイトとエージェントが同期できない状態と検知された場合に、検知した日時が表示されます。管理サイトと同期ができている場合、もしくは管理外検知されている場合は「(なし)」と表示されます。 同期不可検知日時が表示された場合は、同期不可検知の種類によって対応が異なります。(※1)

※1：同期不可検知の種類によって対応が異なります。該当の手順にしたがって対応してください。

≪MDM 構成プロファイル同期不可検知日時または管理外検知が表示された場合≫
再認証以外に復旧方法はありませんので、再度認証を行ってください。

≪エージェント同期不可検知日時が表示された場合≫
iOS 端末からエージェントを立ち上げ、同期を行うことで復旧できます。

4.1.10.12 （情報－iOS）アプリケーション

対象の iOS 端末にインストールされているアプリの一覧を表示します。iOS 16.0 未満／以上で表示される項目が異なります。また、詳細画面を表示して、アプリの詳細情報を確認することもできます。

画面（iOS 16.0 未満）

画面（iOS 16.0 以上）

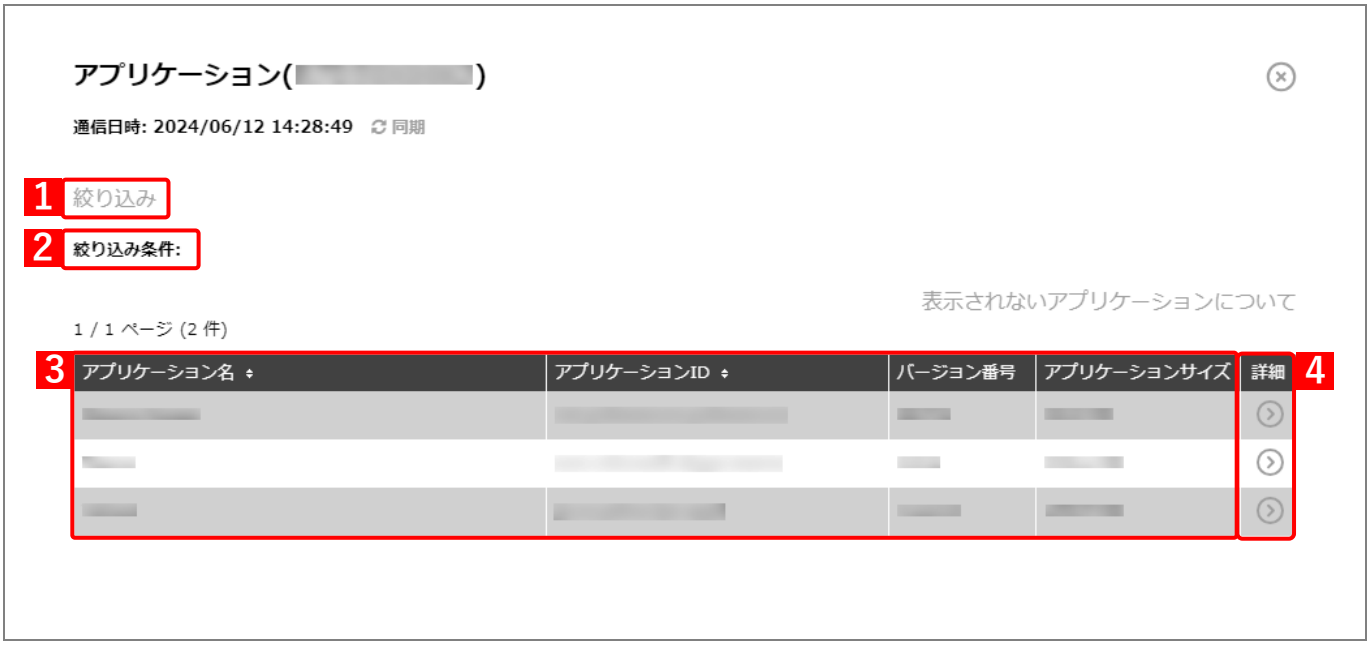
画面（アプリの詳細）

iOS 端末に内蔵されているアプリは、本画面では確認できません。Apple のサイトで対象の iOS 端末の情報から確認してください。ただし、Apple 製の無料アプリは、本画面で確認できます。

本画面で表示されるアプリ名は、App Store で表示されているアプリ名と異なることがあります。

◆画面（iOS 16.0 未満）

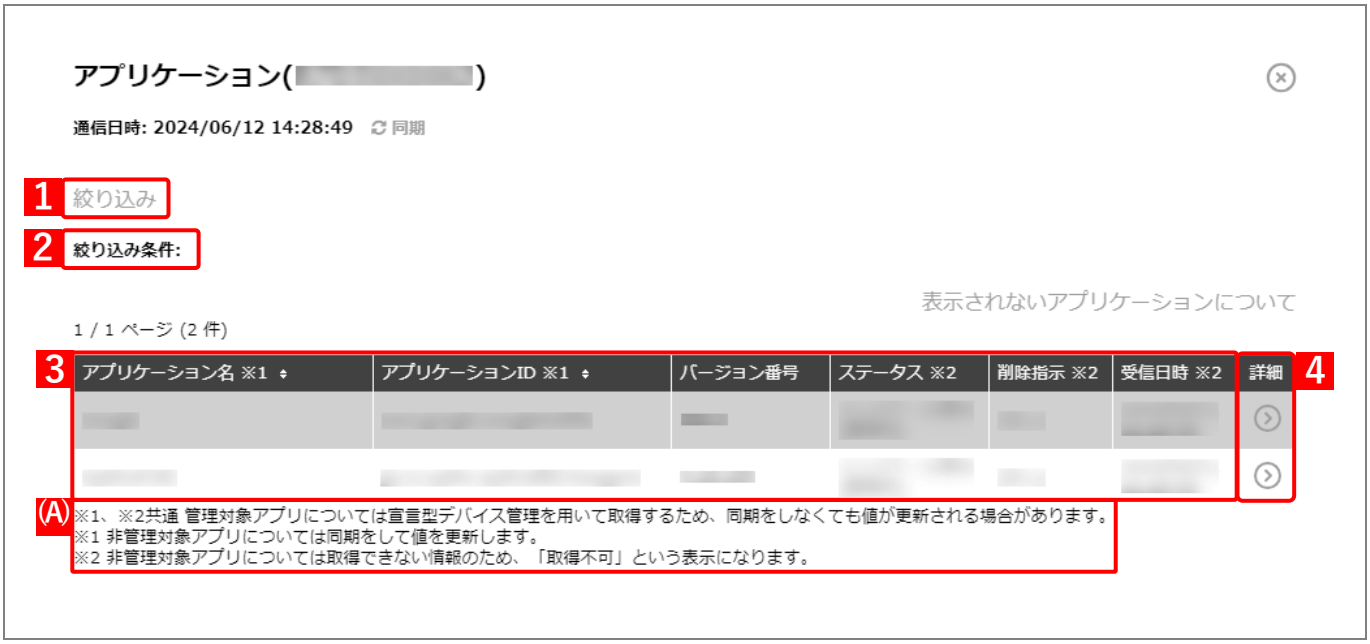
表示操作　［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［アプリケーション］**



項番	項目	説明
1	［絞り込み］	項番 3「アプリ一覧」に表示する情報を以下の項目を条件にして絞り込めます。 ●アプリケーション名 ●アプリケーション ID
2	絞り込み条件	項番 1［絞り込み］を設定した場合、設定した条件が表示されます。 ✖ をクリックすると、設定した条件はクリアされ、すべてのアプリが項番 3「アプリ一覧」に表示されます。
3	アプリ一覧	対象の機器にインストールされているアプリの以下の情報が表示されます。 ●アプリケーション名 ●アプリケーション ID ●バージョン番号 ●アプリケーションサイズ
4	ⓘ（詳細）	クリックすると、対象のアプリの詳細な情報が表示されます。 「画面（アプリの詳細）」159 ページ

◆画面（iOS 16.0 以上）

表示操作［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［アプリケーション］**



項番	項目	説明
1	［絞り込み］	項番 3「アプリ一覧」に表示する情報を以下の項目を条件にして絞り込めます。 ●アプリケーション名 ●アプリケーション ID
2	絞り込み条件	項番 1［絞り込み］を設定した場合、設定した条件が表示されます。 ✎✖ をクリックすると、設定した条件はクリアされ、すべてのアプリが項番 3「アプリ一覧」に表示されます。
3	アプリ一覧	対象の機器にインストールされているアプリの以下の情報が表示されます。 ●アプリケーション名 ※1 ●アプリケーション ID ※1 ●バージョン番号 ●ステータス ※2 ●削除指示 ※2 ●受信日時 ※2 ✎※1、※2 については、(A) を参照してください。
4	ⓘ（詳細）	クリックすると、対象のアプリの詳細な情報が表示されます。 ☞「画面（アプリの詳細）」159 ページ

◆画面（アプリの詳細）

iOS 16.0 未満／以上で表示される項目が異なります。ここでは、iOS 16.0 以上の端末の画像を例に使用しています。
表示される各項目の詳細については、メーカーまたは開発・提供元へ確認してください。

表示操作　［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「情報」の［アプリケーション］→一覧から対象のアプリの ＞

項番	項目	説明
1	アプリケーション名 ※1	アプリ名が表示されます。 ※1 は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※1 については（A）を参照してください。
2	アプリケーション ID ※1	アプリケーション ID が表示されます。 ※1 は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※1 については（A）を参照してください。
3	バージョン番号	アプリの CFBundleShortVersionString が表示されます。
4	ビルド番号 ※1	アプリの CFBundleVersion が表示されます。 ※1 は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※1 については（A）を参照してください。
5	アプリケーションサイズ	アプリのファイルサイズが表示されます。
6	メモリサイズ	アプリのメモリサイズが表示されます。
7	データサイズ	アプリのデータサイズが表示されます。
8	インストール済み	アプリがインストール済みか表示されます。
9	実行可能	アプリが実行可能か表示されます。
10	外部バージョン ID（iTunes Search API 用）	アプリの自動バージョンアップを判定する情報として、外部バージョン ID が表示されます。
11	App Store 機能を利用可能	App Store 機能を利用可能かどうか表示されます。
12	「App とブック」管理配布	「App とブック」管理配布があるかどうか表示されます。
13	ベータ版アプリ	ベータ版アプリがあるかどうか表示されます。
14	アドホックコード署名	アドホックコード署名が表示されます。
15	アップデート可能	アプリが App Store でアップデートできるか以下のとおり表示されます。 ●「はい」または「App Store 機能：はい」 現在、アップデートができます。 配信方法が App Store 配信、手動 App インストールおよび App とブック（ユーザー）の場合は、「App Store 機能：はい」と表示されます。 ●「いいえ」または「App Store 機能：いいえ」 現在、アップデートができません。 配信方法が App とブック（機器）の場合は、「App Store 機能：いいえ」と表示されます。 ●「(なし)」 以下の理由により、アップデートができません ・アプリをサポートしていない端末を利用しているため ・アプリの最後通信日時が、本機能が追加される以前のため
16	アプリケーション削除防止	アプリの削除が防止されているかどうか表示されます。 すでに配信しているアプリの削除を防止したい場合は、以下の機能で「削除防止」を設定して端末と同期してください。 「アプリケーション配信」530 ページ
17	ステータス ※2	アプリの状態が表示されます。 本項目は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※2 については（A）を参照してください。
18	削除指示 ※2	アプリの削除指示がされているかどうか表示されます。 本項目は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※2 については（A）を参照してください。
19	受信日時 ※2	端末から宣言型デバイス管理の通知を受信した日時が表示されます。 本項目は端末の OS バージョンが iOS 16.0 以上の場合、表示されます。※2 については（A）を参照してください。

項番	項目	説明
20	［強制バージョンアップ］	アプリを強制的にバージョンアップしたいときは、クリックします。 アプリのアップデートの有無にかかわらず、強制的にバージョンアップできます。 以下の条件をすべて満たしていない場合は、アプリを強制的にバージョンアップできません。 ・管理対象アプリ ・アプリケーション配信で配信されたアプリ 「アプリケーション配信」530 ページ ・App Store アプリまたは B2B アプリ ・管理サイトにログインしているユーザーのユーザー種別が「管理者」または「操作」

4.1.10.13 （情報－iOS）プロファイル

対象の iOS 端末にインストールされているプロファイル情報を表示します。

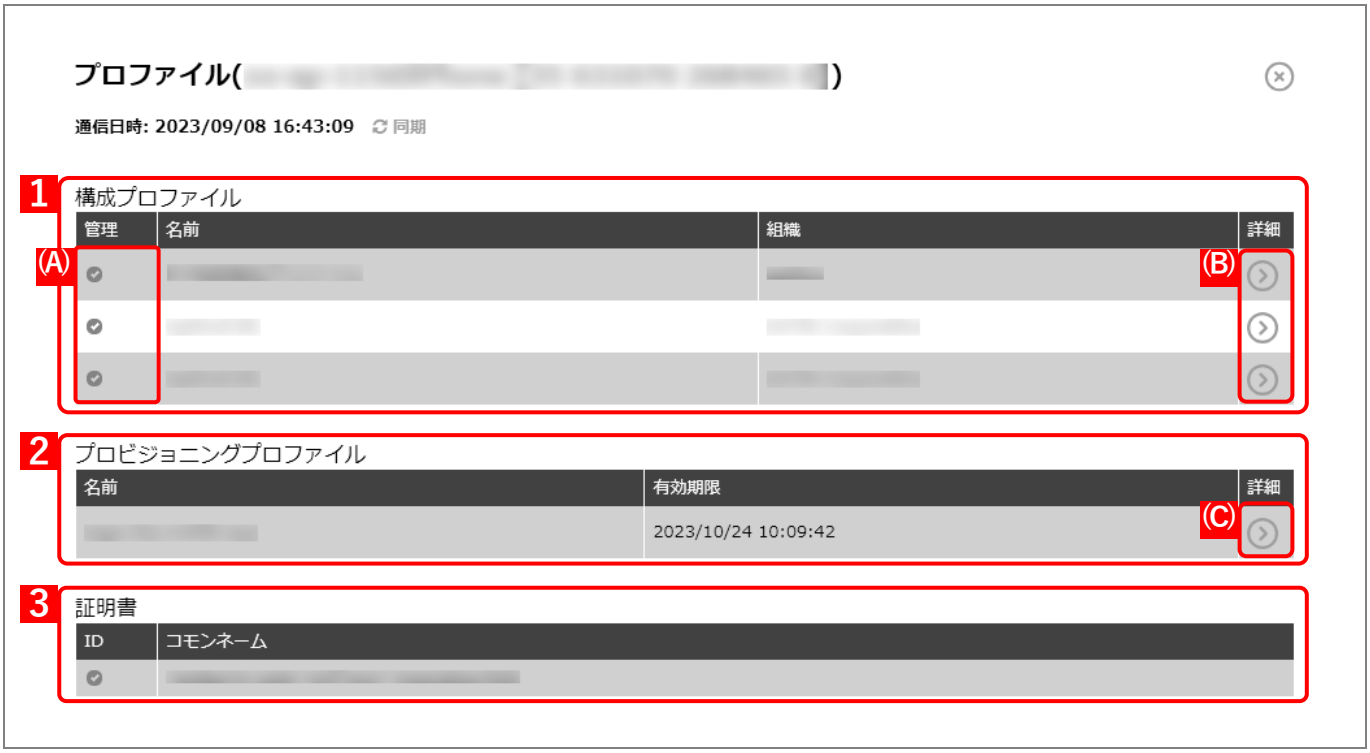
画面

画面（構成プロファイルの詳細）

画面（プロビジョニングプロファイルの詳細）

◆画面

表示操作 ［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ›**→詳細画面の「情報」の［プロファイル］**

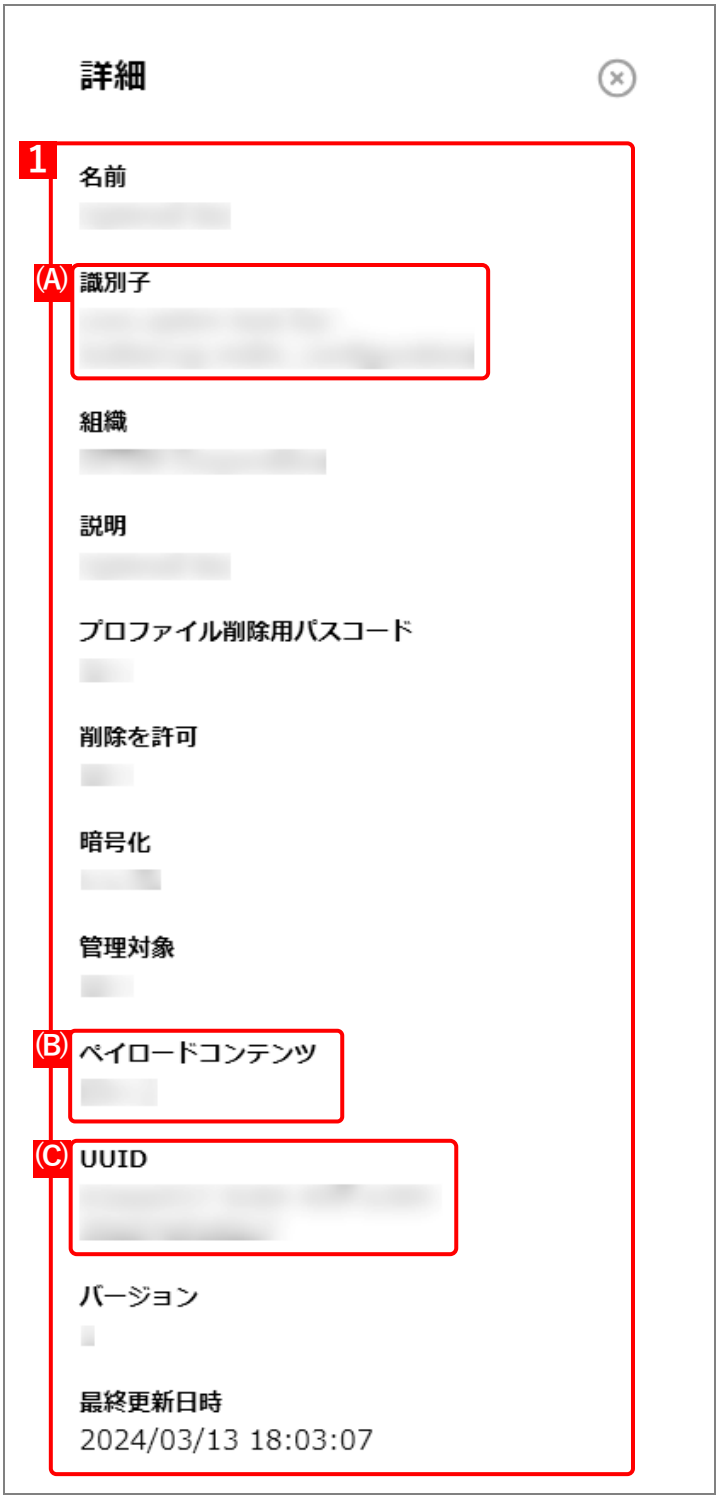


項番	項目	説明
1	構成プロファイル	対象の iOS 端末にインストールされている構成プロファイルが表示されます。 本製品からインストールした構成プロファイルは、(A)「管理」にチェックマークが表示されます。ただし、削除防止を設定している構成プロファイルは、チェックマークが表示されません。チェックマークの有無は関係なく、構成プロファイルの挙動は同じです。構成プロファイルの詳細については、以下を参照してください。 「構成プロファイル」500 ページ (B)「詳細」の›をクリックすると、構成プロファイルの詳細が確認できます。詳細については、以下を参照してください。 「画面（構成プロファイルの詳細）」163 ページ
2	プロビジョニングプロファイル	対象の iOS 端末にインストールされているプロビジョニングプロファイルが表示されます。 プロビジョニングプロファイルは、本製品からは削除できません。Apple Configurator 2 から削除してください。 (C)「詳細」の›をクリックすると、プロビジョニングプロファイルの詳細が確認できます。詳細については、以下を参照してください。 「画面（プロビジョニングプロファイルの詳細）」164 ページ

項番	項目	説明
3	証明書	対象の iOS 端末にインストールされている TLS 証明書が表示されます。 (D)「コモンネーム」は、プロファイルレポートを作成するときに必要な入力値です。 「画面（［証明書］選択時）」250 ページ

◆画面（構成プロファイルの詳細）

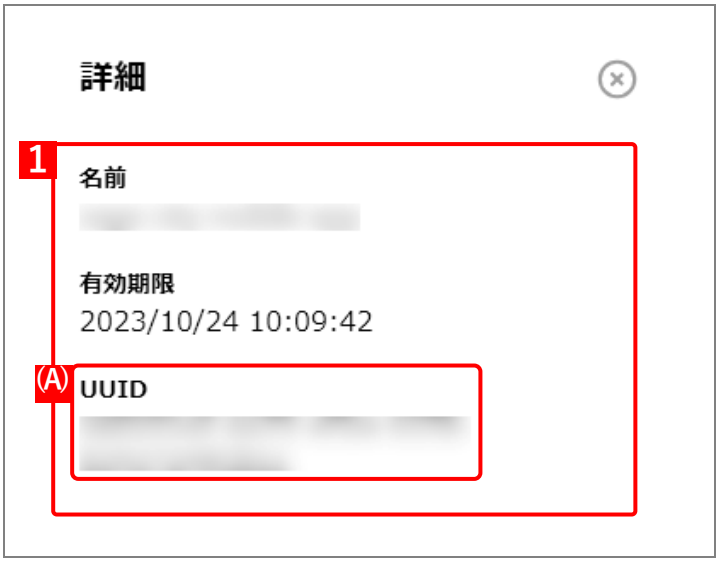
表示操作 **［機器］→［一覧］→iOS 端末の機器名または「詳細」の → →詳細画面の「情報」の［プロファイル］→一覧から対象の構成プロファイルの →**



項番	項目	説明
1	（詳細）	構成プロファイルの各項目の詳細情報が表示されます。 各項目については、Apple に問い合わせてください。 （A）「識別子」は、OS バージョンやキッティング方法によって異なります。 （B）「ペイロードコンテンツ」、（C）「UUID」は、プロファイルレポートを作成するときに必要な入力値です。 「画面（［構成プロファイル］選択時）」249 ページ

◆画面（プロビジョニングプロファイルの詳細）

表示操作　**［機器］→［一覧］→iOS 端末の機器名または「詳細」の ＞ →詳細画面の「情報」の［プロファイル］→一覧から対象のプロビジョニングプロファイルの ＞**



項番	項目	説明
1	（詳細）	プロビジョニングプロファイルの各項目の詳細情報が表示されます。 各項目については、Apple に問い合わせてください。 （A）「UUID」は、プロファイルレポートを作成するときに必要な入力値です。 「画面（［プロビジョニングプロファイル］選択時）」250 ページ

4.1.10.14 （情報－iOS）位置

iOS 端末から送られた位置情報を表示します。

位置情報取得の条件については、以下を参照してください。

「iOS 端末の位置情報の諸条件」166 ページ

- 位置情報送信を一度も行っていない端末は、［位置］メニューが表示されません。
- 本製品から端末の GPS を ON にすることはできません。
- 取得した位置情報の精度が低いと情報が破棄されるため、管理サイトに反映されません。
- エージェントバージョン 5.9.0 以上の端末に対応しています。

◆画面

表示操作　［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ＞ **→詳細画面の「情報」の［位置］**

項番	項目	説明
1	［位置情報を更新］	位置情報を更新します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 端末の状態によっては反映に時間がかかる場合があります。 エージェントバージョン 5.9.0 以上の端末に対応しています。
2	測位情報	以下の情報が表示されます。 ●受信日時 管理サイトが端末の位置情報を取得した日時が表示されます。 ●測位日時 端末が保持している位置情報を測位した日時が表示されます。 ●北緯 測位した位置の北緯が表示されます。 ●東経 測位した位置の東経が表示されます。
3	位置情報履歴	対象の端末が取得した位置情報の履歴を確認できます。 位置情報の履歴は最大 100 件まで表示されます。 例えば、「1/38」と表示されている場合は、履歴が 38 件あるうちの、最新の履歴が表示されていることを示しています。 をクリックして、履歴の表示を切り替えることができます。
4	地図	位置情報が地図で表示されます。 が表示されている位置が、地図上の端末の位置です。
5	［Google マップで表示］	クリックすると、新しいウインドウで Google マップとして表示されます。

◆iOS 端末の位置情報の諸条件

iOS 端末から位置情報を受信するための動作条件、位置情報測位契機、位置情報送信契機は以下のとおりです。内容を確認し、位置情報の受信を行ってください。

測位結果の情報は確実性を保証できる情報ではありません。

測位条件は端末の仕様に準じます。

iOS 13 以上の端末は、エージェントの位置情報を常に許可にしていても、3 日に 1 回「位置情報の使用許可」のポップアップが表示されます。

項目	エージェント利用で AppSwitcher 上にある（推奨）	エージェント利用で AppSwitcher 上にない（非推奨）	紛失モード
動作条件	以下の動作条件が満たされている必要があります。 ●エージェントがインストールされている。 ●エージェントの認証が済んでいる。 ●エージェントが起動している（AppSwitcher 上にある）。 ●端末の「プライバシー」以下の「位置情報サービス」でアクセスが許可されている。 ●端末の設定内の「App のバックグラウンド更新」で、本製品が「有効」になっている。 ●iOS 9 以上の端末の場合、「低電力モード」が無効に設定されている（この設定を有効にすると、「App のバックグラウンド更新」が強制的に無効になるため）。	以下の動作条件が満たされている必要があります。 ●エージェントがインストールされている。 ●エージェントの認証が済んでいる。 ●エージェントが起動していない（AppSwitcher 上にない）。	以下の動作条件が満たされている必要があります。 ●iOS 9.3 以上で、監視対象状態の端末である。 紛失モードの場合は、エージェントアプリの有無に関係なく利用できます。

項目	エージェント利用で AppSwitcher 上にある（推奨）	エージェント利用で AppSwitcher 上にない（非推奨）	紛失モード
位置情報測位契機	以下のいずれかの契機で測位します。 ●バックグラウンドで動作している ●エージェント起動時 ●エージェント同期ボタン押下時 ●メッセージ配信受信後にメッセージ画面を表示したとき ●基地局変更時（※2） ●管理サイトの位置情報更新ボタン押下時 ●Background Fetch（※1） ●他アプリ利用による測位	iOS の大幅位置情報変更サービスが位置情報の更新を検知したときに測位します。（※3）	端末が紛失モード中で、管理サイトのリモート操作の「位置情報取得」の操作がされたときに測位します。
位置情報送信契機	端末のロックの状態にかかわらず、以下の契機で位置情報を送信します。 ●エージェント認証時 ●エージェント同期ボタン押下時 ●メッセージ配信受信後にメッセージ画面を表示したとき ●基地局変更時（※2） ●管理サイトの位置情報更新ボタン押下時 ●Background Fetch（※1）	端末がロックされていない状態で位置情報を送信します。 （※4）	端末のロックの状態にかかわらず、端末が紛失モード状態で、管理サイトのリモート操作の「位置情報取得」の操作がされて、端末がその情報を受信したあとに位置情報を送信します。

※1：Background Fetch は、Apple から提供されている機能で iOS 7.0 以上に搭載されています。
この機能を使用すると iOS 側が日々のユーザーの使用状況を学習し、適切なタイミングで対象のアプリを呼び起こすことができます。詳細については、Apple に問い合わせてください。

※2：基地局の境界で通信が頻発することを防ぐため、前回の送信時間からおよそ 1 分以上経過した場合のみ送信します。また、OS 仕様の制約上、そのときに取得した位置情報は送信できません。端末内に保有していた位置情報のみを送信します。

※3：大幅位置情報変更サービスの動作条件は Apple の仕様に準じます。また、大幅位置情報変更サービスによる動作条件仕様は Apple により非公開となっています。

※4：ロック解除後の画面になっている状態です。大幅位置情報変更サービスによる送信条件は Apple の仕様に準じます。また、大幅位置情報変更サービスによる送信条件仕様は Apple により非公開となっています。

4.1.10.15 （情報－iOS）ADE

対象の iOS 端末の ADE の情報を表示します。詳細については、以下を参照してください。

「ADE 機器管理」509 ページ

◆画面

表示操作［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［他の情報を見る］→［ADE］**

項番	項目	説明
1	ADE	ADE に関する以下の情報が表示されます。 ●ADE 状態 ●ADE 定義プロファイル(適用済) ●ADE 定義プロファイル ●モデル ●ADE 登録日時 ●ADE プロファイル割り当て日時 ●端末反映日時

項番	項目	説明
2	［ADE と同期］または［ADE から機器情報を取得］	ADE と同期します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ログインしているユーザー種別によって、表示されるボタン名、処理が異なります。 ・ユーザー種別が管理者および操作の場合 ［ADE と同期］と表示されます。 ADE サーバーから ADE トークンに紐づいている機器一覧の差分を取得します。また、ADE 定義プロファイル（適用済）と ADE 定義プロファイルが異なる機器について、ADE 定義プロファイルを ADE 機器に紐づける処理を行います。 ・ユーザー種別が閲覧者の場合 ［ADE から機器情報を取得］と表示されます。 ADE サーバーから ADE トークンに紐づいている機器一覧の差分を取得します。

4.1.10.16 （情報－iOS）メッセージ

対象の iOS 端末に配信されるメッセージの予定と、配信済みのメッセージを表示します。

配信するメッセージの詳細については、以下を参照してください。

☞「メッセージ通知」223 ページ

◆画面

表示操作 ［機器］→［一覧］→**iOS 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［他の情報を見る］→［メッセージ］**

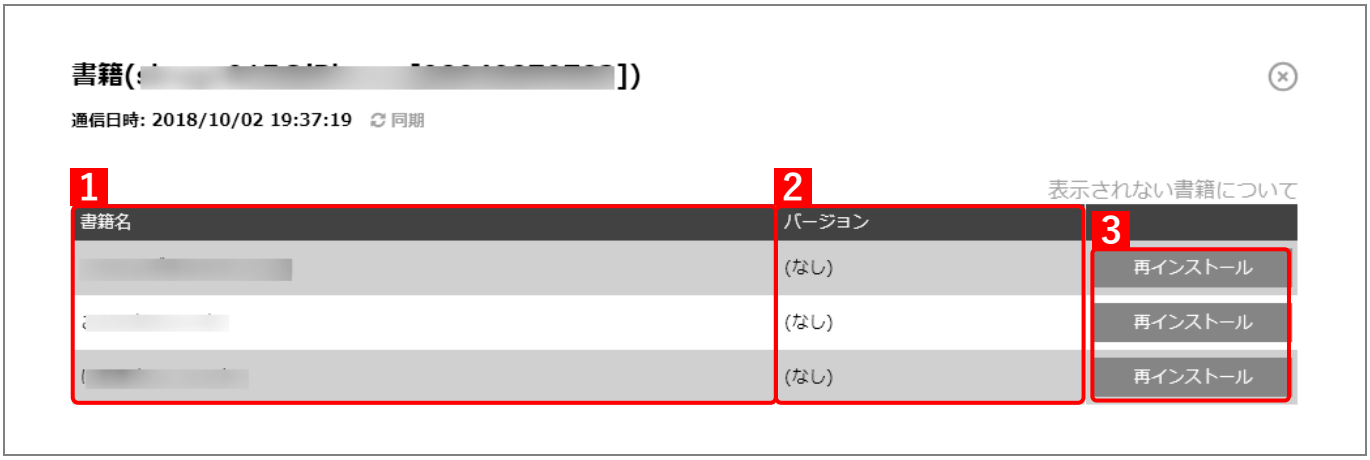
項番	項目	説明
1	配信されるメッセージ	配信されるメッセージ通知の一覧が表示されます。 ●タイトル メールの件名に該当するタイトルが表示されます。 タイトルをクリックすると該当メッセージの詳細画面に移動し、内容を編集できます。詳細については、以下を参照してください。 ☞「メッセージ通知」223 ページ ●スケジュール 設定されているスケジュールが表示されます。 ●次回配信予定 次回の配信予定スケジュールが表示されます。
2	メッセージボックス	対象の iOS 端末に配信したメッセージ通知の一覧が表示されます。 ●ステータス 機器側でメッセージ通知が開封済みの場合は 📧 が、未開封の場合は 📥 が表示されます。 ●メッセージ 配信したメッセージ通知の配信日時、タイトル、本文が表示されます。

4.1.10.17 （情報－iOS）書籍

「App とブック」で配信した書籍を一覧表示します。

◆画面

表示操作 ［機器］→［一覧］→iOS 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［他の情報を見る］→［書籍］



項番	項目	説明
1	書籍名	「App とブック」で配信された書籍名が表示されます。
2	バージョン	すでにインストールされている書籍のバージョンが更新された場合にバージョン情報が表示されます。 書籍のバージョンが更新されていない場合は「(なし)」と表示されます。
3	［再インストール］	クリックすると、書籍が iOS 端末に再インストールされます。新しいバージョンがある場合は、更新されたバージョンの書籍がインストールされます。

4.1.10.18 （情報－Windows）ログ

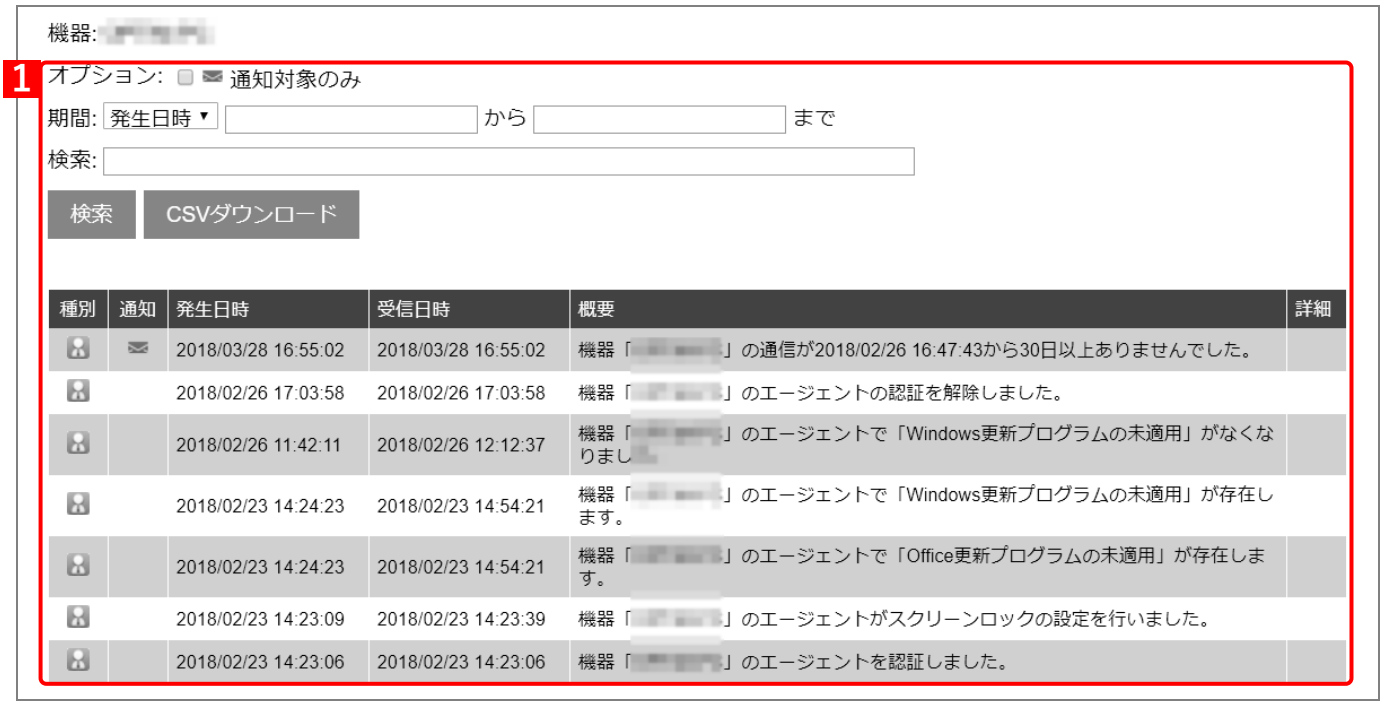
対象の Windows 端末のログをログ画面に表示します。

ログ画面の詳細については、以下を参照してください。

「ログ画面の見かた」646 ページ

◆画面

表示操作［機器］→［一覧］→Windows 端末の機器名または「詳細」の ›› →詳細画面の「情報」の［ログ］



項番	項目	説明
1	ログ画面	ログ画面に、対象の端末のログだけが表示されます。ログ画面の詳細については、以下を参照してください。 「ログ画面の見かた」646 ページ

4.1.10.19 （情報－Windows）デバイス

対象の Windows 端末の現在の状態を表示します。

情報を取得できない場合は、「(Unknown)」と表示されます。

ドメインに参加している PC の場合は、パスワードポリシーのパネルに「(Unknown)」と表示されます。

◆画面

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ＞ →詳細画面の「情報」の［デバイス］**

項番	項目	説明
1	基本	以下の情報が表示されます。 ●コンピューター名 ●ワークグループ コンピューターがワークグループに参加しているときのみ表示されます。 ●ドメイン コンピューターがドメインに参加しているときのみ表示されます。 ●Windows バージョン ●Windows プロダクト ID ●システム製造元 ●システムモデル ●シリアル番号 ●コンピューターSID
2	OS	以下の情報が表示されます。 ●OS バージョン
3	グローバル IP アドレス	以下の情報が表示されます。 ●グローバル IP アドレス 「NNN.NNN.NNN.NNN」形式の IP アドレスが表示されます。
4	ネットワーク	検知されたネットワークごとにパネルが表示され、ネットワークの情報が表示されます。パネルタイトルにネットワーク表示名が、「ネットワーク - 表示名」の形式で表示されます。 ●NIC 名 ●接続方法 以下のいずれかの接続方法が表示されます。 ・「有線」、「無線」、「モバイル」、「Bluetooth」 ●MAC アドレス 「XX:XX:XX:XX:XX:XX」形式の MAC アドレスが表示されます。 ●IP アドレス ・形式（IPv4）：「NNN.NNN.NNN.NNN/NNN」 ・形式（IPv6）：「XX:XX:...:XX」 ・IP アドレスが 0 個の場合は空欄。 ●デフォルトゲートウェイ ・0 個の場合は「(なし)」 ●DHCP 「有効」または「無効」が表示されます。 ●DHCP サーバー DHCP サーバーの IP アドレスが表示されます。 ●DNS サーバー DNS サーバーの IP アドレスが表示されます。 ・0 個の場合は「(なし)」 ●DNS サフィックス ・0 個の場合は「(なし)」 ●ネットワーク グローバルネットワーク名が表示されます。グローバルネットワーク名をクリックすると、ネットワーク画面へリンクします。 外部ネットワークに繋がっていない NIC の場合は、「(なし)」と表示され、外部ネットワークに繋がっているが当該のネットワークがネットワーク画面で登録がされていない場合は、「未作成」と表示されます。詳細については、以下を参照してください。 「ネットワーク」653 ページ 「ネットワークマップ」187 ページ

項番	項目	説明
		●電話番号 SIM カード情報が存在する場合は、電話番号が表示されます。 ●現在のキャリアネットワーク SIM カード情報が存在する場合は、キャリアネットワークが表示されます。 ●IMEI/MEID SIM カード情報が存在する場合は、IMEI/MEID が表示されます。 検知されたネットワークごとに表示されます。 ●ICCID SIM カード情報が存在する場合は、SIM カード／UIM カードごとに固有な認識番号が表示されます。
5	プリンター1～	以下の情報が表示されます。 ●名前 プリンター名が表示されます。 ●ポート ポート番号が表示されます。 検知されたプリンターごとに表示されます。
6	ハードウェア	以下の情報が表示されます。 ●種別 機種の種別が以下の項目から表示されます。 ・「デスクトップ」、「ノート PC」、「タブレット」、「その他」 ●CPU CPU 名、クロック数（GHz 単位で小数点以下 2 桁まで）が表示されます ●メモリ メモリサイズが小数点以下 2 桁まで表示されます。 ●マザーボード マザーボード名が表示されます。 検知されたマザーボードごとに表示されます。 ●ビデオカード ビデオカード名が表示されます。 ●TPM TPM のバージョンが表示されます。
7	BIOS	以下の情報が表示されます。 ●メーカー メーカー名が表示されます。 ●バージョン ●日付 日付が「YYYY/mm/dd」形式で表示されます。 タイムゾーンに関係なく取得した日付を表示します。
8	ドライブ	以下の情報が表示されます。 ●パネルタイトル ドライブ名が表示されます。 ●総容量 総容量が小数点以下 2 桁まで表示されます。 ●空き容量 空き容量が小数点以下 3 桁まで表示されます。 検知されたドライブごとに表示されます。
9	ログオンユーザー1	以下の情報が表示されます。 ●ユーザー名 ●SID ●既定の Web ブラウザー名前 ●既定の Web ブラウザーバージョン ●既定の電子メールプログラム 名前

項番	項目	説明
		●既定の電子メールプログラム バージョン ●通常使うプリンター 名前 ●通常使うプリンター ポート 検知されたユーザーごとに表示されます。
10	パスワードポリシー	以下の情報が表示されます。 ●文字数 パスワードポリシーの文字数が表示されます。 ●有効期間 パスワードポリシーの有効期間の日数が表示されます。 ●履歴記録数 パスワードポリシーの履歴記録数が表示されます。 ●変更禁止期間 パスワードポリシーの変更禁止期間が表示されます。 ●複雑なパスワードを強制する 「有効」または「無効」が表示されます。
11	リモートロック	以下の情報が表示されます。 ●状態 リモートロック状態が「ロックされています」または「解除されています」で表示されます。
12	リモートデスクトップ	対象の Windows 端末のリモートデスクトップ接続設定の情報が表示されます。 ●リモートデスクトップ接続の許可 「有効」または「無効」が表示されます。 ●コンピュータの接続にネットワークレベル認証の使用を求める 「有効」または「無効」が表示されます。

4.1.10.20 （情報－Windows）エージェント

対象の Windows 端末のエージェント情報を表示します。

◆画面

表示操作 ［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［エージェント］

項番	項目	説明
1	エージェントバージョン	機器を管理、運用するためのアプリのバージョンです。
2	通信日時	通信を確認できた最新の日時が表示されています。 通信日時が赤字で表示されている場合は、無通信検知されています。
3	認証日時	Windows 端末を認証した日時が表示されています。

4.1.10.21 （情報－Windows）アプリケーション

対象の Windows 端末にインストールされているアプリの一覧を表示します。また、詳細画面を表示して、アプリの詳細情報を確認することもできます。

画面

画面（アプリの詳細）

◆画面

表示操作 ［機器］→［一覧］→**Windows 端末の機器名または「詳細」の** ⓘ **→詳細画面の「情報」の［アプリケーション］**

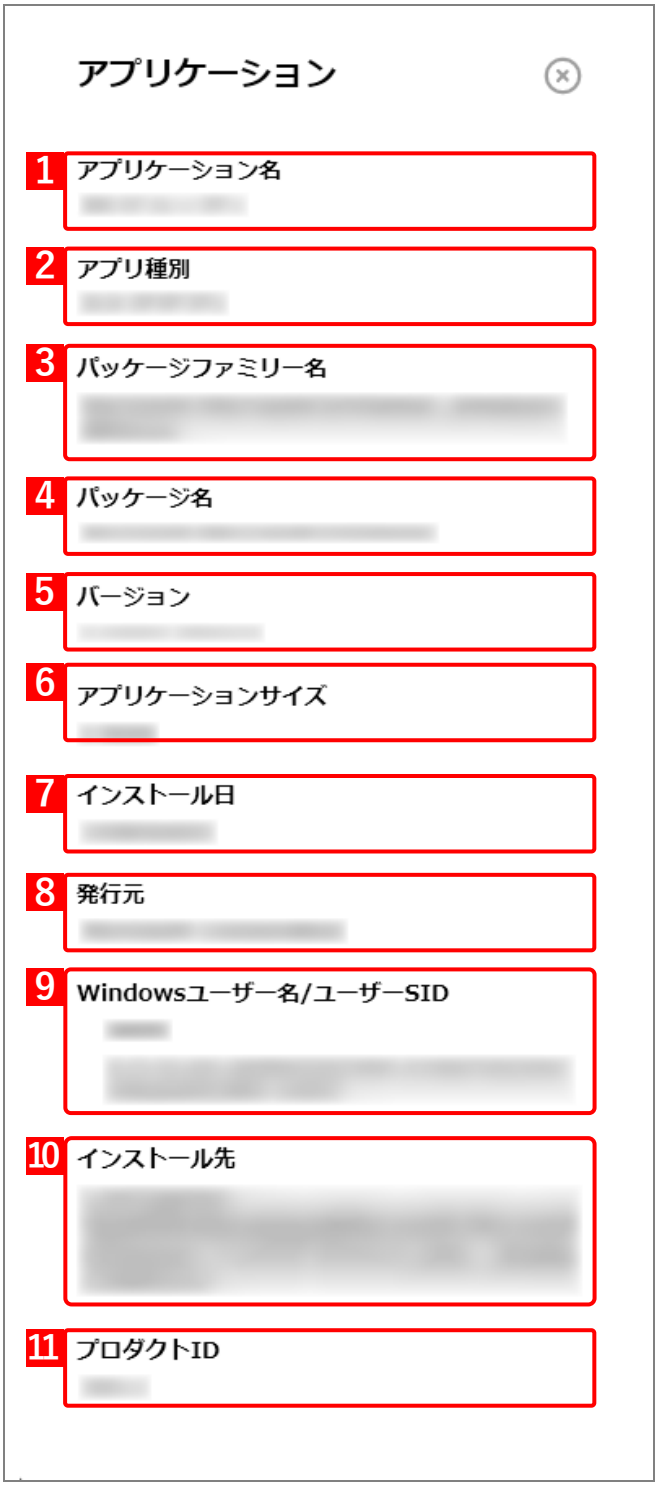
項番	項目	説明
1	［絞り込み］	項番【2】に表示する情報を以下の項目を条件にして絞り込めます。 ●「アプリケーション名」、「パッケージファミリー名」、「Windows ユーザー名」、「ユーザーSID」
2	絞り込み条件	［絞り込み］をクリックして検索した場合、その条件が表示されます。 ✖ をクリックすると、再度すべてのアプリが一覧に表示されます。
3	アプリ一覧	対象の機器にインストールされているアプリの一覧に以下の情報が表示されます。 ●「アプリケーション名」、「パッケージファミリー名」、「Windows ユーザー名」、「バージョン」、「アプリケーションサイズ」、「インストール日」

項番	項目	説明
4	（詳細）	クリックすると、アプリ一覧の右側に対象のアプリの詳細情報が表示されます。 ☞「画面（アプリの詳細）」179 ページ

◆画面（アプリの詳細）

アプリの詳細を確認できます。表示される各項目の詳細については、メーカーまたは開発・提供元へご確認ください。

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の → 詳細画面の「情報」の［アプリケーション］→一覧から対象のアプリの →**



項番	項目	説明
1	アプリケーション名	アプリ名が表示されます。
2	アプリ種別	アプリの種別が以下のどちらかで表示されます。 ●デスクトップアプリ ●ストアアプリ
3	パッケージファミリー名	アプリのパッケージファミリーが表示されます。 項番 2 の「アプリ種別」がデスクトップアプリの場合は、表示されません。
4	パッケージ名	アプリのパッケージ名が表示されます。 項番 2 の「アプリ種別」がデスクトップアプリの場合は、表示されません。
5	バージョン	アプリのバージョンが表示されます。
6	アプリケーションサイズ	アプリのファイルサイズが表示されます。
7	インストール日	アプリをインストールした日付が表示されます。
8	発行元	アプリの発行元が表示されます。
9	Windows ユーザー名/ユーザーSID	ユーザーにインストールされているアプリの Windows ユーザー名とユーザーSID が表示されます。 システムにインストールされた全ユーザー対象のアプリの場合は、表示されません。
10	インストール先	アプリのインストール先が表示されます。
11	プロダクト ID	アプリのプロダクト ID が表示されます。

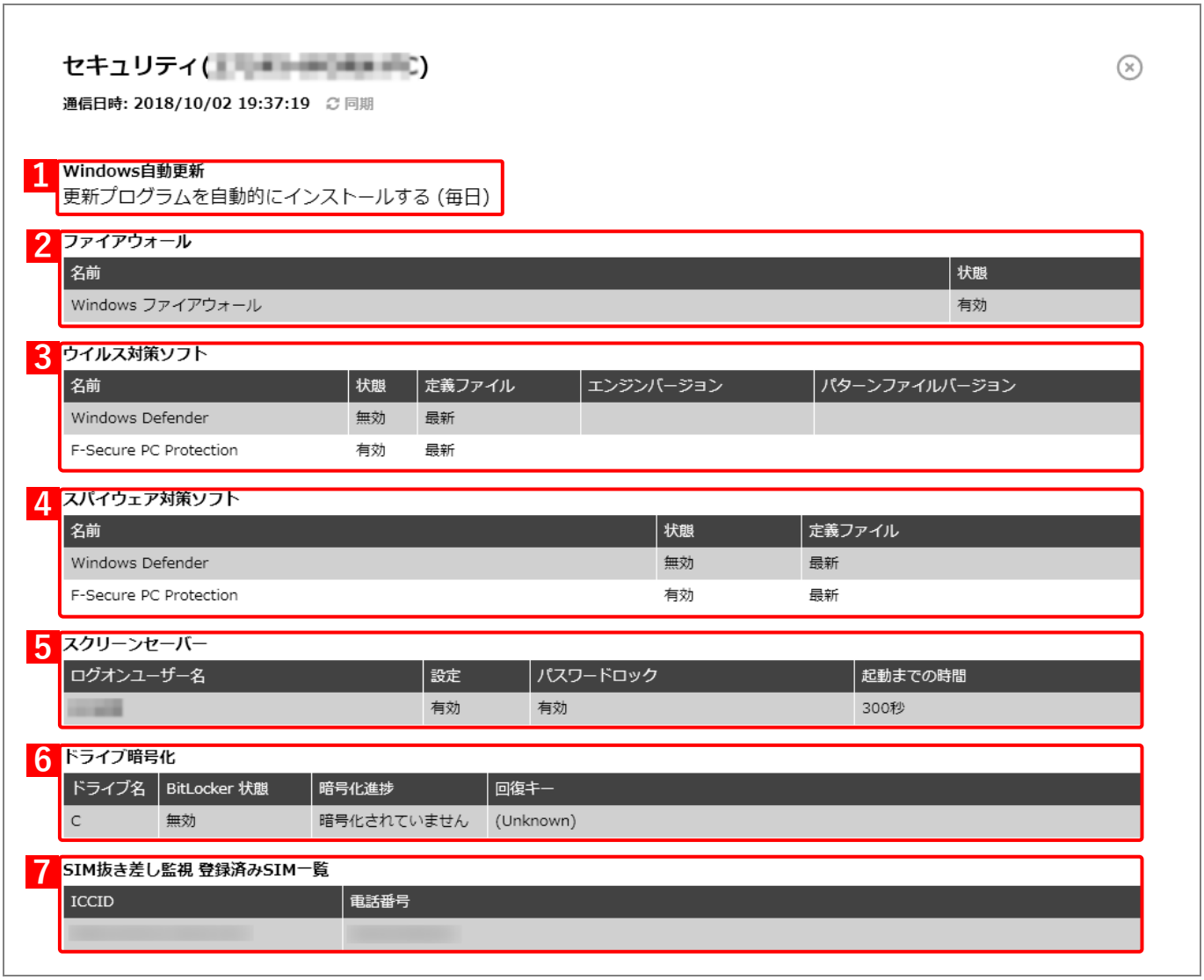
4.1.10.22 （情報－Windows）セキュリティ

更新プログラムの自動設定やファイアウォールの状態など、Windows 端末のセキュリティに関する機能の設定状態を表示します。

「セキュリティ」画面では、設定状態の確認はできますが、設定の変更はできません。

◆画面

表示操作　［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［セキュリティ］



項番	項目	説明
1	Windows 自動更新	機器に設定されている Windows 自動更新の設定値を表示します。 Windows Update と Windows Defender に対応していない場合に表示されます。詳細な対応条件については、以下を参照してください。 「Windows Update」580 ページ 「Windows Defender」582 ページ
	Windows Update	機器に設定されている Windows Update の設定値を表示します。 Windows Update に対応している場合に表示されます。詳細な対応条件については、以下を参照してください。 「Windows Update」580 ページ
	Windows Defender	機器に設定されている Windows Defender の設定値を表示します。 Windows Defender に対応している場合に表示されます。詳細な対応条件については、以下を参照してください。 「Windows Defender」582 ページ
2	ファイアウォール	機器に導入されているファイアウォールの状態を表示します。
3	ウイルス対策ソフト	機器に導入されているウイルス対策ソフトの状態を表示します。エンジンバージョンおよびパターンファイルバージョンの表示については、以下の製品のみに対応しています。 ●Windows Defender
4	スパイウェア対策ソフト	機器に導入されているスパイウェア対策ソフトの状態を表示します。
5	スクリーンセーバー	機器に設定されているスクリーンセーバーの設定値を表示します。
6	ドライブ暗号化	各ドライブの暗号化状況および回復キーを表示します。 回復キーはパスワードを忘れた場合やコンピューターの構成が変更された場合に用いるパスワードです。詳細については、Microsoft へ問い合わせてください。 ドライブ暗号化については、以下を参照してください。 「暗号化」573 ページ
7	SIM 抜き差し監視 登録済み SIM 一覧	登録済み SIM の ICCID と電話番号が表示されます。 登録済み SIM が存在しないときは、「(なし)」と表示されます。 登録済み SIM が存在するときは、表示されます。

4.1.10.23 （情報－Windows）位置

Windows 端末から送られた位置情報を表示します。

- 以下を参照し、位置情報取得の条件を確認してください。
  ☞「Windows 端末の位置情報の諸条件」184 ページ
- あらかじめ、Windows 端末に「位置情報管理」の設定セットを反映してください。
  ☞「位置情報管理」576 ページ
- ご利用の Windows 端末で位置情報の設定をオンにしてください。
  位置情報の設定方法については、Windows 端末の取扱説明書、または Microsoft の Web サイトを参照してください。
  ☞ https://privacy.microsoft.com/ja-jp/windows-10-location-and-privacy

位置情報送信を一度も行っていない端末は、［位置］メニューが表示されません。

本製品から端末の GPS を ON にすることはできません。

取得した位置情報の精度が低いと情報が破棄されるため、管理サイトに反映されません。

◆画面

表示操作　**［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［位置］**

項番	項目	説明
1	測位情報	以下の情報が表示されます。 ●受信日時 管理サイトが端末の位置情報を取得した日時が表示されます。 ●測位日時 端末が保持している位置情報を測位した日時が表示されます。 ●北緯 測位した位置の北緯が表示されます。 ●東経 測位した位置の東経が表示されます。
2	位置情報履歴	対象の端末が取得した位置情報の履歴を確認できます。 位置情報の履歴は最大 100 件まで表示されます。 例えば、「1/38」と表示されている場合は、履歴が 38 件あるうちの、最新の履歴が表示されていることを示しています。 をクリックして、履歴の表示を切り替えることができます。
3	地図	位置情報が地図で表示されます。 が表示されている位置が、地図上の端末の位置です。
4	［Google マップで表示］	クリックすると、新しいウインドウで Google マップとして表示されます。

◆Windows 端末の位置情報の諸条件

Windows 端末から位置情報を受信するための動作条件、位置情報測位契機、位置情報送信契機は以下のとおりです。内容を確認し、位置情報の受信を行ってください。

測位結果の情報は確実性を保証できる情報ではありません。

測位条件は端末の仕様に準じます。

項番	項目	条件
1	動作条件	以下の動作条件が満たされている必要があります。 ●端末が管理サイトと通信できる状態である必要があります。 ●端末の設定で位置情報の取得を許可している必要があります。
2	位置情報測位契機	以下のいずれかの契機で測位します。 ●端末の位置情報設定が OFF から ON に変更したとき ●管理サイトと同期時 ●端末を移動したときなど、OS が位置情報の測位をしたとき ●位置情報管理の「エージェントによる測位」で設定した契機 「位置情報管理」576 ページ ●他アプリが位置情報を測位したとき 同期処理自体にかかる時間は、負荷状態や通信状態に依存します。
3	位置情報送信契機	管理サイトと同期時に位置情報を送信します。 同期処理自体にかかる時間は、負荷状態や通信状態に依存します。

4.1.10.24 （情報－Windows）Zone Management

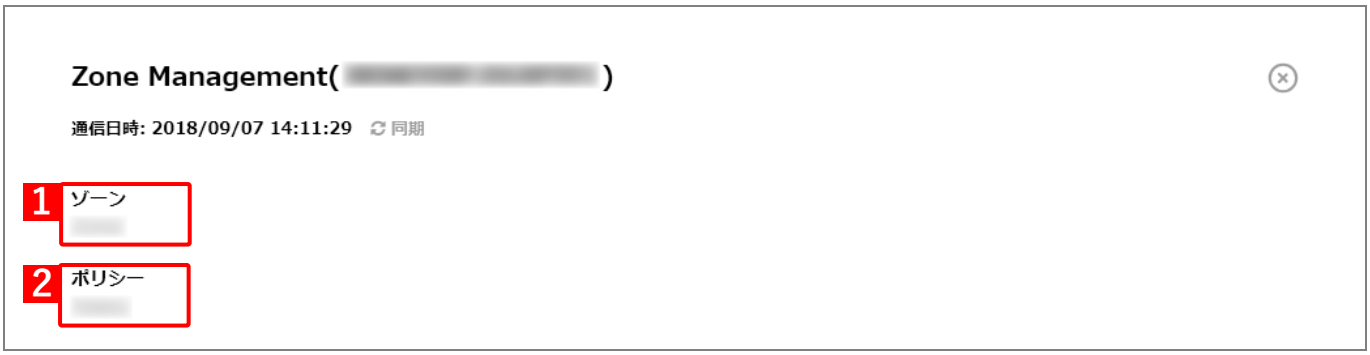
対象の Windows 端末に反映されている「ゾーンポリシー構成」の設定セットの登録内容を表示します。表示された「ゾーン」と「ポリシー」の名称から、「ゾーンポリシー構成」の内容を把握することができます。

詳細については、以下を参照してください。

☞「Zone Management」625 ページ

◆画面

表示操作［機器］→［一覧］→Windows 機器の機器名または「詳細」の ›› →詳細画面の「情報」の［他の情報を見る］→［Zone Management］



項番	項目	説明
1	ゾーン	対象の Windows 端末に適用されているゾーン名が表示されます。 表示されているゾーン名をクリックすると、該当のゾーンの設定内容を確認できます。 ☞「ゾーン」625 ページ ゾーンが適用されていない場合は、「ゾーン外」と表示されます。
2	ポリシー	対象の Windows 端末に適用されているポリシー名が表示されます。 表示されているポリシー名をクリックすると、該当のポリシーの設定内容を確認できます。 ☞「ポリシー」628 ページ ポリシーが適用されていない場合は、「機器の設定」と表示されます。

4.1.10.25 （情報－Windows）Microsoft Update 更新プログラム

対象の Windows 端末に行われた Microsoft Update の更新状態と、更新プログラムの内容を確認することができます。

◆画面

表示操作 ［機器］→［一覧］→Windows 端末の機器名または「詳細」の ⓘ →詳細画面の「情報」の［他の情報を見る］→［Microsoft Update 更新プログラム］

項番	項目	説明
1	Microsoft Update 更新プログラム	Microsoft Update 更新プログラム名が表示されます。
2	製品ファミリー	製品ファミリー名が以下のいずれかで表示されます。 ●「Windows Update」、「Office Update」、「その他」
3	状態	アップデートの状態が以下のいずれかで表示されます。 ●「適用済み」、「未適用」、「失敗」

4.2 ネットワークマップ

各端末の IP アドレスを表示して、どのネットワークの配下で利用しているかをマップ上で確認することができます。

4.2.1 ネットワークマップの見かた

ネットワークマップでは、ネットワーク別に端末のアイコン（機器アイコン）をマップ上に表示しており、目的の端末がどのネットワークに属しているかを確認することができます。

また、機器アイコンをクリックすると、端末の詳細情報を表示することができます。

その他のマップ上の各要素の詳細については、以下を参照してください。

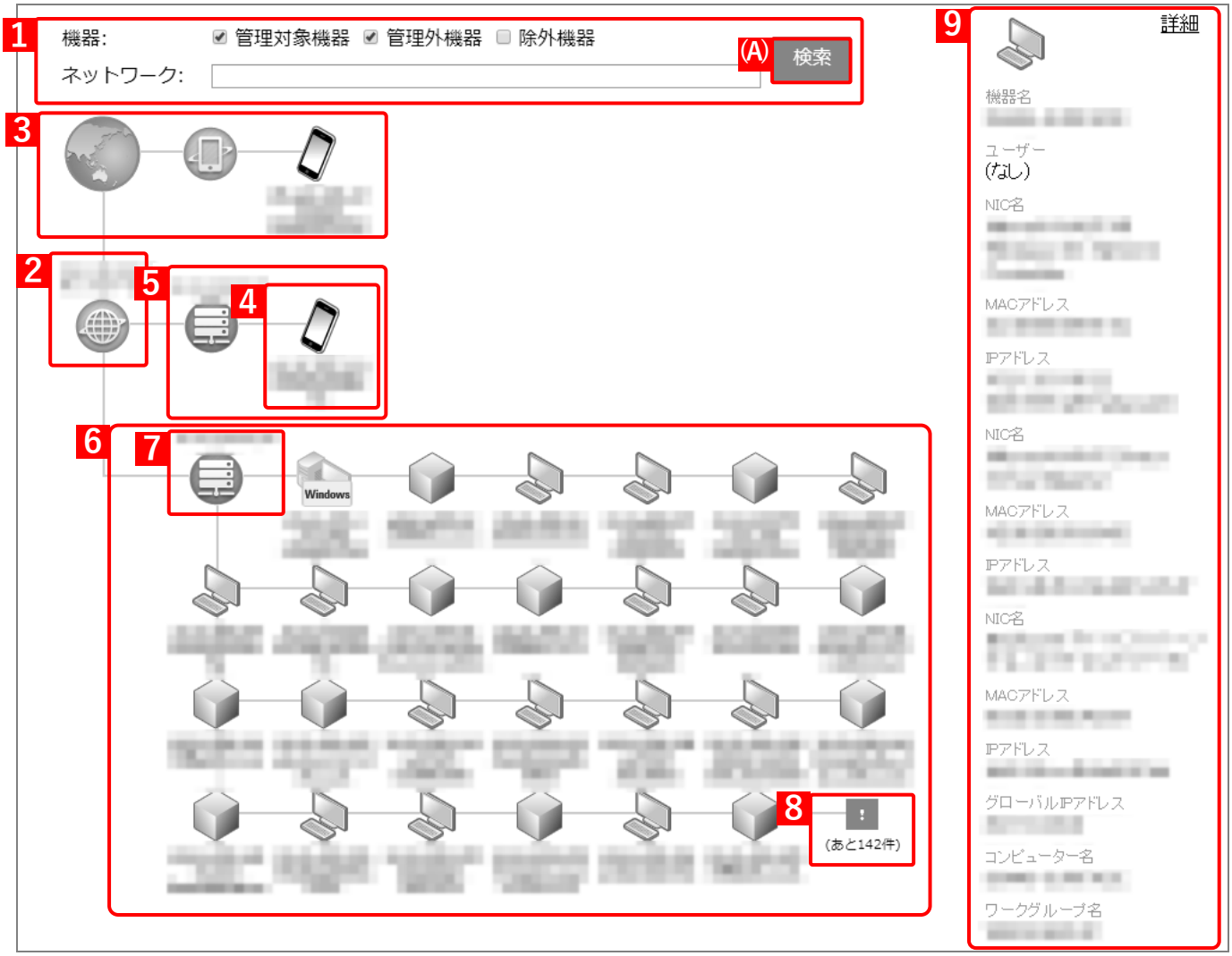
「機器アイコン一覧」191 ページ

USB 無線 LAN アダプターを使用してネットワークに接続している Windows 端末は、検出されない場合があります。

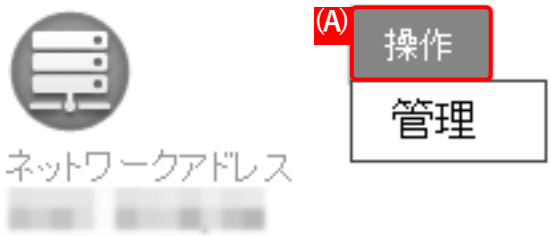
USB LAN アダプターや、仮想ネットワークアダプターを使用してネットワークに接続している場合、機器が正しく検出されない場合があります。

◆画面

表示操作　［機器］→［ネットワークマップ］



項番	名称	説明
1	検索機能	検索機能を利用し、表示するネットワークマップを絞り込めます。機器の種類を選択、または、ネットワーク名を入力し、(A)［検索］をクリックします。どちらか片方だけの入力でも検索できます。再度すべてのネットワークを表示するにはブラウザーを再読み込み、または機器、ネットワーク名入力欄を空欄にし、(A)［検索］をクリックします。 管理対象機器、管理外機器、除外機器の説明については、以下を参照してください。 「機器の種類」190 ページ
2	グローバルネットワークアイコン	グローバルネットワークの IP アドレスとネットワーク名が表示されます。クリックすると詳細情報が【9】に表示されます。 ネットワーク名は設定した場合のみ表示されます。ネットワーク名の設定方法は、以下を参照してください。 「ネットワーク」653 ページ
3	モバイルネットワーク	以下の端末が表示されます。 ・3G、4G/LTE、5G、Wi-Fi 接続されている Android 端末 ・3G、4G/LTE、5G、Wi-Fi 接続されている iOS 端末 ・3G、4G/LTE、5G、Wi-Fi および有線で接続されている Windows 端末 iOS 端末は Wi-Fi 接続の場合でも、3G、4G/LTE、5G 接続ができる端末であればモバイルネットワークに表示されます。
4	機器アイコン	機器アイコンをクリックすると詳細情報が【9】に表示されます。
5	iOS ローカルネットワーク	3G、4G/LTE、5G 接続ができない iOS は、ローカルネットワーク（IP アドレスなし）に表示されます。
6	ローカルエリアネットワーク	ローカルエリアネットワークに接続されている機器が表示されます。
7	ローカルエリアネットワークアイコン	ローカルエリアネットワークの IP アドレスとネットワーク名が表示されます。クリックすると詳細情報が【9】に表示されます。ネットワーク名は設定した場合のみ表示されます。ネットワーク名の設定方法は、以下を参照してください。 「ネットワーク」653 ページ
8	［さらに読み込む］	機器は 4 行表示されています。4 行以上ある場合は、［さらに読み込む］をクリックすると、表示行数が倍になります。

項番	名称	説明
9	詳細情報	マップ上でクリックされた機器やネットワークの詳細情報が表示されます。表示される情報は機器やネットワークによって異なります。［詳細］をクリックすると、機器やネットワークの詳細画面が表示されます。 ●機器の場合 ［詳細］をクリックすると、機器画面が表示され、機器情報の編集や設定の変更などを行えます。機器画面の詳細については、以下を参照してください。 ☞「機器の詳細画面」59 ページ ●管理外機器の場合 (A)［操作］が表示されます。管理外機器を管理対象機器に設定する場合は、以下を参照してください。 ☞「管理外機器を管理対象機器に設定」194 ページ ●ネットワークの場合 ・詳細 ［詳細］をクリックすると、ネットワーク画面が表示され、ネットワーク名などの変更を行えます。ネットワーク画面でまだ登録を行っていないネットワークの場合は（A）［操作］が表示されます。［管理］をクリックし、［管理］を選択すると、ネットワーク画面が表示されます。ネットワーク画面の詳細については、以下を参照してください。 ☞「ネットワーク」653 ページ 

4.2.1.1 機器の種類

管理サーバーで管理される端末の種類とその状態を説明します。

機器の種類	説明
ライセンス認証済み機器	機器にエージェントがインストールされており、ライセンス認証済みの機器。
ライセンス認証待ち機器	これからライセンス認証を行う予定がある機器で、機器検出機能により検出され、ライセンス認証待ち機器と登録されたもの。 管理外機器をライセンス認証待ち機器へ登録する方法については、以下を参照してください。 「管理外機器を管理対象機器に設定」194 ページ
ライセンス認証対象機器	「ライセンス認証済み機器」と「ライセンス認証待ち機器」の総称。
資産管理対象機器	機器検出機能により検出された機器のうち、資産管理対象機器と登録されたもの。ラベリングのみができます。 管理外機器を資産管理対象機器へ変更する方法については、以下を参照してください。 「管理外機器を管理対象機器に設定」194 ページ
管理対象機器	「ライセンス認証対象機器」と「資産管理対象機器」の総称。
管理外機器	機器検出機能により検出された、マップ上表示のみができる機器。 ・マップに表示されただけで、機器ライセンスを使用することはありません。管理対象機器へ変更すると機器ライセンスが使用されます。 管理外機器を管理対象機器へ変更する方法については、以下を参照してください。 「管理外機器を管理対象機器に設定」194 ページ 管理外機器を除外機器へ変更する方法については、以下を参照してください。 「管理外機器を除外機器に設定」196 ページ 1 企業あたりの管理外機器の上限は 10,000 までです。上限を超えて検出された場合は、最終検出日時が新しい管理外機器を優先してマップに表示します。 管理外機器は機器レポートに表示されません。機器レポートについては以下を参照してください。 「機器レポート」237 ページ 管理外機器は無通信検知の対象外です。無通信検知については、以下を参照してください。 「通知設定」633 ページ
除外機器	管理外機器をマップ上非表示の指定とした機器。 除外機器を管理外機器に戻す方法については、以下を参照してください。 「除外機器を管理外機器に設定」197 ページ

4.2.1.2 機器アイコン一覧

管理サイトのネットワークマップに表示される各種の機器アイコンについて説明します。

◆Android 端末

アイコン	端末	アイコン	端末
	GALAXY Tab		スマートグラス
	FOLIO 100		その他
	LifeTouch		

◆iOS 端末

アイコン	端末	アイコン	端末
	iPhone		その他
	iPad		

◆Windows 端末

アイコン	端末	アイコン	端末
	タブレット		ノート PC
	デスクトップ PC		その他

◆Mac OS 端末

アイコン	端末
	Mac

◆資産管理限定機器（AV 系）

アイコン	端末	アイコン	端末
	ネット TV 端末		オーディオ
	レコーダー		プレイヤー
	STB		プロジェクター
	AV アンプ		フォトフレーム
	デジタルカメラ		AV 系その他
	デジタルビデオカメラ		

◆資産管理限定機器（PC 系）

アイコン	端末	アイコン	端末
	デスクトップ		プリンター
	ノート PC		タブレット
	ストレージ		スマートフォン
	PDA		PC 系その他

◆資産管理限定機器（娯楽系）

アイコン	端末	アイコン	端末
	据置ゲーム機		家庭用ロボット
	ポータブルゲーム機		娯楽系その他

◆資産管理限定機器（通信系）

アイコン	端末	アイコン	端末
	携帯電話		PLC モデム
	IP 電話		無線 LAN モデム
	ルーター		同軸ケーブルモデム
	FAX		通信系その他
	スイッチングハブ		

◆資産管理限定機器（くらし系）

アイコン	端末
	くらし系その他

くらし系は、資産管理限定機器を新規作成し、種別で以下の項目を選んだ場合に表示されるアイコンです。
エアコン、冷蔵庫、洗濯機、照明、電子レンジ、Web カメラ、ゲートウェイ、ドアホン、センサー、換気扇、ブラインド、シャッター、雨戸、散水器、給湯器、便座、電気錠、太陽光発電、床暖房、ポット、IH 調理器、炊飯器、掃除機、くらし系その他

「画面（新規作成：「資産管理対象機器」を選択した場合）」65 ページ

◆資産管理限定機器（その他）

アイコン	端末
	その他

4.2.2 管理外機器を管理対象機器に設定

管理対象外機器を管理対象機器に設定します。

機器の種類については、以下を参照してください。

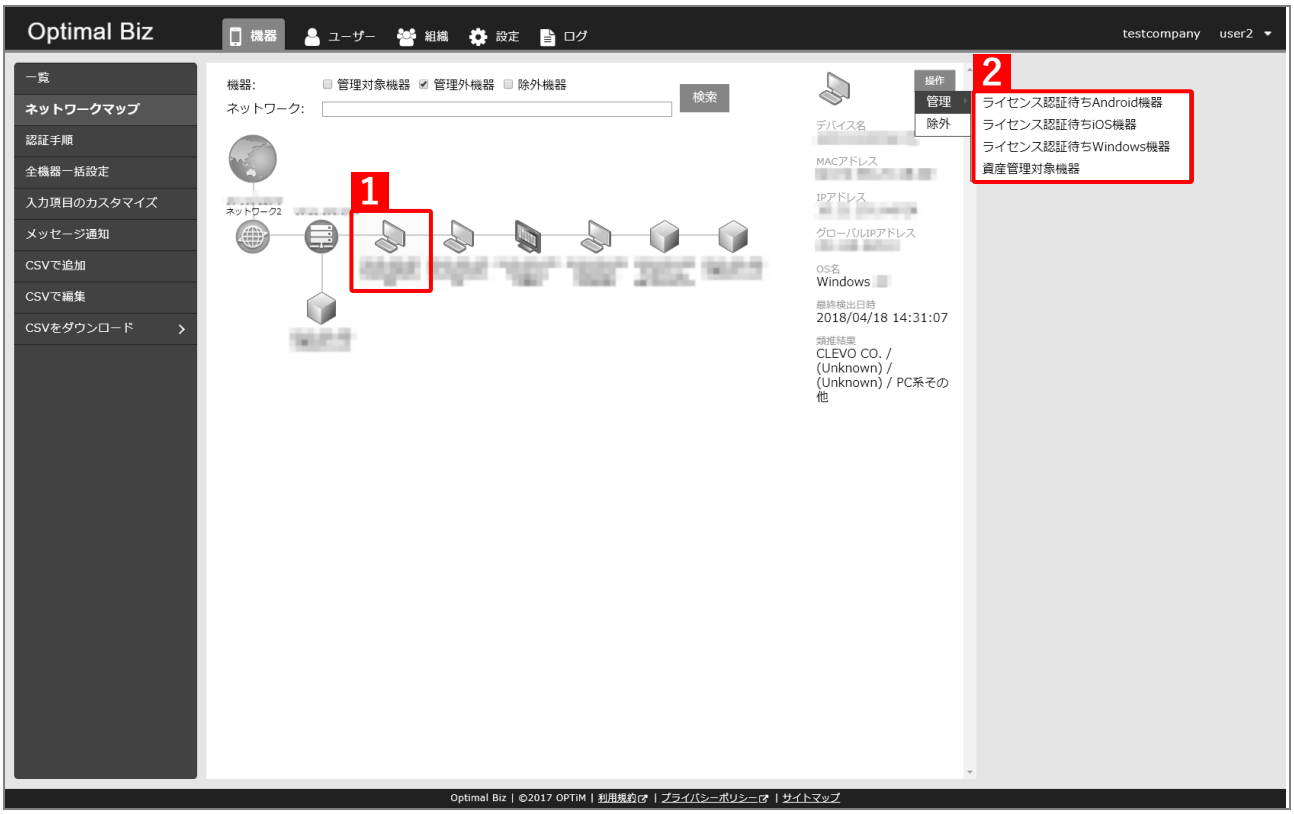
☞「機器の種類」190 ページ

【1】［機器］→［ネットワークマップ］→管理外機器をクリックします。

管理外機器が表示されていない場合は、検索機能で「管理外機器」にチェックを入れて、［検索］をクリックしてください。

【2】詳細情報の［操作］→［管理］→［ライセンス認証待ち XXXX 機器］または「資産管理対象機器」を選択します。

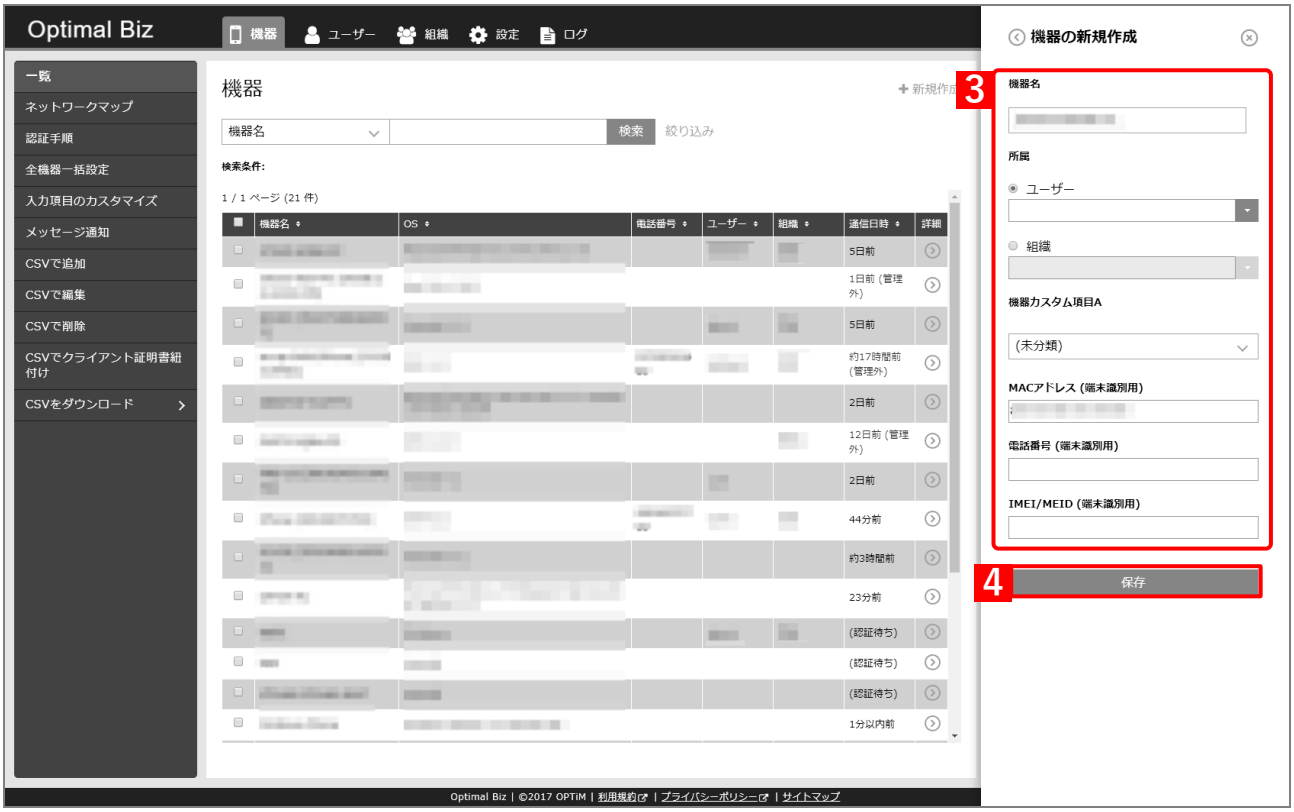
⇒機器の新規作成画面が表示されます。



【3】機器情報を入力します。

【4】［保存］をクリックします。

⇒対象の機器が管理対象機器に変更されます。



4.2.3 管理外機器を除外機器に設定

管理対象外機器を管理対象機器に設定します。

機器の種類については、以下を参照してください。

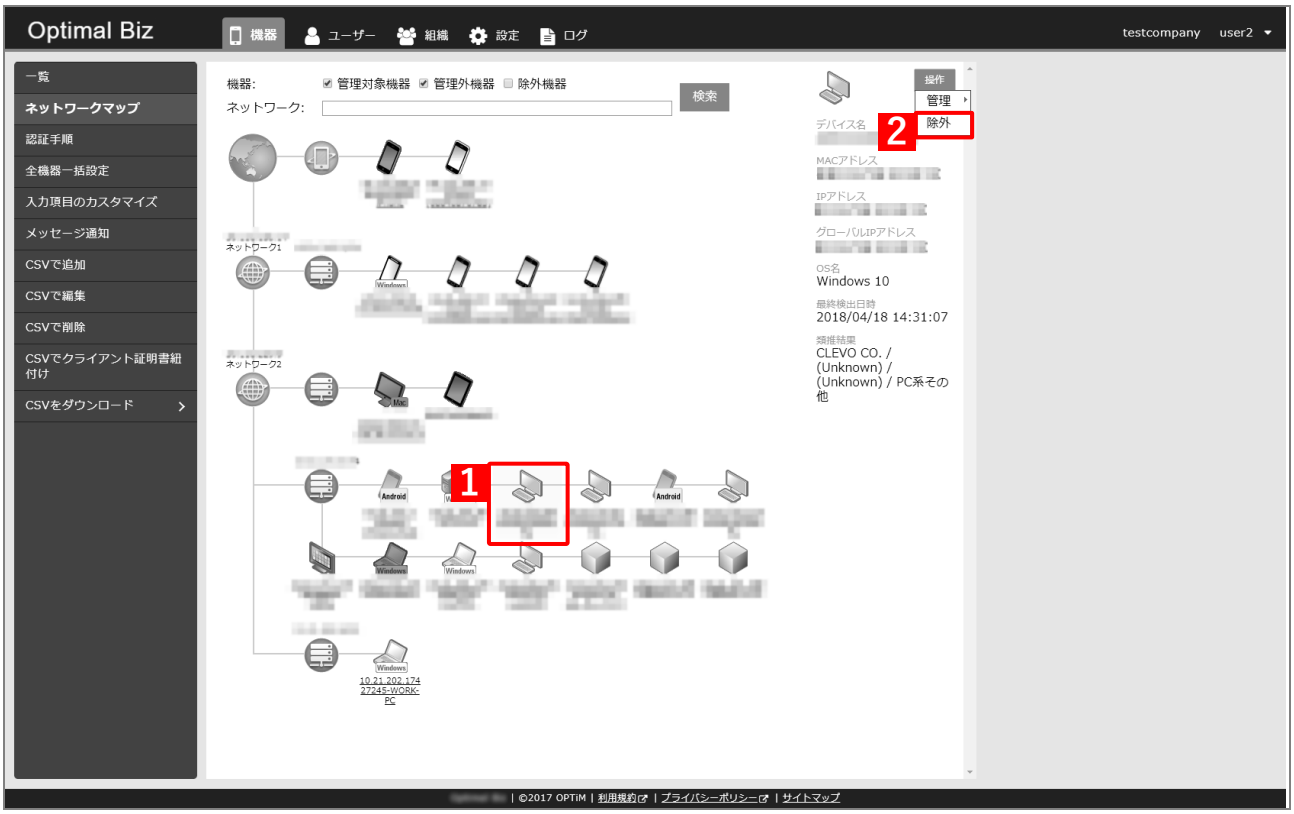
☞「機器の種類」190 ページ

【1】［機器］→［ネットワークマップ］→管理外機器をクリックします。

管理外機器が表示されていない場合は、検索機能で「管理外機器」にチェックを入れて、［検索］をクリックしてください。

【2】詳細情報の［操作］→［除外］を選択します。

⇒対象の機器が除外機器に変更されます。



4.2.4 除外機器を管理外機器に設定

除外機器を管理外機器に設定します。

機器の種類については、以下を参照してください。

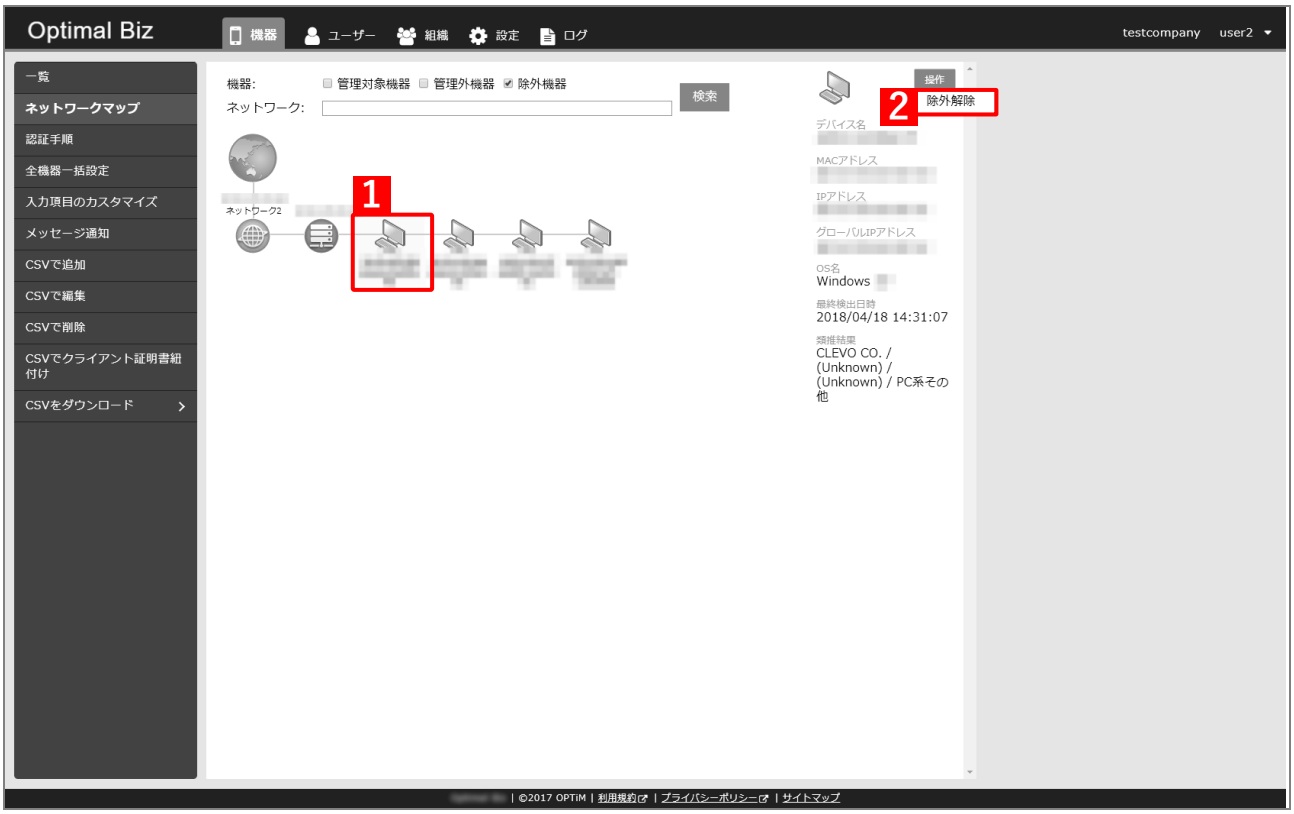
「機器の種類」190 ページ

【1】［機器］→［ネットワークマップ］→除外機器を選択します。

除外機器が表示されていない場合は、検索機能で「除外機器」にチェックを入れて、［検索］をクリックしてください。

【2】詳細情報の［操作］→［除外解除］をクリックします。

⇒対象の機器が、対象外機器に変更されます。

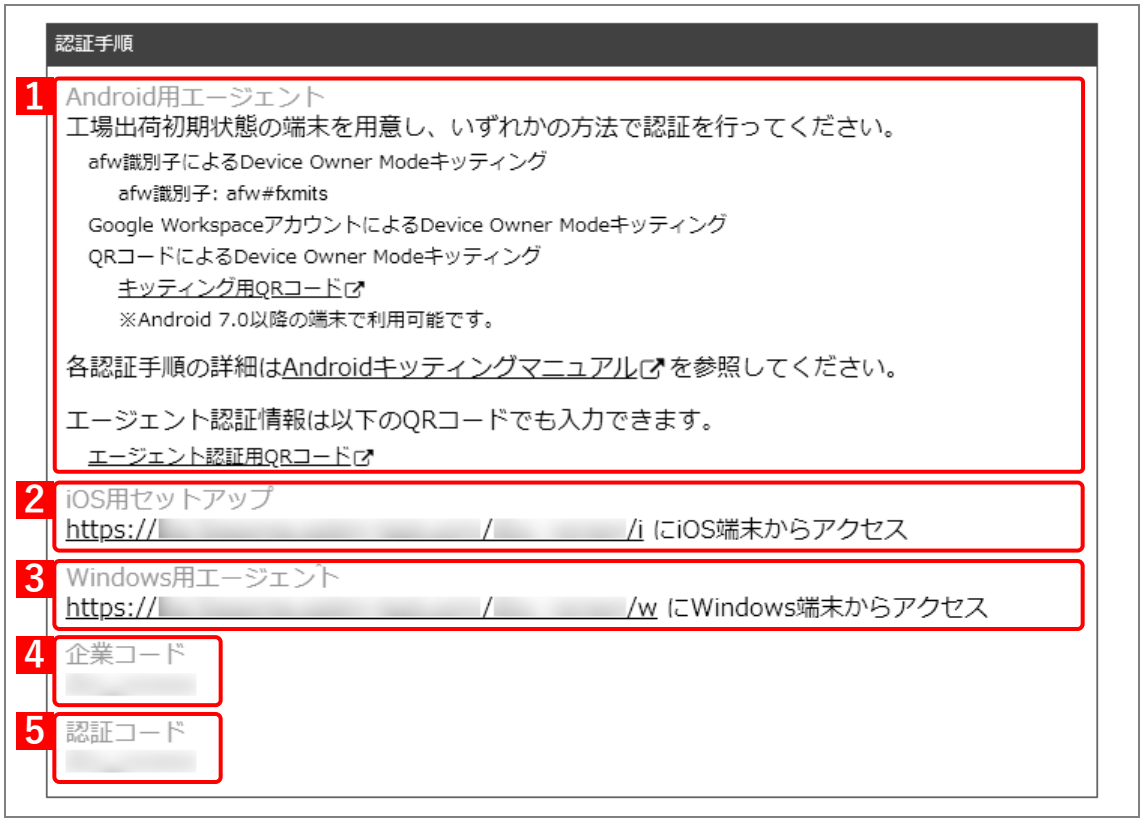


4.3 認証手順

各 OS のエージェントアプリのダウンロード先や、企業コード、認証コードを確認することができます。

◆画面

表示操作［機器］→［認証手順］



項番	項目	説明
1	Android 用エージェント	Android エージェントの認証方法が表示されます。 各認証手順の詳細については、以下を参照してください。 『Android キッティングマニュアル』 以下のいずれかの方法で認証を行ってください。 ●afw 識別子による Device Owner Mode キッティング afw 識別子は「afw#fxmits」です。 ●Google Workspace アカウントによる Device Owner Mode キッティング ●QR コードによる Device Owner Mode キッティング ［キッティング用 QR コード］をクリックし、表示された QR コードを読み込むことで、Device Owner Mode キッティングを行えます。 Android 7.0 以上の端末で利用できます。
2	iOS 用セットアップ	iOS エージェントのライセンス認証先の URL が表示されます。iOS 端末でライセンス認証先の URL を表示して、エージェントのライセンス認証をします。iOS 端末の操作については、以下を参照してください。 『iOS キッティングマニュアル』
3	Windows 用エージェント	Windows エージェントのダウンロード先の URL が表示されます。Windows 端末でダウンロード先の URL を表示して、エージェントをダウンロードします。Windows 端末の操作については、以下を参照してください。 『Windows キッティングマニュアル』

項番	項目	説明
4	企業コード	企業コードが表示されます。各エージェントの認証操作で使用するコードです。
5	認証コード	認証コードが表示されます。各エージェントの認証操作で使用するコードです。

4.4 全機器一括設定

OS ごとに設定した各機能の設定セットを、対象の機器に一括で反映することができます。

また、各種のリモート操作を、対象の機器に一括で行うこともできます。

◆画面

表示操作［機器］→［全機器一括設定］

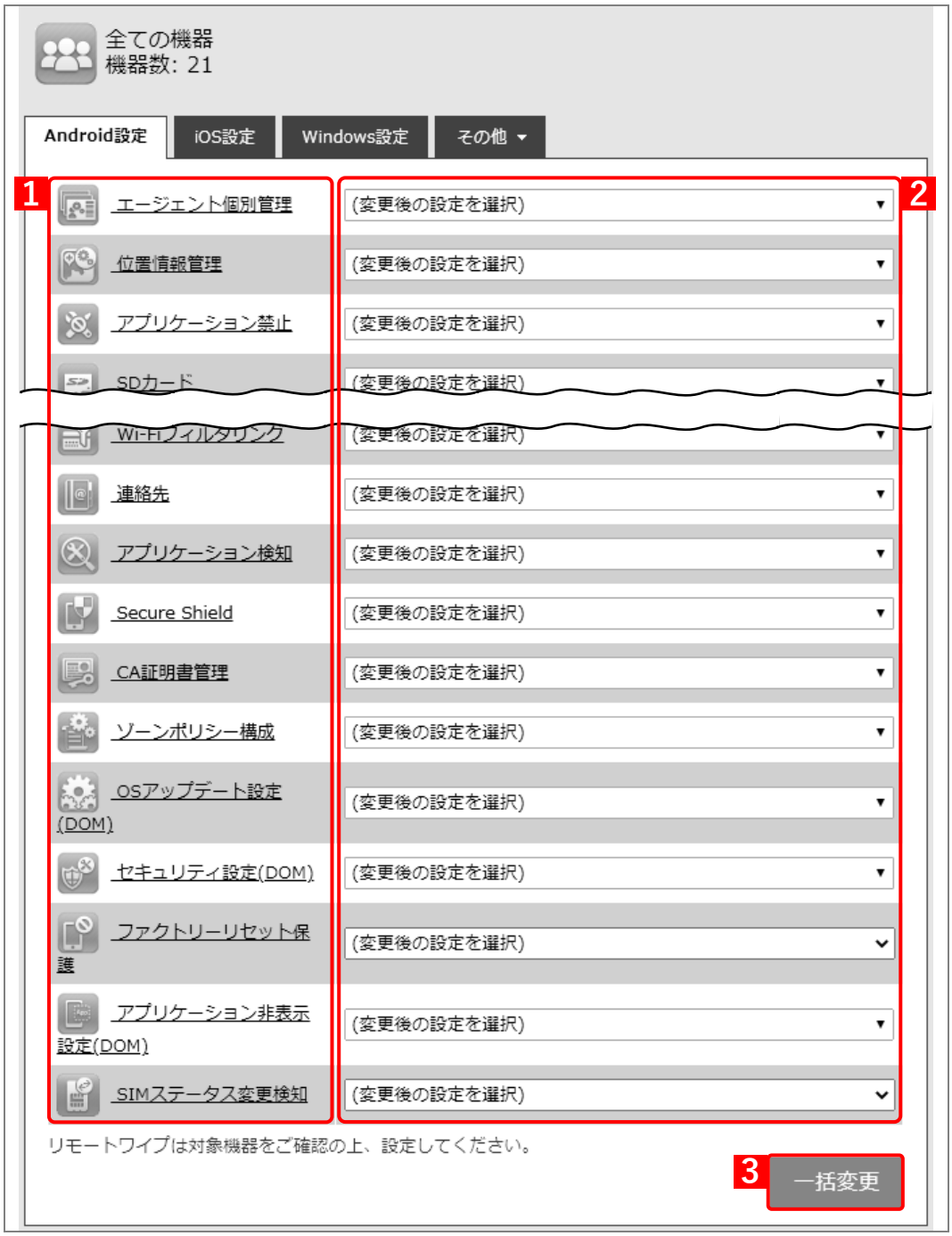
項番	項目	説明
1	対象機器条件	クリックすると、対象となるすべての機器に、設定セットを反映します。 ［機器］や［ユーザー］の［入力項目のカスタマイズ］で項目を追加していない場合は、この条件のみ表示されます。
2	対象機器条件（機器）	［機器］の［入力項目のカスタマイズ］で、［分類］タブの項目を追加した場合に表示されます。 リストメニューから条件を選択すると、対象となるすべての機器に設定セットを反映します。 ［入力項目のカスタマイズ］の［分類］タブの詳細については、以下を参照してください。 「［分類］タブ」219 ページ

項番	項目	説明
3	対象機器条件（ユーザー）	［ユーザー］の［入力項目のカスタマイズ］で、［分類］タブの項目を追加した場合に表示されます。 リストメニューから条件を選択すると、対象となるすべての機器に設定セットを反映します。 ユーザーの対象機器条件を表示するには、ユーザーと機器を紐づけする必要があります。ユーザーと機器の紐づけの詳細については、以下を参照してください。 「機器の新規作成」61 ページ ［入力項目のカスタマイズ］の［分類］タブの詳細については、以下を参照してください。 「［分類］タブ」272 ページ
4	対象機器	項番 1、2、3 で選択した機器の条件と数が表示されます。
5	OS タブ	各 OS に適用する設定セットの選択や、リモート操作の内容を設定します。

4.4.1 ［Android 設定］タブ

◆画面

表示操作　**［機器］→［全機器一括設定］→［Android 設定］タブ**



項番	項目	説明
1	機能名	各機能名が表示されます。アイコンまたは機能名のリンクをクリックすると、該当の設定に切り替わります。
2	（変更後の設定を選択）	適用する設定セット名をリストボックスから以下のいずれかを選択します。 ● ［(変更後の設定を選択)］ 設定は変更されません。 ● ［(設定なし)］ 設定なしが適用されます。 ● ［各機能の設定名］ 各機能で作成した設定が適用されます。 ［(設定なし)］または［各機能の設定名］を選択して、項番 3［一括変更］を実行したあとは、初期値の［(変更後の設定を選択)］に戻ります。
3	［一括変更］	項番 2 の「(変更後の設定を選択)」で選択した設定セットを、一括で Android 端末に適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 機器に反映されるまでの時間は、サーバーや機器の通信状態に依存するため、お急ぎの場合は、機器ごとに設定をし、同期を行ってください。 「(設定－Android）設定の割り当て」75 ページ 「機器との同期」70 ページ

4.4.2 ［iOS 設定］タブ

◆画面

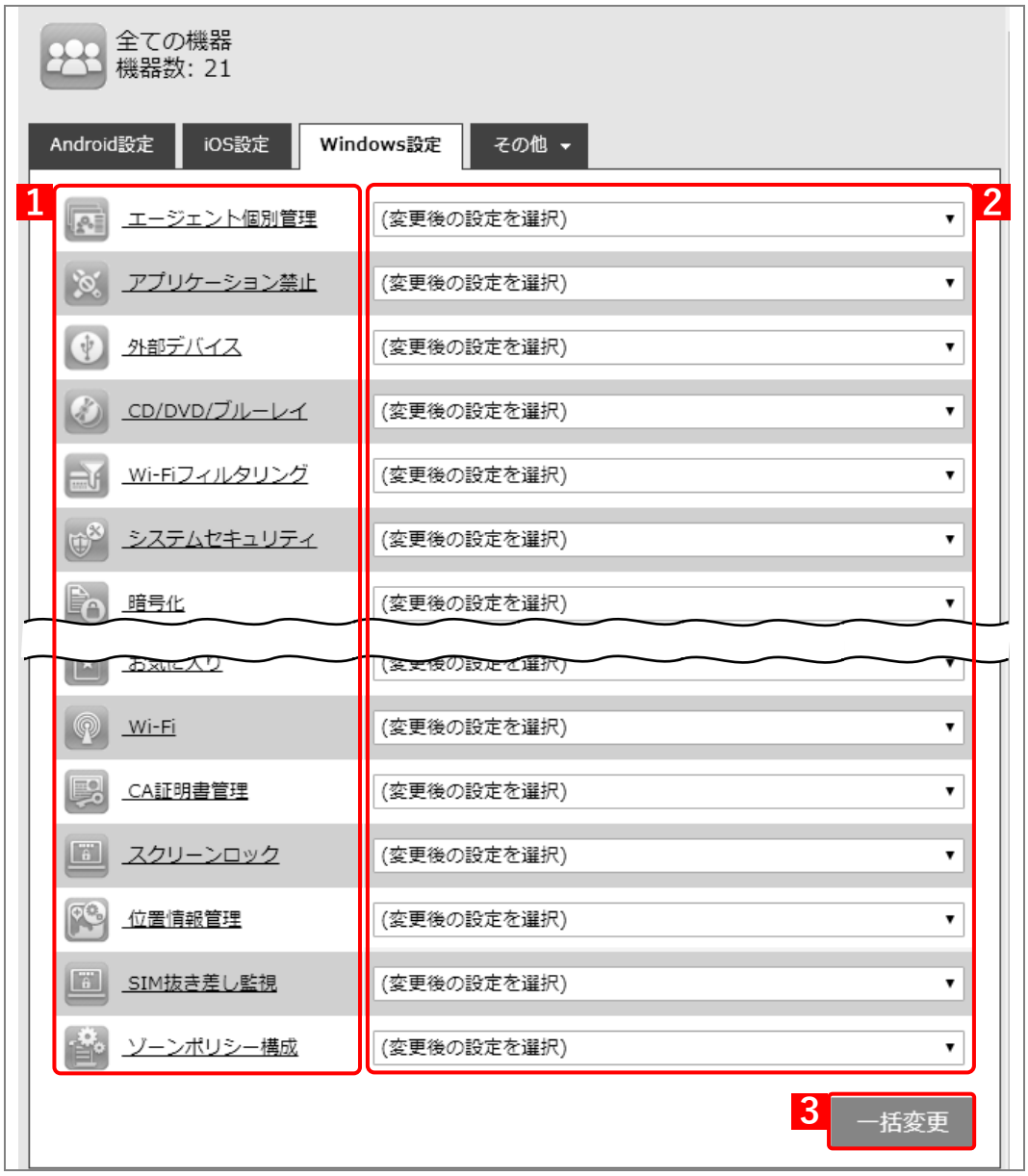
表示操作　［機器］→［全機器一括設定］→［iOS 設定］タブ

項番	項目	説明
1	機能名	各機能名が表示されます。アイコンまたは機能名のリンクをクリックすると、該当の設定に切り替わります。
2	(変更後の設定を選択)	適用する設定セット名をリストボックスから以下のいずれかを選択します。 ● ［(変更後の設定を選択)］ 設定は変更されません。 ● ［(設定なし)］ 設定なしが適用されます。 ● ［各機能の設定名］ 各機能で作成した設定が適用されます。 ［(設定なし)］または［各機能の設定名］を選択して、項番 3［一括変更］を実行したあとは、初期値の［(変更後の設定を選択)］に戻ります。
3	［一括変更］	項番 2 の「(変更後の設定を選択)」で選択した設定セットを、一括で iOS 端末に適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 機器に反映されるまでの時間は、サーバーや機器の通信状態に依存するため、お急ぎの場合は、機器ごとに設定をし、同期を行ってください。 ☞「(設定－iOS) 設定の割り当て」83 ページ ☞「機器との同期」70 ページ

4.4.3 ［Windows 設定］タブ

◆画面

表示操作　［機器］→［全機器一括設定］→［Windows 設定］タブ



項番	項目	説明
1	機能名	各機能名が表示されます。アイコンまたは機能名のリンクをクリックすると、該当の設定に切り替わります。
2	（変更後の設定を選択）	適用する設定セット名をリストボックスから以下のいずれかを選択します。 ●［(変更後の設定を選択)］ 設定は変更されません。 ●［(設定なし)］ 設定なしが適用されます。 ●［各機能の設定名］ 各機能で作成した設定が適用されます。 ［(設定なし)］または［各機能の設定名］を選択して、項番 3［一括変更］を実行したあとは、初期値の［(変更後の設定を選択)］に戻ります。
3	［一括変更］	項番 2 の「(変更後の設定を選択)」で選択した設定セットを、一括で Windows 端末に適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 機器に反映されるまでの時間は、サーバーや機器の通信状態に依存するため、お急ぎの場合は、機器ごとに設定をし、同期を行ってください。 「(設定－Windows）設定セットの割り当て」103 ページ 「機器との同期」70 ページ

4.4.4 ［その他▼］タブ／Android リモート操作

すべての Android 端末に、以下のリモート操作を行うことができます。

●リモートロック

●ロック解除

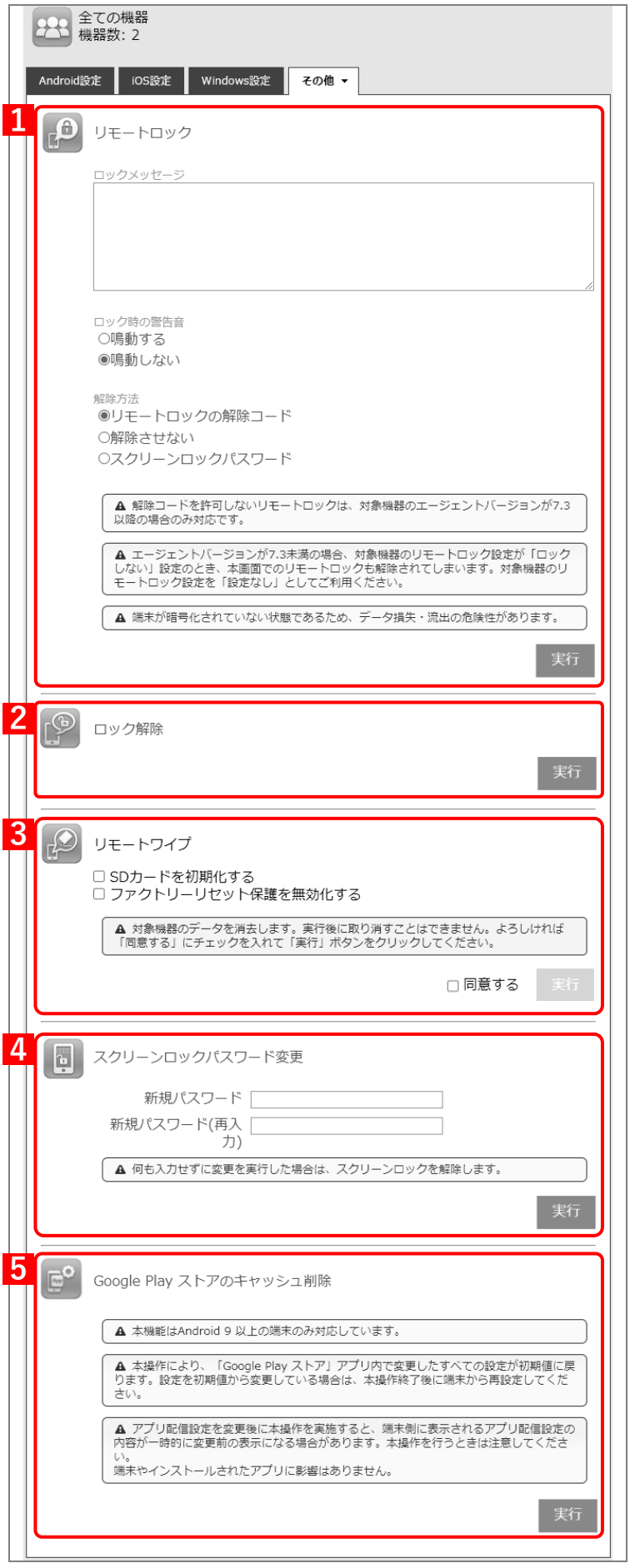
●リモートワイプ

●スクリーンロックパスワード変更

●Google Play ストアのキャッシュ削除

◆画面

表示操作［機器］→［全機器一括設定］→［その他▼］→［Android リモート操作］



項番	項目	説明
1	リモートロック	以下の項目を設定して［実行］をクリックすると、Android 端末に一括でリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●ロックメッセージ リモートロックがかかったときに、端末に表示するメッセージを 200 文字以内で入力します。 解除方法で「スクリーンロックパスワード」を選択した場合は、入力したメッセージの文字数にかかわらず、端末に表示されるのは、最大全角 18 文字までです。 ●ロック時の警告音 リモートロックした端末から警告音を鳴らすかどうかを以下から選択します。 警告音は、端末で設定している通知音を利用します。音量は、最大です。 本機能は Android 4.0 以上に対応しています。 ・鳴動する リモートロックした端末を鳴動させます。リモートロック画面が表示されている間は鳴動が続きます。 イヤホン利用時の動作は機種によって異なります。 ハードウェアスイッチによりサイレントモードになっている端末は鳴動しませんのでご注意ください。 ・鳴動しない リモートロックした端末を鳴動させません。 ●解除方法 解除コードによるロック解除を許可するかどうかを以下から選択します。 エージェントバージョン 7.3 未満の場合、対象機器のリモートロック設定が「ロックしない」設定のとき、本画面でのリモートロックも解除されてしまいます。対象機器のリモートロック設定を「設定なし」として利用してください。 ・リモートロックの解除コード 本製品独自のロック画面を表示してロックします。「リモートロックの解除コード」を端末から入力する、もしくは管理サイトからリモートロック解除を行うことでロック画面を解除できます。 ・解除させない 本製品独自のロック画面を表示してロックします。管理サイトからリモートロック解除を行うことでロック画面を解除できます。 「解除させない」の設定は、対象機器のエージェントバージョン 7.3 以上に対応しています。 ・スクリーンロックパスワード Android OS 標準のスクリーンロック画面が表示されます。管理サイトからリモートロック解除を行うことはできず、利用者が事前に設定したスクリーンロックパスワードによって解除できます。 パスワードがかかっていない場合は第三者が自由にデータへアクセスできてしまうため、パスワードポリシー設定を行っていない環境では、必ず「リモートロックの解除コード」または「解除させない」を選択してください。 ロックメッセージは、端末に表示されるのは、最大全角 18 文字までです。 端末の通知の設定が「すべての通知内容を表示する」になっていない場合は、メッセージは表示されません。 「スクリーンロックパスワード」の設定項目は、対象の端末が Android 6.0 以上で、エージェントバージョン 9.3 以上の場合に表示されます。
2	ロック解除	［実行］をクリックすると、Android 端末のリモートロックを一括で解除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

項番	項目	説明
3	リモートワイプ	以下の項目にチェックを入れて［実行］をクリックすると、Android 端末に一括でリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●SD カードを初期化する 端末に挿入されている SD カードも一緒に初期化する場合は、チェックを入れます。 ●ファクトリーリセット保護を無効化する ファクトリーリセット保護を無効化したい場合は、チェックを入れます。 ファクトリーリセット保護とは、Android 端末を初期化したとき、Google アカウントの認証が必要になることで、キッティングが完了できないようにする機能です。Android 端末の盗難防止になります。 ●同意する リモートワイプを実行する場合は、必ずチェックを入れます。 端末のデータ消去が開始されると、途中で中止できません。
4	スクリーンロックパスワード変更	以下の項目を設定して［実行］をクリックすると、Android 端末に一括でスクリーンロックパスワード変更の内容を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●新規パスワード 新しいパスワードを 16 文字以内の半角英数字、記号で入力します。 ●新規パスワード(再入力) 「新規パスワード」で入力したパスワードと同じパスワードを入力します。 「新規パスワード」と「新規パスワード(再入力)」に何も入力しないでパスワードの変更を行った場合は、スクリーンロックが解除されます。 端末にパスワードの変更が適用されると、その旨のメッセージが表示されます。
5	Google Play ストアのキャッシュ削除	Android 端末の Google Play ストアのキャッシュを削除します。 エージェントバージョン 9.14.1 以上かつ Android 9 以上の端末が対象です。 本操作により、「Google Play ストア」アプリ内で変更したすべての設定が初期値に戻ります。設定を初期値から変更している場合は、本操作終了後に端末から再設定してください。「アプリの自動更新」を［アプリを自動更新しない］に設定している場合や、企業で Wi-Fi の使用を制限している場合は、初期値の［Wi-Fi 接続時のみ］に設定されるため、特に注意してください。 アプリ配信設定を変更後に本操作を実施すると、端末側に表示されるアプリ配信設定の内容が一時的に変更前の表示になる場合があります。本操作を行うときは、注意してください。端末やインストールされたアプリに影響はありません。

4.4.5 ［その他▼］タブ／iOS リモート操作

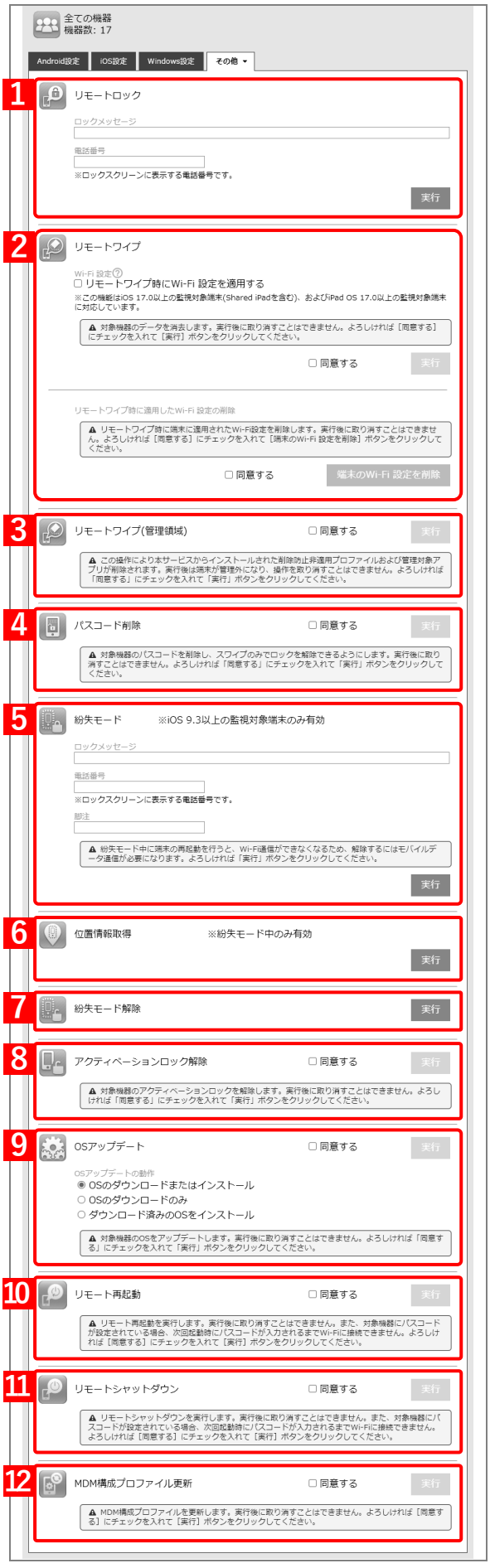
すべての iOS 端末に、以下のリモート操作を行うことができます。

- リモートロック
- リモートワイプ
- リモートワイプ（管理領域）
- パスコード削除
- 紛失モード
- 位置情報取得
- 紛失モード解除
- アクティベーションロック解除
- OS アップデート
- リモート再起動
- リモートシャットダウン
- MDM 構成プロファイル更新

「紛失モード」を設定すると、エージェント認証をしていない端末でも、端末の場所を特定できます。

◆画面

表示操作［機器］→［全機器一括設定］→［その他▼］→［iOS リモート操作］



項番	項目	説明
1	リモートロック	以下の項目を設定して［実行］をクリックすると、iOS 端末に一括でリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●ロックメッセージ リモートロックがかかったときに、端末に表示するメッセージを 200 文字以内で入力します。 ●電話番号 リモートロックがかかったときに、端末に表示する電話番号を 20 文字以内の半角数字、記号（「-」、「+」、「*」、「#」、「,」）で入力します。 iOS 端末にパスコードが設定されていない場合、デフォルトのロック解除画面だけが表示されます。このため、「ロックメッセージ」、「電話番号」で設定された連絡情報をユーザーが確認はできません。リモートロックを行う前に、対象の機器の詳細画面の「情報」の「デバイス」で「スクリーンロック」の「パスコード保護」が有効になっていることを必ず確認してください。 ☞「(情報－iOS）デバイス」151 ページ iOS 7.0 以下の OS では、「ロックメッセージ」と「電話番号」は表示されません。
2	リモートワイプ	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末に一括でリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●同意する リモートワイプを実行する場合は、必ずチェックを入れます。 端末のデータ消去が開始されると、途中で中止できません。 iOS 17 以上の監視対象端末では、［リモートワイプ時に Wi-Fi 設定を適用する］にチェックを入れると、リモートワイプ時に Wi-Fi 設定が含まれる構成プロファイルを適用することができます。端末を初期化したあと、手動で Wi-Fi 設定をする必要がなくなります。また、適用した構成プロファイルを削除することもできます。詳細は、以下を参照してください。 ☞「(操作－iOS）リモートワイプ」118 ページ
3	リモートワイプ（管理領域）	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末に一括でリモートワイプ（管理領域）を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●同意する リモートワイプ（管理領域）を実行する場合は、必ずチェックを入れます。 端末の管理領域のデータ消去が開始されると、途中で中止できません。
4	パスコード削除	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末のパスコードを一括で削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●同意する パスコード削除を実行する場合は、必ずチェックを入れます。

項番	項目	説明
5	紛失モード	以下の項目を設定して［実行］をクリックすると、iOS 端末に一括で紛失モードの設定を適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●ロックメッセージ 紛失モード中になったときに、端末に表示するメッセージを 200 文字以内で入力します。 ●電話番号 紛失モード中になったときに、端末に表示する電話番号を 20 文字以内の半角数字、「-」、「+」、「*」、「#」、「,」で入力します。 ●脚注 ロックメッセージや電話番号以外に表示する内容があれば、30 文字以内で入力します。 iOS 9.3 以上の監視対象端末のみ有効です。 「ロックメッセージ」または「電話番号」のいずれかは入力必須です。
6	位置情報取得	紛失モードを適用して［実行］をクリックすると、iOS 端末の位置情報を一括で取得します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 位置情報取得を実行する場合は、紛失モードを実行する必要があります。 エージェント認証をしていない端末でも端末の位置情報を取得します。
7	紛失モード解除	［実行］をクリックすると、iOS 端末の紛失モードを一括で解除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 紛失モード解除を実行する場合は、紛失モードを実行する必要があります。
8	アクティベーションロック解除	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末のアクティベーションロックを一括で解除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●同意する アクティベーションロック解除を実行する場合は、必ずチェックを入れます。 以下の 4 つの条件を満たしている場合に表示され、解除ができます。 ・監視対象端末である。 ・端末の機器タブに表示されるアクティベーションロックステータスが「有効」になっている。 ・エージェント共通管理のアクティベーションロックの設定が「許可する」になっている。 ・端末の Bypass Code が取得できている（機器タブの Bypass Code が表示されている）。
9	OS アップデート	以下の項目を設定し、「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末の OS を一括でアップデートします。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●OS アップデートの動作 ●OS のダウンロードまたはインストール ●OS のダウンロードのみ ●ダウンロード済みの OS をインストール ●同意する OS のアップデートを実行する場合は、必ずチェックを入れます。 OS アップデートができなかった場合は、原因のログが表示されます。詳細については、以下を参照してください。 『FAQ 一覧』の「管理サイト」－「Q30」、「iOS」－「Q35」「Q37」

項番	項目	説明
10	リモート再起動	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末を一括で再起動します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 本機能を実行すると操作を取り消すことはできません。十分に注意してください。 監視対象端末で有効です。 端末にパスコードが設定されている場合は、再起動後、パスコードを入力しないと Wi-Fi に接続することができません。
11	リモートシャットダウン	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末を一括でシャットダウンします。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 本機能を実行すると操作を取り消すことはできません。十分に注意してください。 監視対象端末で有効です。 端末にパスコードが設定されている場合は、再起動後、パスコードを入力しないと Wi-Fi に接続することができません。
12	MDM 構成プロファイル更新	「同意する」にチェックを入れて［実行］をクリックすると、iOS 端末の MDM 構成プロファイルを更新します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 本機能を実行すると操作を取り消すことはできません。十分に注意してください。

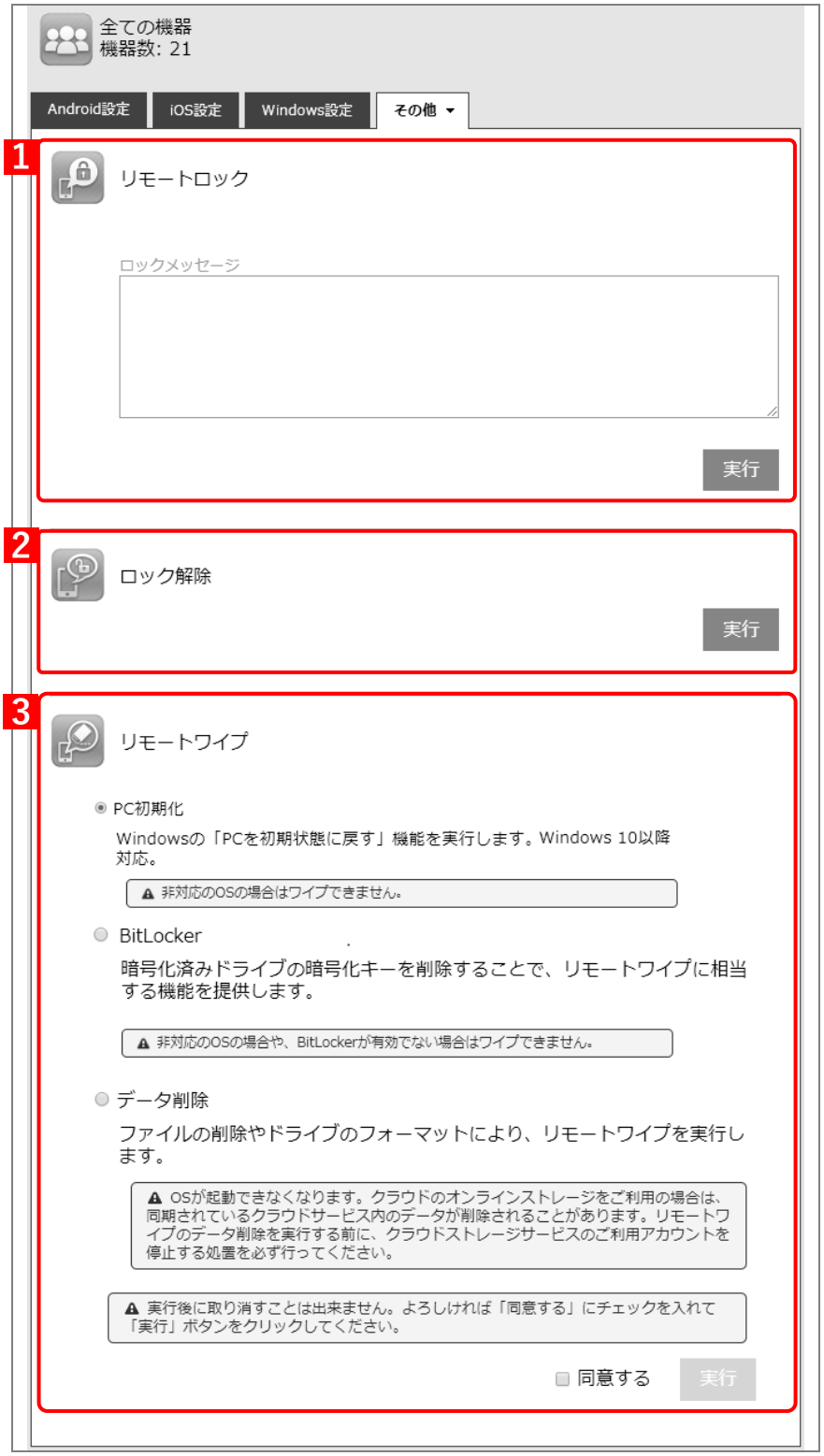
4.4.6 ［その他▼］タブ／Windows リモート操作

すべての Windows 端末に、以下のリモート操作を行うことができます。

- リモートロック
- ロック解除
- リモートワイプ

◆画面

表示操作［機器］→［全機器一括設定］→［その他▼］→［Windows リモート操作］



項番	項目	説明
1	リモートロック	以下の項目を設定して［実行］をクリックすると、Windows 端末に一括でリモートロックを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●ロックメッセージ リモートロックがかかったときに、端末に表示するメッセージを 200 文字以内で入力します。 システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本機能を利用できないことがあります。グループポリシーについては、システム管理者に問い合わせてください。
2	ロック解除	［実行］をクリックすると、Windows 端末のリモートロックを一括で解除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本機能を利用できないことがあります。グループポリシーについては、システム管理者に問い合わせてください。
3	リモートワイプ	以下の項目を設定し、「同意する」にチェックを入れて［実行］をクリックすると、Windows 端末に一括でリモートワイプを適用します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ●ワイプの方法 ワイプの方法を以下から選択します。 ・PC 初期化 Windows の「PC を初期状態に戻す」機能を実行します。 工場出荷時のリカバリー領域が必要です。リカバリ領域がないと、リモートワイプに失敗します。 ・BitLocker BitLocker で暗号化済みドライブの回復キー以外のキープロテクターを削除します。 BitLocker でのワイプを実行したあとは、端末を起動したときに BitLocker の回復キー入力画面が表示されます。回復キーを入力するまでドライブのデータにアクセスできません。 回復キーのキープロテクターがないドライブは、BitLocker でのワイプができません。 削除した回復キーを新規で作成するには、以下の URL で「構文」と「パラメーター」を参照してください。回復キーの作成方法については、システム管理者に問い合わせてください。 https://learn.microsoft.com/ja-jp/windows-server/administration/windows-commands/manage-bde-protectors 本製品の暗号化機能を利用している場合は、暗号化機能の設定セットを無効、有効の順で割り当てて同期すると、回復キーを遠隔で新規作成することができます。 BitLocker 以外の暗号化ツールを使用している場合は、本機能は使用できません。 Windows 11 Pro/Enterprise/Education の端末に対応しています。詳細については、以下を参照してください。 「暗号化」573 ページ BitLocker については、Microsoft の Web サイトを参照してください。 https://learn.microsoft.com/ja-jp/windows/security/operating-system-security/data-protection/bitlocker/ 回復キーとは、48 桁の文字列です。回復パスワードという場合もあります。詳細については、以下を参照してください。

項番	項目	説明
		「(情報－Windows) セキュリティ」181 ページ ・データ削除 ファイルの削除とドライブのフォーマットによりリモートワイプを行います。 データ削除が実行されるため、OS が起動しなくなることがあります。 ●同意する リモートワイプを実行する場合は、必ずチェックを入れます。 データ削除によるリモートワイプ後も、復元技術により第三者にデータが閲覧されてしまう可能性があります。 ドライブのフォーマットは、ドライブ文字・ボリュームラベルを持つドライブが対象です。キャッシュ用途のドライブや、メーカーが設置したリカバリーディスク領域にドライブ文字・ボリュームラベルが割り当てられていると、削除される可能性があります。この場合は、フォーマットしたあとで、PC 機器が再利用できなくなることがあります。 アプリの実行中にリモートワイプ（データ削除）が発生した場合、実行中のアプリにより開かれているファイルやアプリの実行ファイルが削除されずに残ってしまう可能性があります。また、これらのファイルやフォルダーが含まれるフォルダー構造も削除されない可能性があります。 ドライブレターが割り当てられていないドライブの場合、リモートワイプ（データ削除）を行うことができません。ドライブレター設定後に、リモートワイプ（データ削除）を行ってください。 端末の初期化が開始されると、途中で中止できません。

4.5 入力項目のカスタマイズ

詳細画面に表示される管理情報に、任意の項目を追加することができます。

☞「機器の詳細画面」59 ページ

追加できる項目には、リストボックスから項目を選択する［分類］と、テキストボックスに文字を直接書き込む［自由入力］があります。

また、［分類］で追加した項目は、［全機器一括設定］画面に表示され、対象機器の選択条件として使用することもできます。

☞「全機器一括設定」200 ページ

●追加した入力項目で一括設定を行う使用例

① ［分類］タブで、項目名に「営業部」、グループ名に「営業 1 課」と「営業 2 課」を設定して新規作成します。

☞「画面（新規作成）」220 ページ

② 各機器の管理情報に表示される「営業部」の項目で「営業 1 課」と「営業 2 課」のいずれかを選択し、機器を分類項目に紐づけます。

☞「機器の管理情報」67 ページ

③ 全機器一括設定で、「営業部」をクリックして表示されるメニューから「営業 1 課」または「営業 2 課」を選択し、機能を一括適用します。

☞「全機器一括設定」200 ページ

4.5.1 ［分類］タブ

詳細画面にリストボックスを追加することができます。

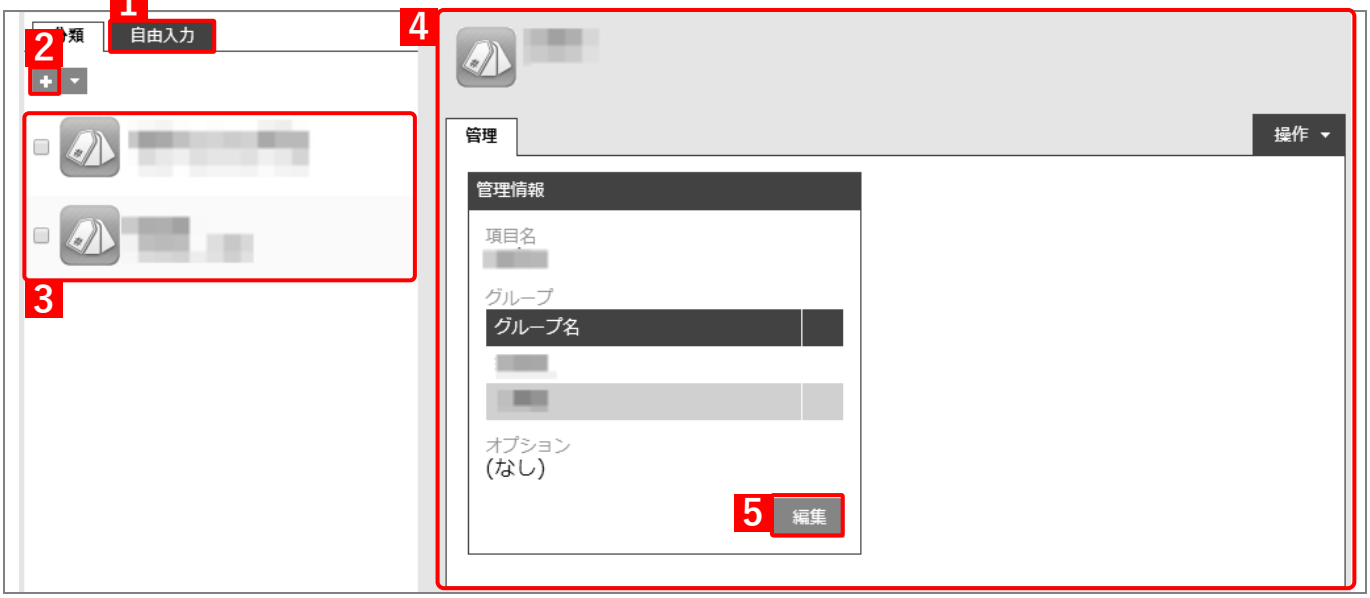
営業部の 1 課から 5 課など、追加したい情報の項目が決まっている場合に有効です。

画面

画面（新規作成）

◆画面

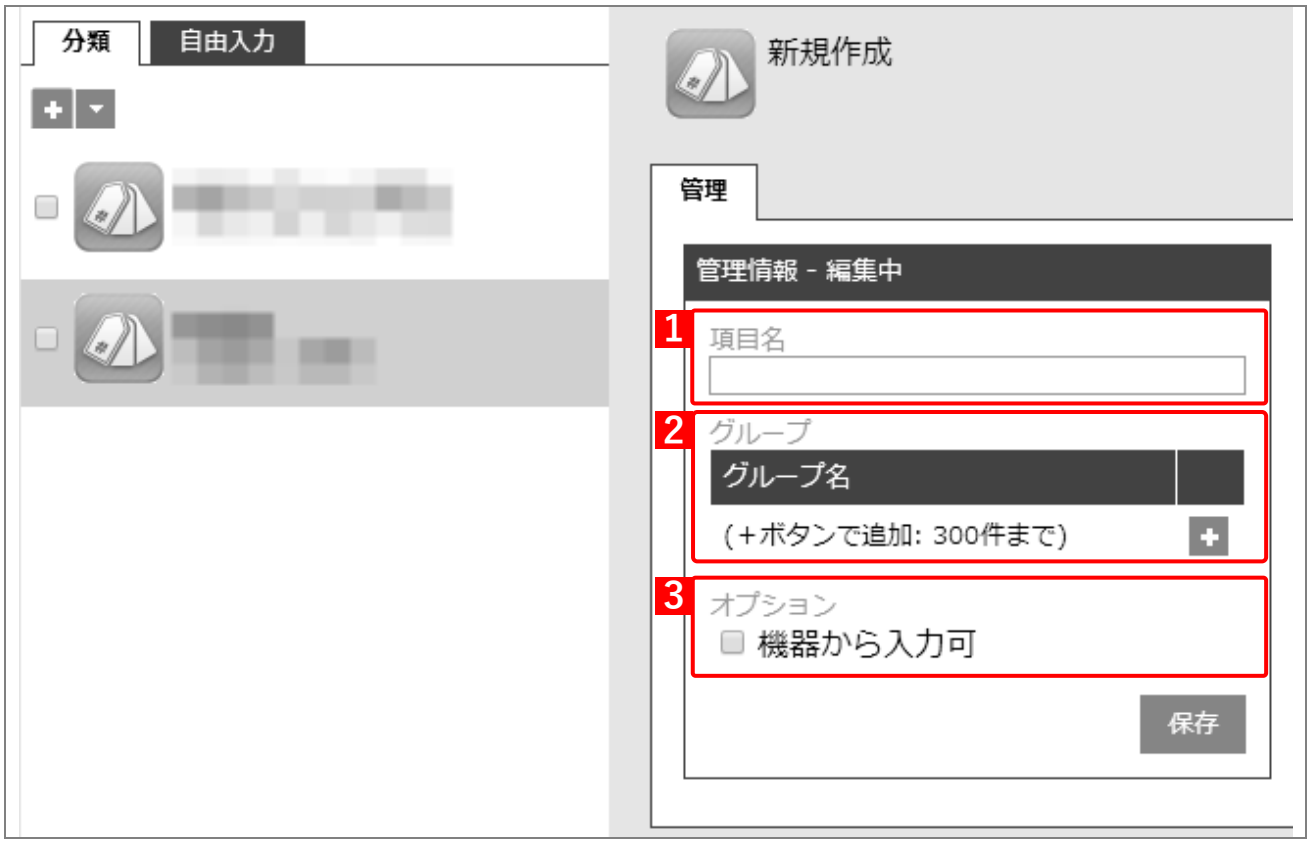
表示操作［機器］→［入力項目のカスタマイズ］→［分類］タブ



項番	名称	説明
1	［自由入力］タブ	クリックすると自由入力画面が表示されます。詳細については、以下を参照してください。 「［自由入力］タブ」221 ページ
2	✚	クリックすると分類の新規作成画面が表示されます。分類は、最大 50 件まで作成できます。カスタマイズ項目の新規作成は、以下を参照してください。 「画面（新規作成）」220 ページ
3	分類一覧	登録されているカスタマイズ項目の項目名が表示されます。
4	管理情報	分類一覧から選択した項目の登録内容が表示されます。
5	［編集］	クリックすると、登録されている入力項目のカスタマイズ情報を編集できます。編集できる項目は、新規作成時と同じです。

◆画面（新規作成）

表示操作［機器］→［入力項目のカスタマイズ］→［分類］タブ→ ✚



項番	項目	説明
1	項目名	分類の項目名を 30 文字以内で入力します。重複する項目名は登録できません。 例）営業部
2	グループ	項目名で指定した分類の下にグループを作成します。項目内で重複するグループ名は登録できません。✚ をクリックして、グループ名を 30 文字以内で入力します。最大 300 件指定できます。 例）営業 1 課、営業 2 課
3	オプション	「機器から入力可」にチェックを入れると、端末の機器情報の変更で、項目を入力できます。

4.5.2 ［自由入力］タブ

詳細画面にテキストボックスを追加することができます。

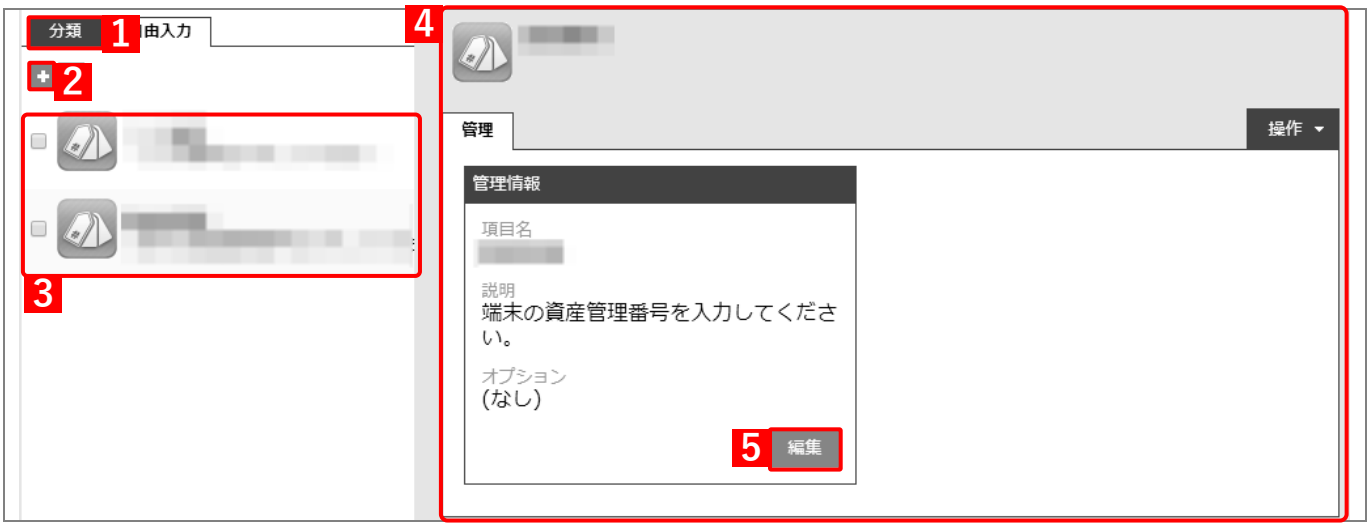
端末の資産管理番号など、追加したい情報を、任意に入力したい場合に有効です。

画面

画面（新規作成）

◆画面

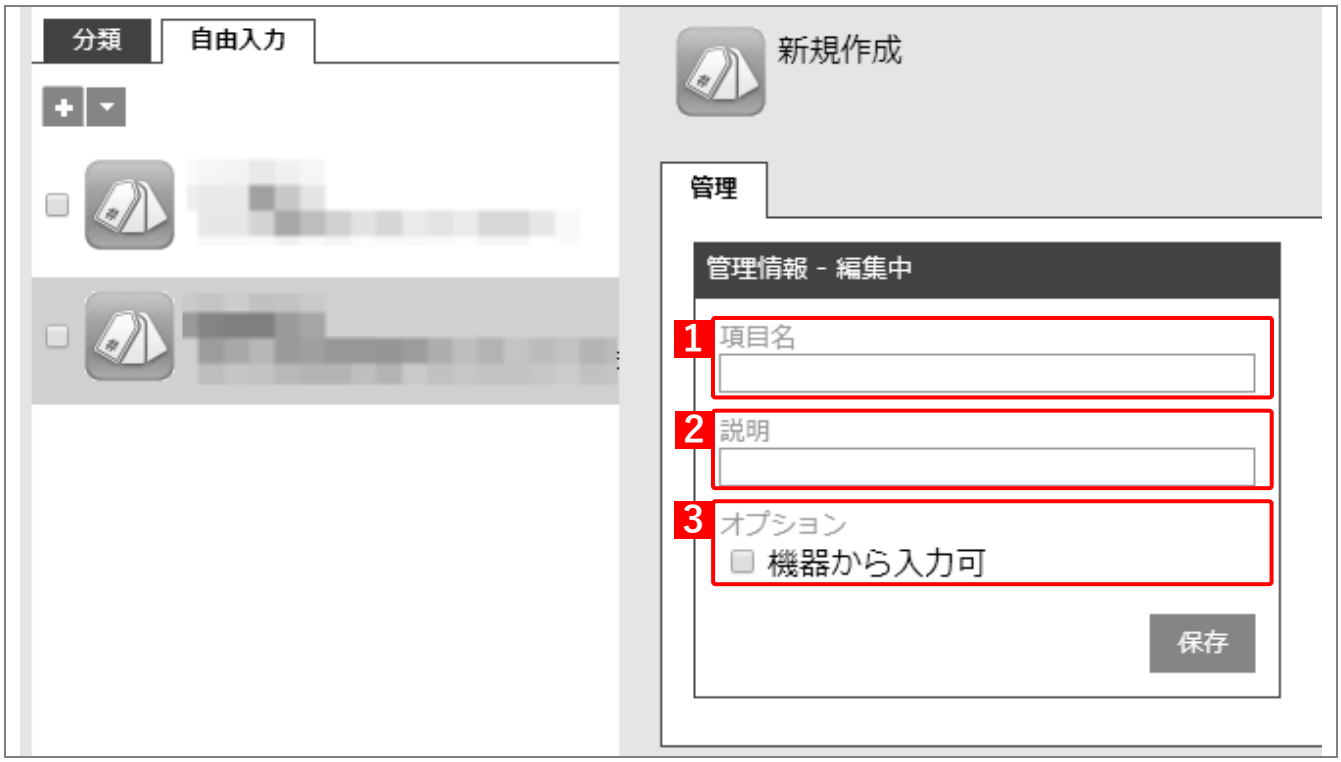
表示操作　**［機器］→［入力項目のカスタマイズ］→［自由入力］タブ**



項番	名称	説明
1	［分類］タブ	クリックするとユーザー分類画面が表示されます。詳細については、以下を参照してください。 「［分類］タブ」219 ページ
2	✚	クリックすると自由入力の新規作成画面が表示されます。自由入力は、最大 50 件まで作成できます。カスタマイズ項目の新規作成は、以下を参照してください。 「画面（新規作成）」222 ページ
3	自由入力一覧	登録されている自由入力の項目名が表示されます。
4	管理情報	自由入力一覧から選択した自由入力の登録内容が表示されます。
5	［編集］	クリックすると、表示されている入力項目の管理情報を編集できます。編集できる項目は、新規作成時と同じです。

◆画面（新規作成）

表示操作［機器］→［入力項目のカスタマイズ］→［自由入力］タブ→ ✚



項番	項目	説明
1	項目名	入力欄の項目名を 30 文字以内で入力します。重複する項目名は登録できません。 例）資産管理番号
2	説明	入力欄についての説明などがあれば、100 文字以内で入力します。 入力した説明文は、各機器の管理情報の該当項目の入力欄の下に「※」付きで表示されます。
3	オプション	「機器から入力可」にチェックを入れると、端末の機器情報の変更で、項目を入力できます。

4.6 メッセージ通知

任意のメッセージを作成し、Android 端末と iOS 端末に配信します。

登録されているすべての Android 端末と iOS 端末への配信や、グループ単位、端末ごとの配信を行うことができます。

また、スケジュールを作成して、定期的なメッセージの配信や配信履歴の確認をすることもできます。

●グループの作成については、以下を参照してください。

☞「入力項目のカスタマイズ」218 ページ

●［機器］→［一覧］の詳細情報で、端末ごとに配信予定、または配信済みのメッセージを確認できます。

☞「（情報－Android）メッセージ」149 ページ

☞「（情報－iOS）メッセージ」170 ページ

メッセージ通知は、Android 端末、iOS 端末にのみ配信することができます。選択されたグループに紐づけされている端末が Android 端末、または iOS 端末以外の場合は、配信されません。

iOS 端末にメッセージを配信する場合は、端末に iOS エージェントのインストールが必要です。

メッセージは、最大 50 件まで作成できます。

4.6.1 ［メッセージ］タブ

Android 端末や iOS 端末に配信するメッセージを作成、編集します。

画面（新規作成）

画面

◆画面（新規作成）

表示操作　［機器］→［メッセージ通知］→ ＋（一覧から対象を選択→［編集］）

項番	項目	説明
1	タイトル	メッセージのタイトルを 30 文字以内で入力します。タイトルはメールの件名に該当します。重複したタイトルは登録できません。
2	内容	メッセージの内容を 250 文字以内（空白、タブ、改行など含む）で入力します。内容はメールの本文に該当します。特殊文字は入力できません。
3	オプション	「端末での表示時に URL をリンクにする（リンクの挙動は端末に依存します）」にチェックを入れると、メッセージの内容に URL が含まれている場合、機器で表示したときに URL 部分がハイパーリンクとして表示されます。

◆画面

表示操作　**［機器］→［メッセージ通知］→一覧から対象を選択**

項番	名称	説明
1	［配信］	クリックすると配信の確認画面が表示され、確認画面で［OK］をクリックすると、登録されているメッセージをただちに配信します。 スケジュールの指定に関係なく、必要なときに配信することができます。 メッセージ通知が端末に配信されるまでの時間は、サーバーや端末の通信状態に依存します。
2	［編集］	クリックするとメッセージ内容を編集することができます。 編集内容は新規作成と同じです。 「画面（新規作成）」224 ページ

4.6.2 ［配信先］タブ

メッセージの配信先を設定します。

登録されているすべての Android 端末、iOS 端末に配信するか、指定したグループ、または個別の端末に配信するかを選択できます。

「機器のグループを指定」で設定する場合は、事前にグループを登録してください。

「入力項目のカスタマイズ」218 ページ

「機器を指定」で設定する場合は、メッセージを通知する Android 端末、または iOS 端末の登録が必要です。

◆画面

表示操作　**［機器］→［メッセージ通知］→一覧から対象を選択→［配信先］タブ→［編集］**

項番	項目	説明
1	一括で指定	「全ての機器」にチェックを入れると、すべての機器が配信先に指定されます。チェックされている間は、ほかの指定は行えません。 「全ての機器」にチェックが入っている場合は、「機器のグループを指定」と「機器を指定」の指定はできません。
2	機器のグループを指定	配信先にグループを指定する場合は、 をクリックして、リストボックスから対象のグループを選択します。最大 100 件指定できます。
3	機器を指定	配信先に機器を指定する場合は、 をクリックして、リストボックスから対象の機器を選択します。最大 100 件指定できます。
4	［配信］	クリックすると、選択中のメッセージを指定した配信先に配信します。 「画面」225 ページ

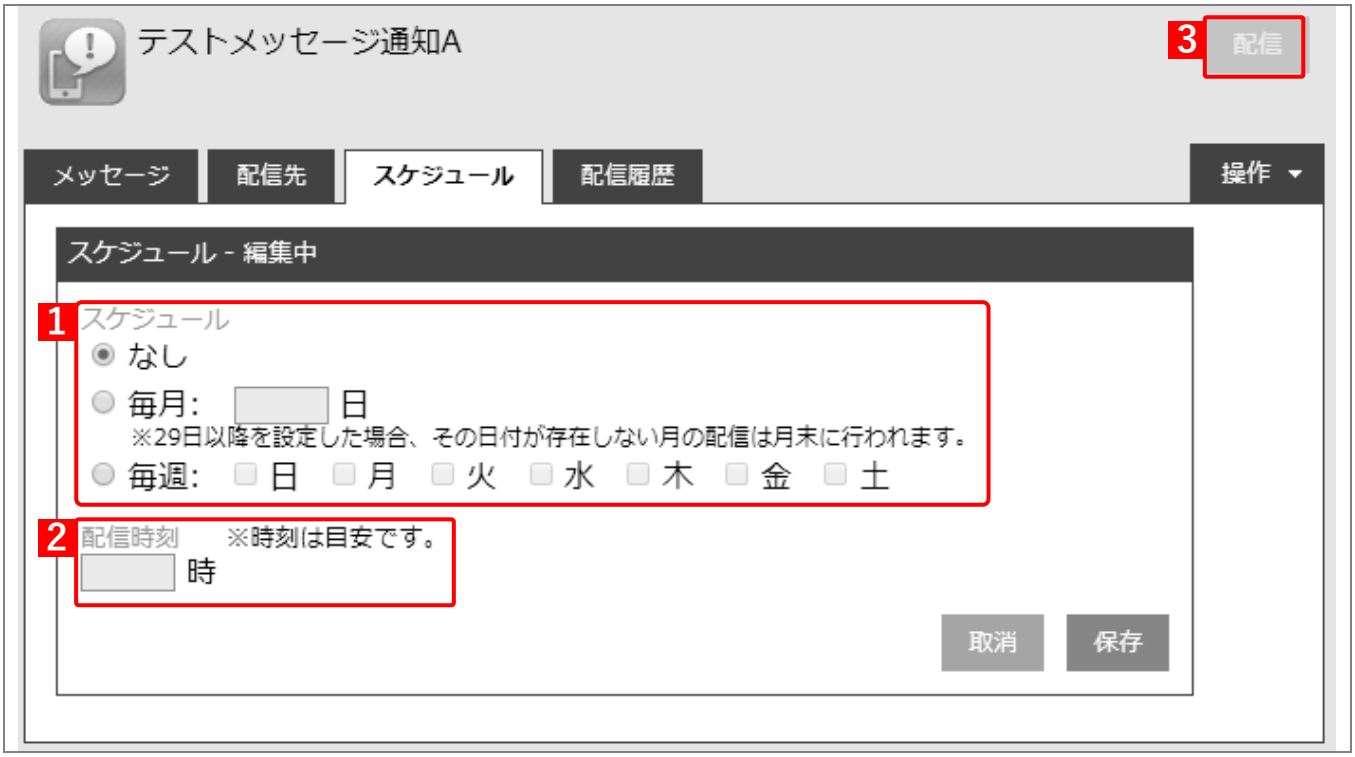
4.6.3 ［スケジュール］タブ

スケジュールを作成し、定期的にメッセージを配信します。

毎月の指定日や毎週の指定曜日ごとに配信することができます。

◆画面

表示操作［機器］→［メッセージ通知］→メッセージを選択→［スケジュール］タブ→［編集］



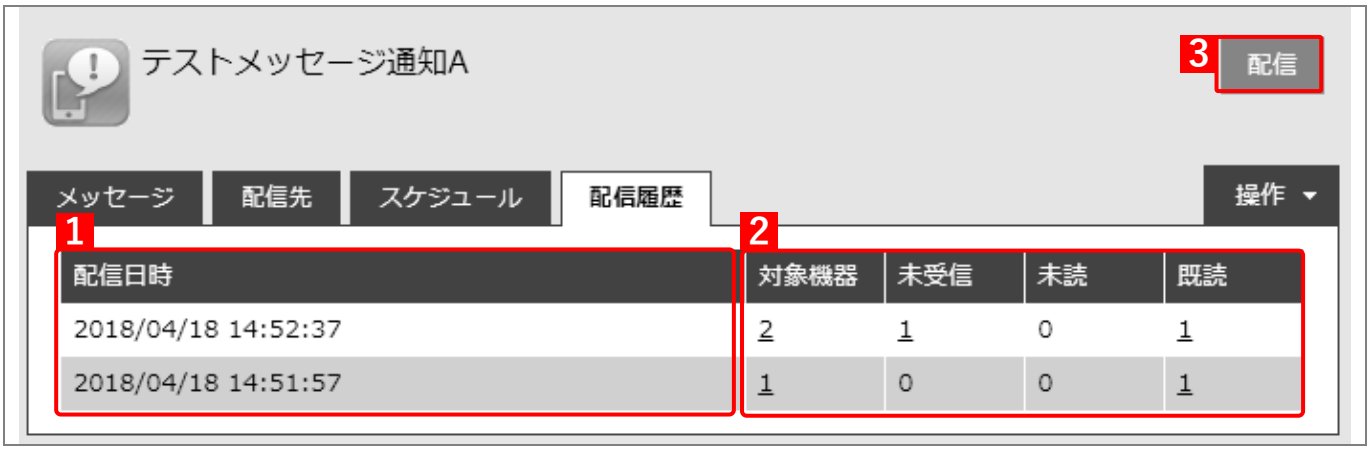
項番	項目	説明
1	スケジュール	スケジュールを以下から選択します。 ●なし スケジュールを設定しません。 ●毎月 毎月指定した日付に配信します。「日」に 1 から 31 の半角数字を入力します。 「日」に 29 以降を入力した場合は、その日付が存在しない月は月末が配信日です。 ●毎週 毎週指定した曜日に配信します。配信する曜日にチェックを入れます。複数の曜日を指定できます。
2	配信時刻	目安となる配信時刻を 0 から 23 の半角数字で入力します。 厳密な配信時刻ではありません。通知メッセージが機器に届くまでの時間は、サーバーや機器の通信状態に依存します。
3	［配信］	クリックすると、選択中のメッセージを指定した配信先に配信します。 「画面」225 ページ

4.6.4 ［配信履歴］タブ

メッセージ通知の配信履歴を確認します。配信日時ごとに、対象機器数／未受信数／未読数／既読数を確認できます。

◆画面

表示操作　**［機器］→［メッセージ通知］→メッセージを選択→［配信履歴］タブ**



項番	項目	説明
1	配信日時	メッセージを配信した日時が表示されます。
2	対象機器／未受信／未読／既読	メッセージを配信した機器の数、そのうちの未受信、未読、既読の機器の数が表示されます。機器数をクリックすると、対象の機器の一覧画面が表示されます。
3	［配信］	クリックすると、選択中のメッセージを指定した配信先に配信します。 ☞「画面」225 ページ

4.7 CSV で追加

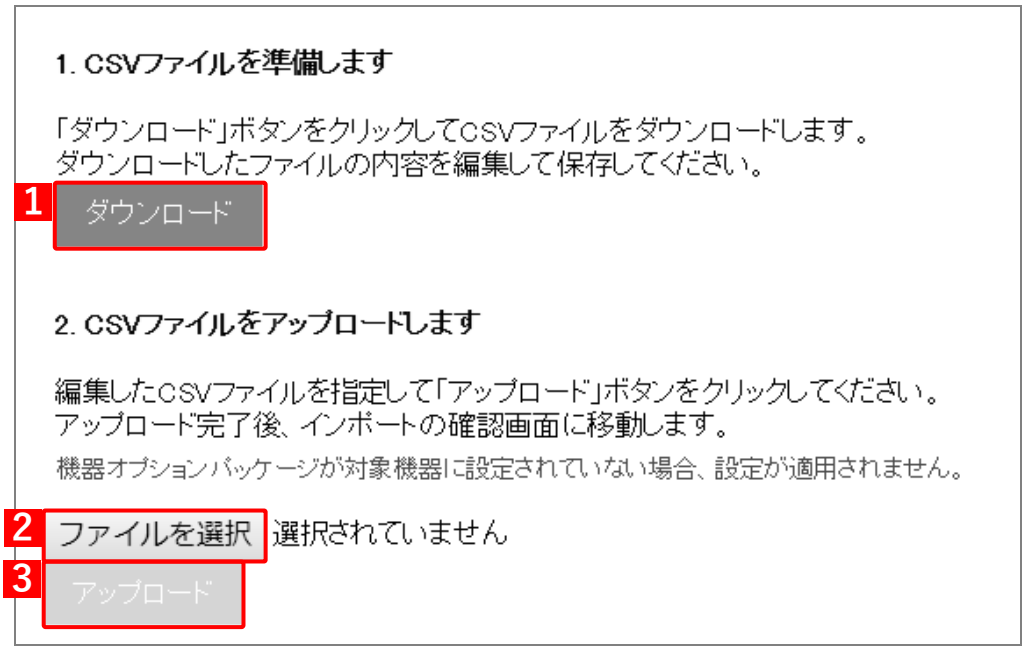
CSV ファイルを利用して、複数の端末情報を一括で管理サイトに登録できます。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

◆画面

表示操作［機器］→［CSV で追加］



項番	項目	説明
1	［ダウンロード］	CSV ファイルがダウンロードされます。ダウンロードした CSV ファイルに機器情報を入力し、インポート用の CSV ファイルを作成します。機器情報の入力方法については、以下を参照してください。 「インポート用の CSV ファイルの項目」230 ページ
2	［ファイルを選択］	機器情報を入力したインポート用の CSV ファイルを選択します。
3	［アップロード］	インポート用の CSV ファイルがアップロードされます。アップロードが完了すると、インポート画面が表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠ データの確認を中断しました。	アップロード処理中に［中断］をクリックしている。	再度アップロードを実施し、アップロード中は［中断］をクリックしないでください。
⚠ 各種エラーメッセージ ※エラーが発生している列により、エラー文言が異なります。	CSV 内の項目いずれかで、不正な値が入った状態でアップロードを行っている。	アップロード失敗画面の表内、一番右の欄のコメントに従い CSV を修正してください。

◆インポート用の CSV ファイルの項目

機器情報を CSV ファイルからインポートして追加、編集する場合、CSV ファイルに以下の項目を入力、編集して作成します。

- CSV ファイルの 1 行目に項目名が表示されています。登録する情報は、2 行目以降に入力してください。
- 変更に使用する CSV ファイルには、登録されている機器の情報が表示されています。列と行の追加や削除は行わず、内容の修正のみ行ってください。
- CSV ファイルの構造については、以下を参照してください

  『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

項目名	入力方法
GUID	変更しないでください。 この項目は「CSV で編集」でダウンロードした CSV ファイルに表示されます。
[S]Android 機器	Android 端末を追加する場合は、「ON」と入力します。
[S]iOS 機器	iOS 端末を追加する場合は、「ON」と入力します。
[S]Windows 機器	Windows 端末を追加する場合は、「ON」と入力します。
[S]資産管理対象機器	資産管理対象機器を追加する場合は、「ON」と入力します。
[F]機器名	制御文字を含まない 100 文字以内で、機器名を入力します。 すでに登録されている機器と同じ機器名にならないことを確認してください。
[S]種別	[S]資産管理対象機器を「ON」にした場合は、種別を入力します。種別については、以下を参照してください。 「画面（新規作成：「資産管理対象機器」を選択した場合）」65 ページ
[S]ユーザー	登録済みのユーザー名を入力します。
[S:iOS]構成プロファイル	登録済みの構成プロファイルの設定名を入力します。
[G]から始まる項目	「入力項目のカスタマイズ」の「分類」で登録した項目です。項目に該当する内容を入力します。 「入力項目のカスタマイズ」の「分類」で何も登録していない場合は、項目は表示されません。
[C]から始まる項目	「入力項目のカスタマイズ」の「自由入力」で登録した項目です。項目に該当する内容を入力します。 「入力項目のカスタマイズ」の「自由入力」で何も登録していない場合は、項目は表示されません。
[I]から始まる項目	変更できません。値を修正しても機器情報に反映されません。 この項目は「CSV で編集」でダウンロードした CSV ファイルに表示されます。
[P]から始まる項目	オプションパッケージを使用する場合は「ON」、使用しない場合は「空白（入力なし）」にしてください。
[S:iOS:Exchange]SSL を使用	「使用する」または「使用しない」を入力します。
[S:iOS:Exchange]過去のメールを同期	以下のいずれかを入力します。 ・「0」（無制限）、「1」（1 日）、「3」（3 日間）、「7」（1 週間）、「14」（2 週間）、「31」（1 か月）
[S:iOS:Exchange]認証に OAuth を使用	「使用する」または「使用しない」を入力します。
その他の[S:iOS:Exchange]から始まる項目	項目名に該当する値を入力します。

項目名	入力方法
その他の[S:から始まる項目	設定名（設定セットの名称）を入力します。 設定テンプレートの設定と競合している場合は、設定テンプレートが優先されます。各 OS の設定テンプレートの詳細については、以下を参照してください。 Android：「設定テンプレート」300 ページ iOS：「設定テンプレート」387 ページ Windows：「設定テンプレート」564 ページ

4.8 CSV で編集

登録されている機器情報をまとめて編集（変更）したい場合に使用します。

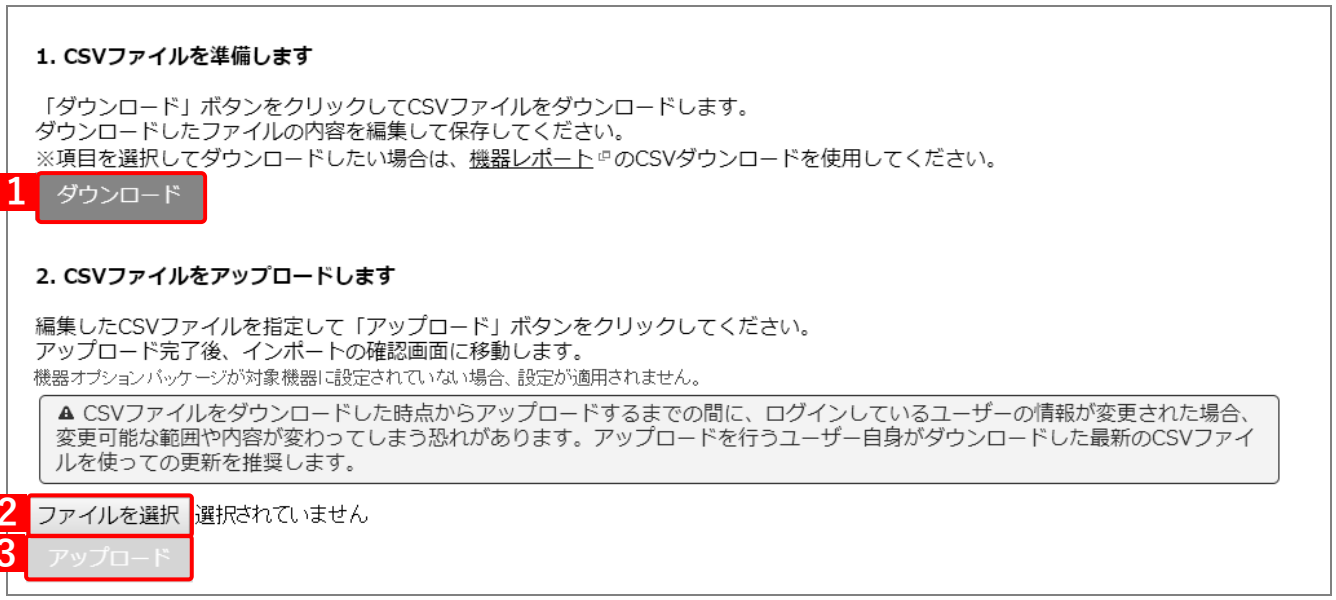
操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

あらかじめすべての機器情報が記載されている CSV ファイルをダウンロードし、Excel やメモ帳などのアプリを使用して、機器情報を編集したファイルを作成してください。

◆画面

表示操作［機器］→［CSV で編集］



項番	項目	説明
1	［ダウンロード］	登録されているすべての機器情報が記載されている CSV ファイルをダウンロードします。ダウンロードした CSV ファイルの編集方法については、以下を参照してください。 「インポート用の CSV ファイルの項目」230 ページ
2	［ファイルを選択］	機器情報を編集したインポート用の CSV ファイルを選択します。
3	［アップロード］	機器情報をアップロードします。アップロードが完了すると、インポート画面が表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠ データの確認を中断しました。	アップロード処理中に［中断］をクリックしている。	再度アップロードを実施し、アップロード中は［中断］をクリックしないでください。
⚠ 各種エラーメッセージ ※エラーが発生している列により、エラー文言が異なります。	CSV 内の項目いずれかで、不正な値が入った状態でアップロードを行っている。	アップロード失敗画面の表内、一番右の欄のコメントに従い CSV を修正してください。

4.9 CSV で削除

CSV ファイルを利用して、複数の端末情報を一括で管理サイトから削除できます。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

- あらかじめすべての機器情報が記載されている CSV ファイルをダウンロードし、Excel やメモ帳などのアプリを使用して、機器情報を編集したファイルを作成してください。
- 本機能を実行したあと、実際に機器が削除されるまで数日かかります。本機能では、削除の予約をすることになります。削除の予約をした機器は、機器一覧に取り消し線が表示されます。取り消し線が表示されている機器は、削除の予約を取り消すことができます。機器一覧の詳細については、以下を参照してください。

「機器一覧」54 ページ

- 削除の予約をしている機器は、実際に削除されるまで機器数およびライセンスの変更はありません。
- 削除の予約をしている機器は、機器レポートの「[I]削除状況」に「D」が表示されます。

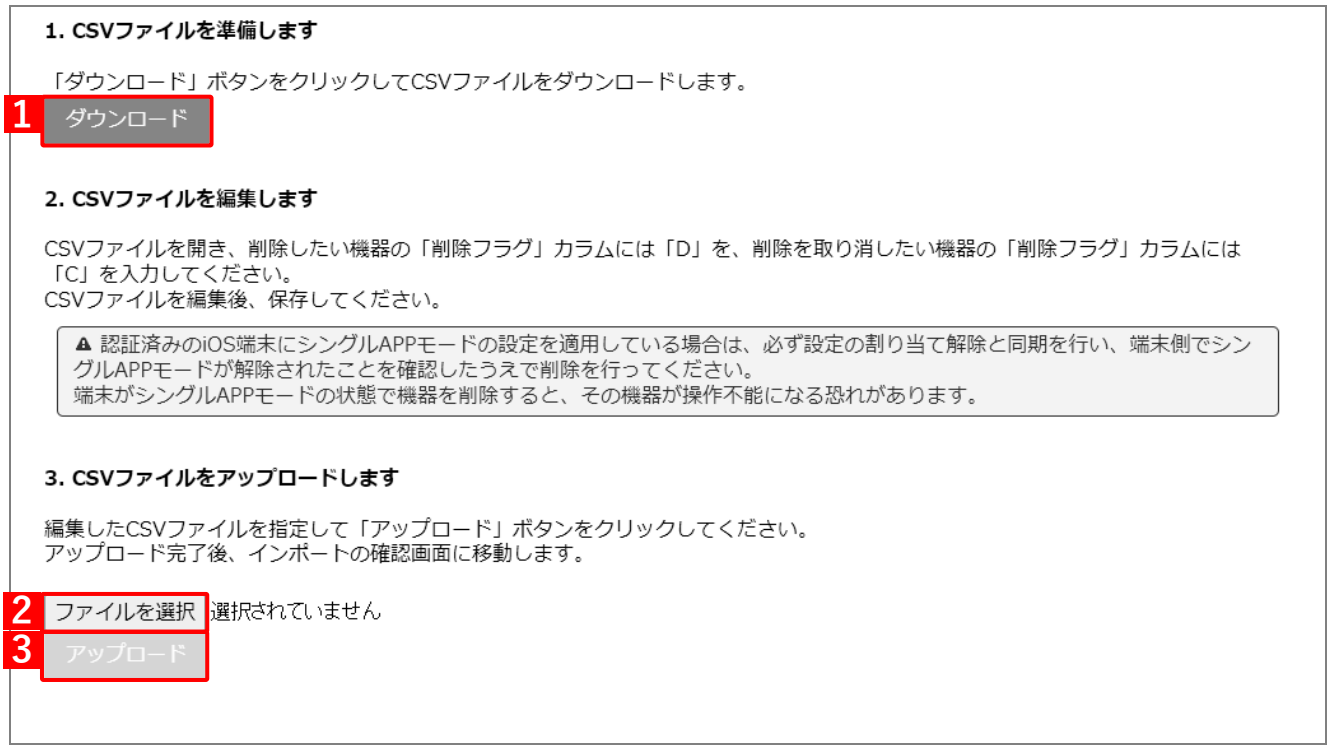
「機器レポート」237 ページ

- 削除の予約をしている機器は、シングル APP モードの設定を割り当てることはできません。
- iOS 端末にシングル APP モードの設定を適用している場合は、必ずシングル APP モードの割り当てを解除／同期を行い、端末で解除されたことを確認してから、機器を削除してください。シングル APP モードが適用されている状態で機器を削除すると、端末が操作不能になる場合があるので、注意してください。

「シングル APP モード（監視対象のみ）」535 ページ

◆画面

表示操作　［機器］→［CSV で削除］



項番	項目	説明
1	［ダウンロード］	任意の場所に機器を削除するための CSV ファイルを保存します。保存した CSV ファイルを Excel やメモ帳で開き、削除したい機器名の右側にある「[S]削除フラグ」列に「D」と入力して保存します。 すでに本機能でインポートした機器には、「[S]削除フラグ」列に「D」と入力されています。「D」を「C」に変更すると、削除の予約を取り消すことができます。 機器名に絵文字など Shift_JIS で表示できない文字を使用していた場合は、対象の文字が「?」に変換されて、CSV ファイルがダウンロードされます。本機能を使用するうえで問題はなく、該当の機器は削除の予約ができます。
2	［ファイルを選択］	項番 1 で保存した CSV ファイルを選択します。
3	［アップロード］	CSV ファイルのアップロードが開始されます。アップロードが完了すると、インポート画面が表示されます。

4.10 CSV でクライアント証明書紐付け（iOS のみ）

CSV ファイルを利用して、iOS 端末と複数のクライアント証明書を一括で紐づけることができます。

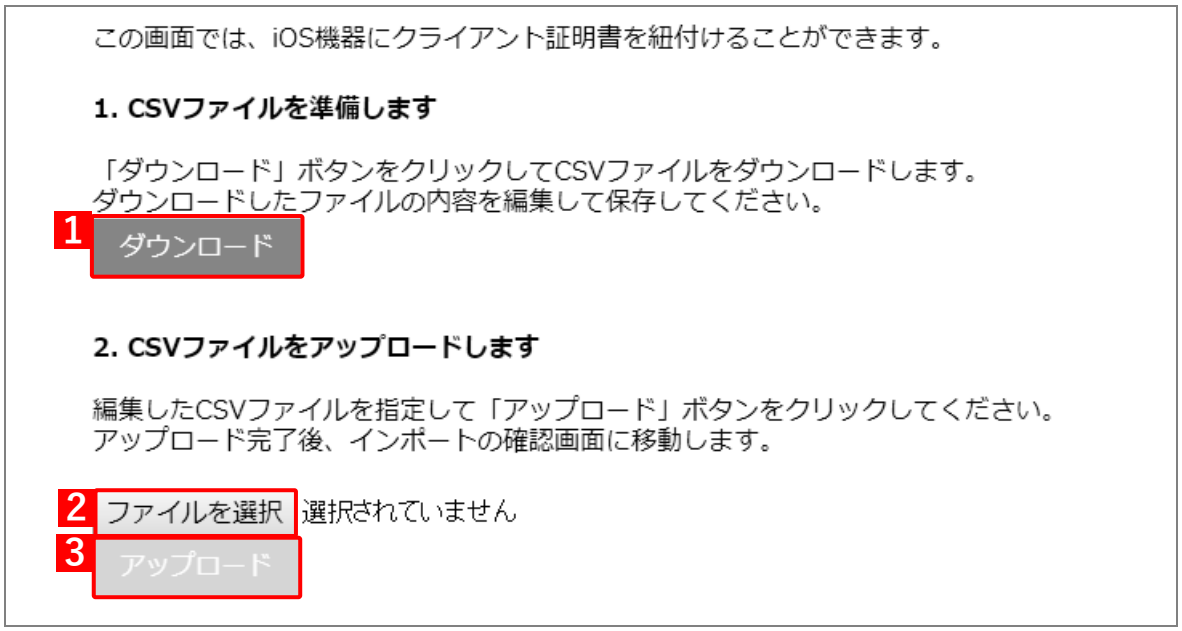
詳細は、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

- 紐づけたいクライアント証明書を、あらかじめ管理サイトにアップロードしてください。
- クライアント証明書は、各 iOS 端末に最大 5 つ（デフォルトのクライアント証明書 1 つ、およびその他のクライアント証明書 4 つ）まで紐づけることができます。
- 端末に紐づけられているクライアント証明書を削除した場合は、端末に割り当てられている設定が動作しなくなることがあります。
- 削除対象のクライアント証明書は、管理サイトおよび iOS 端末からも削除されます。

◆画面

表示操作　［機器］→［CSV でクライアント証明書紐付け］



項番	項目	説明
1	［ダウンロード］	iOS 端末にクライアント証明書を紐づけるための CSV ファイルを任意の場所に保存します。保存した CSV ファイルを Excel やメモ帳で開き、機器名の右側にある「[S]クライアント証明書（デフォルト）」列、および「[S]クライアント証明書[1]」～「[S]クライアント証明書[4]」列に紐づけたいクライアント証明書名を入力して保存します。
2	［ファイルを選択］	項番 1 で保存した CSV ファイルを選択します。
3	［アップロード］	CSV ファイルのアップロードが開始されます。アップロードが完了すると、インポート画面が表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠ 証明書「(証明書名)」は存在しません。	管理サイト上に存在しない名前の証明書が CSV 内に記載されている状態でアップロードを実行している。	管理サイト上に存在している名前の証明書を指定して、アップロードを行ってください。
⚠ 1 機器に対して証明書「(証明書名)」を 2 つ以上割り当てることができません。	CSV 内で 1 機器に対して同じ名前のクライアント証明書を複数指定した状態で、アップロードを実行している。	1 機器に対して同じ名前のクライアント証明書を複数指定しないでください。
⚠ GUID の一致する iOS 機器が存在しません。	CSV ダウンロード後に、機器画面から機器を削除している。	もう一度 CSV をダウンロードし、最新の CSV 情報を編集してください。
⚠ CSV ファイルのカラム名、またはカラム数が変更されています。	CSV のカラム名がデフォルトの値から書き換えられた状態で、アップロードを行っている。	再度 CSV をダウンロードし、カラム名をデフォルトの値から書き換えずに編集したものをアップロードしてください。
⚠ CSV ファイルの行数の上限は(上限件数) です。	行数の上限 (50,000 行) を超過した CSV ファイルをアップロードしている。	CSV ファイルの行数は 50,000 行を超えないように編集し、アップロードを行ってください。
⚠ データの確認を中断しました。	処理中に［中断］をクリックしている。	再度アップロードを実施し、アップロード中は［中断］をクリックしないでください。
⚠ 各種エラーメッセージ ※エラーが発生している列により、エラー文言が異なります。	CSV 内の項目いずれかで、不正な値が入った状態でアップロードを行っている。	アップロード失敗画面の表内、一番右の欄のコメントに従い CSV を修正してください。

4.11 CSV をダウンロード

機器情報のレポートや、機器にインストールされているアプリのレポートを作成し、作成したレポートを CSV ファイルとしてダウンロードすることができます。

4.11.1 機器レポート

管理情報や機器情報、設定状況を一覧で確認できます。

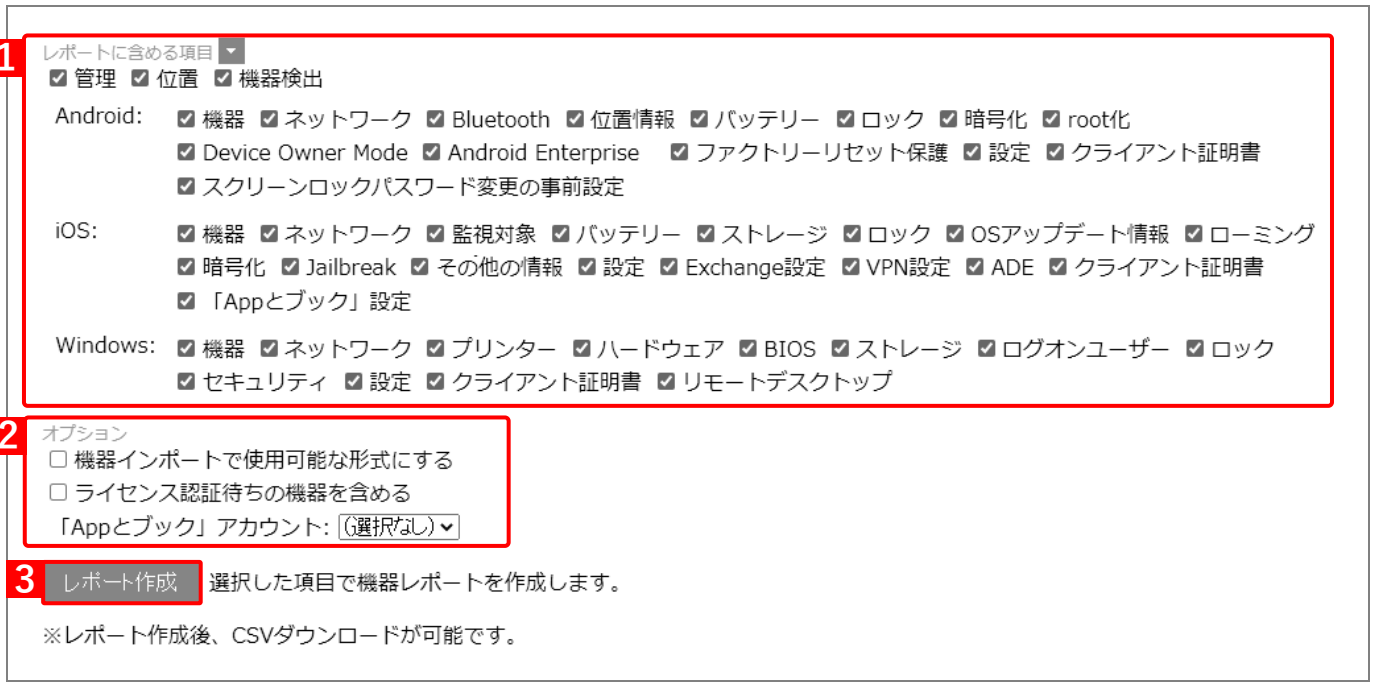
作成した機器レポートは、CSV ファイルとして出力することができます。

画面

画面（レポート作成結果）

◆画面

表示操作［機器］→［CSV をダウンロード］→［機器レポート］



項番	項目	説明
1	レポートに含める項目	レポートに含めたい項目にチェックを入れます。 ●管理 管理している機器の情報をレポートに含める。 ●位置 取得した位置情報をレポートに含める。 ●機器検出 機器検出した機器の情報をレポートに含める。 ●Android Android の機器レポートの条件にする項目にチェックを入れます。 ●iOS iOS の機器レポートの条件にする項目にチェックを入れます。 「Jailbreak」は iOS エージェントがインストールされていない場合は表示されません。 ●Windows Windows の機器レポートの条件にする項目にチェックを入れます。 をクリックすると、メニューから OS ごとのすべての項目にチェックを入れたり、すべての項目のチェックを入れたり、外したりする操作がで

項番	項目	説明
		きます。
2	オプション	必要に応じて、以下のオプションを指定します。 ●機器インポートで使用可能な形式にする チェックを入れると作成したレポートを CSV ファイルに出力し、機器インポートで使用できます。 ●ライセンス認証待ちの機器を含める チェックを入れるとライセンス認証待ちの機器を含めてレポートを作成します。 ●「App とブック」アカウント 「App とブック」アカウントを選択すると、以下のいずれかの条件を満たす機器のアプリライセンスの割り当て状況が機器ごとに CSV 出力されます。 ・機器または機器が所属する組織に、選択した「App とブック」アカウント（「App とブック」場所のトークン）が紐づいている ・機器のユーザーまたは機器のユーザーが所属する組織に、選択した「App とブック」アカウント（「App とブック」場所のトークン）が紐づいている 機器とユーザーのどちらにも「App とブック」アカウントを設定している場合は、ユーザーの設定が優先されます。 機器にアプリライセンスが付与している場合は機器への割り当て状況、機器のユーザーにアプリライセンスが付与している場合は機器のユーザーへの割り当て状況が出力されます。 アプリのライセンス割り当て状況には、以下のいずれかが表示されます。 ・割当済 ライセンスが割り当てられている ・割当待ち ライセンスが割り当てられていない ・ライセンス残数 0 ライセンスが割り当てられていなく、ライセンスの残数が 0 になっている ABM で「App とブック」ライセンスを購入するか、不要な「App とブック」ライセンスを機器から外して、ライセンス数を確保し、再度割り当てを行ってください。
3	［レポート作成］	クリックすると、レポート作成が開始されます。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 「画面（レポート作成結果）」239 ページ レポート作成に時間がかかる場合があります。

◆画面（レポート作成結果）

表示操作　［機器］→［CSV をダウンロード］→［機器レポート］→［レポート作成］

項番	項目	説明
1	［レポート更新］	対象や抽出条件を変更してからクリックすると、変更した条件でレポートを再作成できます。
2	［CSV ダウンロード］	クリックすると、現在のレポート作成結果の CSV ファイルをダウンロードします。 レポート作成結果が CSV ファイルに保存されるときの文字コードが、日本語環境では Shift-JIS（CP932）、その他の環境では UTF-8 です。
3	機器数	レポートした機器数が表示されます。
4	更新日時	レポートの更新日時が表示されます。
5	（レポート作成結果）	対象の機器レポートの一覧が表示されます。 レポートに表示される項目は、設定された条件や機器カスタム項目によって異なります。詳細については、以下を参照してください。 「レポート作成結果の項目」240 ページ

◆レポート作成結果の項目

項目名	説明
[I]または[I:から始まる項目	端末もしくは本製品の情報です。 本製品の情報は、以下のとおりです。 ・ユーザー氏名 ・ユーザー社員番号 ・エージェントバージョン ・ゾーン ・ポリシー
[S]または[S:から始まる項目	本製品で設定した情報です。
[F]から始まる項目	本製品で設定した情報です。
[G]から始まる項目	本製品で設定した情報です。
[C]から始まる項目	本製品で設定した情報です。

4.11.2 アプリケーションレポート

端末にインストールされているアプリを一覧で確認します。作成したアプリケーションレポートは、CSV ファイルとして出力することができます。

画面

画面（App Configuration の設定値を対象にする場合）

画面（レポート作成結果）

また、対象を指定すると、以下のようなアプリを確認できます。

●アプリケーション検知を設定している場合は、「インストール推奨アプリケーション」に設定はされているが、まだインストールされていないアプリや、「インストール非推奨アプリケーション」に設定はされているが、すでにインストールされているアプリの一覧を閲覧することができます。

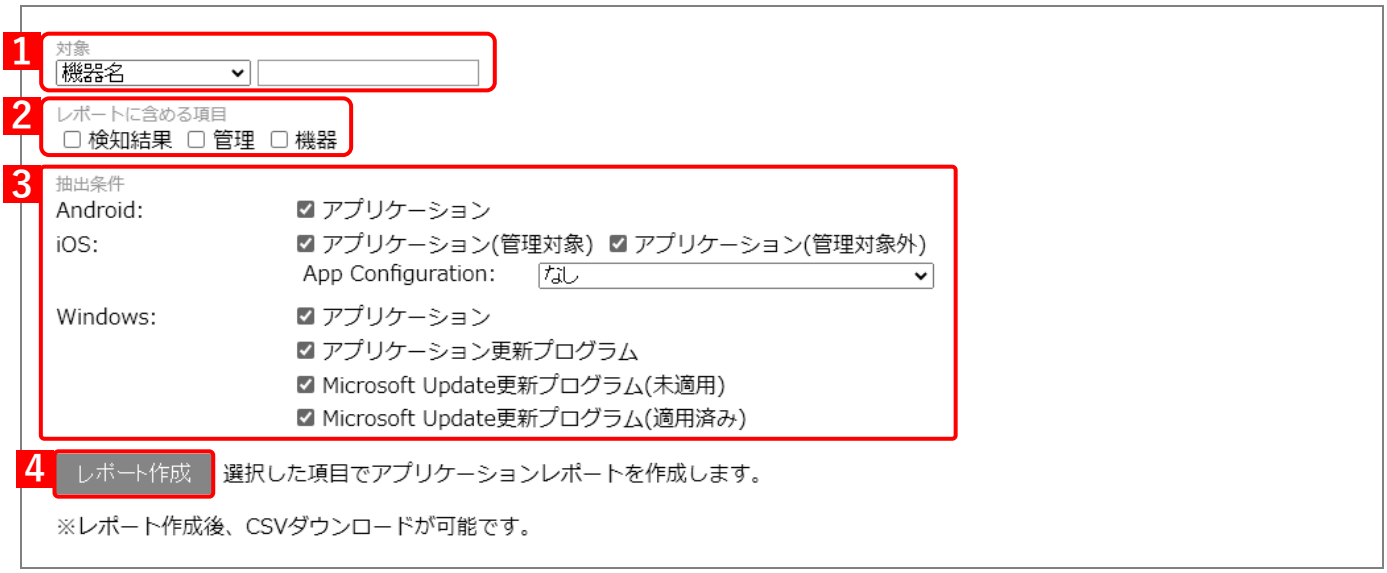
●「アプリケーション名」、「パッケージ名」を対象に指定してレポート作成を行うと、脆弱性が明らかになったアプリなどのインストール数を確認することができます。

アプリケーションレポートの作成には、時間がかかることがあります。そのような場合は、アプリケーションレポート（高速版）をすると、抽出条件や出力項目が少なくなりますが、時間がかからず CSV ファイルを出力することができます。

「アプリケーションレポート（高速版）」245 ページ

◆画面

表示操作　［機器］→［CSV をダウンロード］→［アプリケーションレポート］



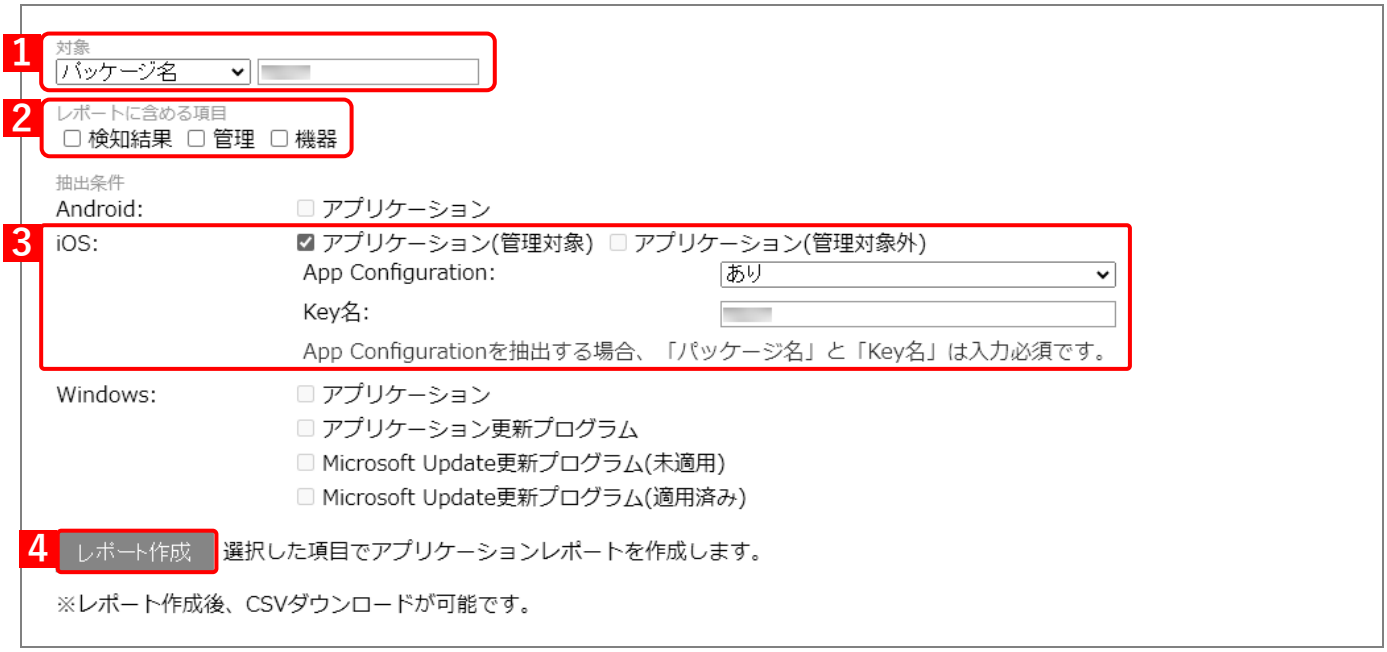
項番	項目	説明
1	対象	アプリケーションレポートの対象の種別を指定します。リストボックスから、「機器名」、「アプリケーション名」、「パッケージ名」「機器分類」、「ユーザー分類」を指定できます。右側のテキストボックスにキーワードを指定すると、指定した種別で、キーワードに該当するアプリを対象にしてレポートを作成します。
2	レポートに含める項目	レポートに含めたい項目にチェックを入れます。 ●検知結果 アプリケーション検知結果を出力したい場合に、チェックを入れます。 ●管理 管理している機器の情報をレポートに含める。 ●機器 機器に設定している情報を含める。

項番	項目		説明
3	抽出条件		OS ごとに抽出条件を設定します。
		Android	Android のアプリを対象にする場合は、［アプリケーション］にチェックを入れます。
		iOS	iOS のアプリを対象にする場合は、［アプリケーション（管理対象）］、［アプリケーション（管理対象外）］のいずれか、または両方にチェックを入れます。 iOS 端末にインストールされているアプリの App Configuration の設定値を対象にする場合は、「App Configuration」のリストボックスから［あり］を選択します。詳細については、以下を参照してください。 「画面（App Configuration の設定値を対象にする場合）」243 ページ
		Windows	Windows のアプリを対象にする場合は、必要に応じて、以下の項目にチェックを入れます。 ● ［アプリケーション更新プログラム］ ● ［Microsoft Update 更新プログラム（未適用）］ ● ［Microsoft Update 更新プログラム（適用済み）］
4	［レポート作成］		クリックすると、レポート作成が開始されます。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 「画面（レポート作成結果）」244 ページ レポート作成に時間がかかる場合があります。

◆画面（App Configuration の設定値を対象にする場合）

表示操作　［機器］→［CSV をダウンロード］→［アプリケーションレポート］→抽出条件 iOS の App Configuration［あり］を選択

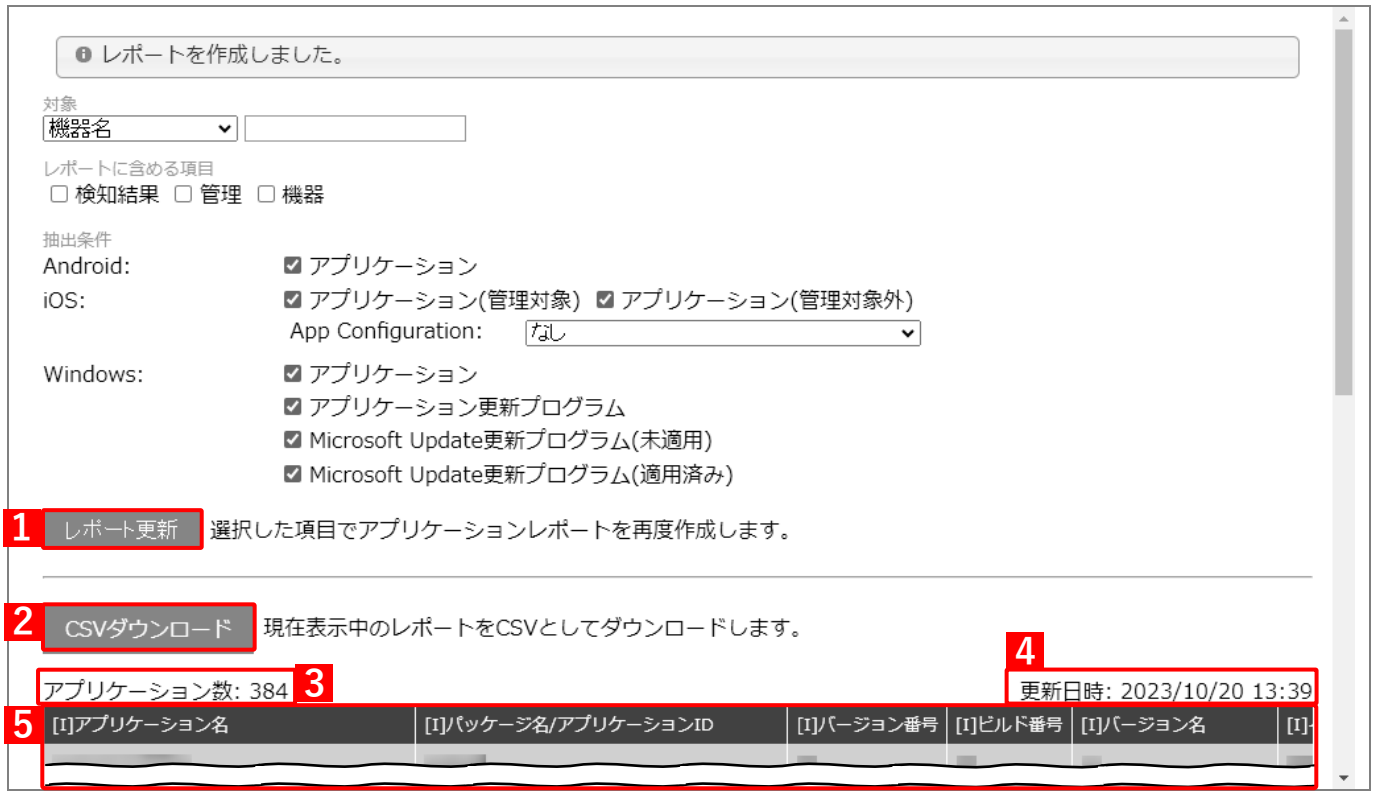
iOS 端末にインストール済みの管理対象アプリのみ出力します。



項番	項目	説明
1	対象	パッケージ名を入力します。 パッケージ名が入力されていないと、項番 4［レポート作成］はクリックできません。 項番 3「抽出条件」の「App Configuration」のリストボックスから［あり］を選択すると、［パッケージ名］のみ対象になります。 完全一致するものが抽出対象です。
2	レポートに含める項目	レポートに含めたい項目にチェックを入れます。 ●検知結果 アプリケーション検知結果を出力したい場合に、チェックを入れます。 ●管理 管理している機器の情報をレポートに含める。 ●機器 機器に設定している情報を含める。
3	抽出条件	
	iOS	以下の項目を設定します。 ●［アプリケーション(管理対象)］にチェックを入れます。 ●「App Configuration」のリストボックスから［あり］を選択します。 ●Key 名を入力します。 Key 名が入力されていないと、項番 4［レポート作成］はクリックできません。 完全一致するものが抽出対象です。
4	［レポート作成］	クリックすると、レポート作成が開始されます。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 「画面（レポート作成結果）」244 ページ レポート作成に時間がかかる場合があります。

◆画面（レポート作成結果）

表示操作　［機器］→［CSV をダウンロード］→［アプリケーションレポート］→［レポート作成］



項番	項目	説明
1	［レポート更新］	対象や抽出条件を変更してからクリックすると、変更した条件でレポートを再作成できます。
2	［CSV ダウンロード］	クリックすると、現在のレポート作成結果の CSV ファイルをダウンロードします。 レポート作成結果が CSV ファイルに保存されるときの文字コードが、日本語環境では Shift-JIS（CP932）、その他の環境では UTF-8 です。
3	アプリケーション数	レポートしたアプリの件数が表示されます。 「レポートに含める項目」で「検知結果」にチェックを入れてレポートを作成した場合は、以下の項目が表示されます。 ・全〇件 レポートしたすべてのアプリの件数が表示されます。リンクをクリックすると、すべてのアプリを表示します。 ・推奨〇件 アプリケーション検知で「推奨アプリケーション」に設定されているアプリの件数が表示されます。インストールされているアプリだけでなく、「推奨アプリケーション」に設定されているが、まだインストールされていないアプリも表示され、「バージョン番号」に「未インストール」と表示されます。リンクをクリックすると、対象のアプリだけが表示されます。 ・非推奨〇件 アプリケーション検知で「非推奨アプリケーション」に設定されているアプリで機器にインストールされているアプリの件数が表示されます。リンクをクリックすると、対象のアプリだけが表示されます。
4	更新日時	レポートの更新日時が表示されます。
5	（レポート作成結果）	対象のアプリケーションレポートの一覧が表示されます。 レポートに表示される項目は設定された条件によって異なります。

4.11.3 アプリケーションレポート（高速版）

「パッケージ名」をレポートの対象にして、アプリケーションレポートを CSV ファイルとして出力します。

画面

画面（App Configuration の設定値を対象にする場合）

画面（出力範囲選択）

端末にインストールされているアプリの以下の情報を一覧で確認することができます。

●アプリケーション名

●パッケージ名/アプリケーション ID

●バージョン番号

●ビルド番号（※1）

●バージョン名（※2）

●インストール日時（※3）

●アップデート日時（※2）

●機器名

●App Configuration Key（※4）

●App Configuration Value（※4）

●App Configuration 最終取得日（※4）

※1：iOS のアプリのみ出力されます。

※2：Android のアプリのみ出力されます。

※3：Android と Windows のアプリのみ出力されます。

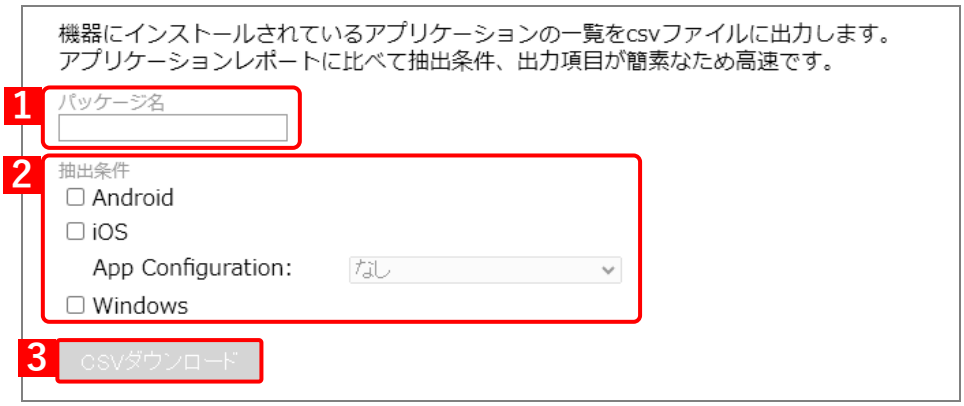
※4：iOS の「App Configuration」ありの場合のみ出力されます。

上記以外の情報を確認したい場合は、時間がかかりますが、アプリケーションレポートを利用してください。

「アプリケーションレポート」241 ページ

◆画面

表示操作　［機器］→［CSV をダウンロード］→［アプリケーションレポート（高速版）］

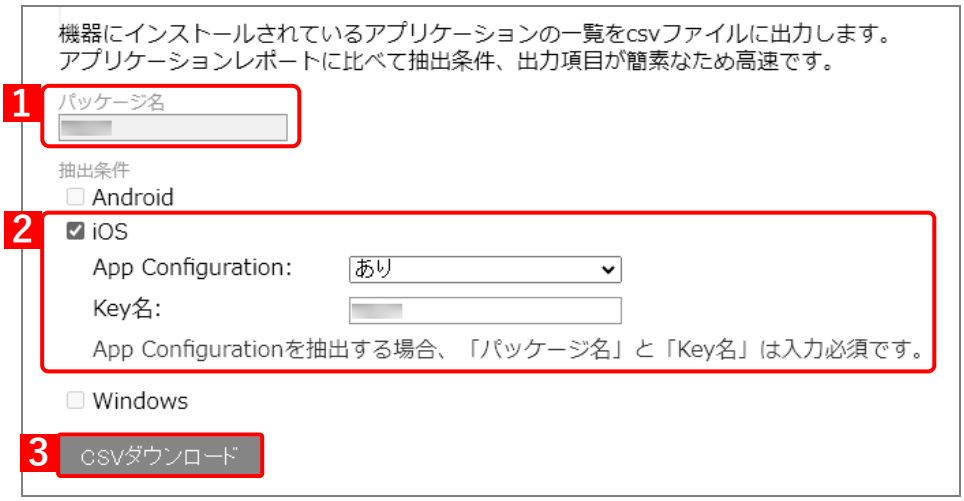


項番	項目	説明
1	パッケージ名	対象のアプリのパッケージ名を入力します。 パッケージ名は、最大 255 文字まで入力できます。 256 文字以上入力して、項番 3［CSV ダウンロード］をクリックすると、エラーメッセージが表示され、CSV ファイルは出力されません。 検索方式は、部分一致です。 入力したパッケージ名の一部分でも一致したアプリが抽出されます。 パッケージ名が空白の場合は、すべてのアプリが対象になります。
2	抽出条件	対象の OS を設定します。 ●Android ●iOS iOS 端末にインストールされているアプリの App Configuration の設定値を対象にする場合は、「App Configuration」のリストボックスから［あり］を選択します。詳細については、以下を参照してください。 「画面（App Configuration の設定値を対象にする場合）」246 ページ ●Windows 1 つ以上設定していないと、項番 3［CSV ダウンロード］をクリックできません。
3	［CSV ダウンロード］	クリックすると、CSV ファイルがダウンロードされます。 対象のアプリが 100,000 件を超える場合は、出力範囲選択画面が表示されます。 「画面（出力範囲選択）」247 ページ CSV ファイルの文字コードは、日本語環境で Shift-JIS（CP932）、その他の環境で UTF-8 です。

◆画面（App Configuration の設定値を対象にする場合）

表示操作　**［機器］→［CSV をダウンロード］→［アプリケーションレポート（高速版）］→抽出条件 iOS にチェックを入れる→App Configuration［あり］を選択**

iOS 端末にインストール済みの管理対象アプリのみ出力します。



項番	項目	説明
1	パッケージ名	アプリのパッケージ名を 255 文字以内で入力します。 パッケージ名が 256 文字以上入力された状態で項番 3［CSV ダウンロード］をクリックすると、エラーメッセージが表示され、CSV ファイルは出力されません。 パッケージ名が入力されていないと、項番 3［CSV ダウンロード］はクリックできません。 完全一致するものが抽出対象です。
2	抽出条件	以下の項目を設定します。 ●［iOS］にチェックを入れます。 ●「App Configuration」のリストボックスから［あり］を選択します。 ●Key 名を入力します。 Key 名が 256 文字以上入力された状態で項番 3［CSV ダウンロード］をクリックすると、エラーメッセージが表示され、CSV ファイルは出力されません。 Key 名が入力されていないと、項番 3［CSV ダウンロード］はクリックできません。 完全一致するものが抽出対象です。
3	［CSV ダウンロード］	クリックすると、CSV ファイルがダウンロードされます。 対象のアプリが 100,000 件を超える場合は、出力範囲選択画面が表示されます。 「画面（出力範囲選択）」247 ページ CSV ファイルの文字コードは、日本語環境で Shift-JIS（CP932）、その他の環境で UTF-8 です。

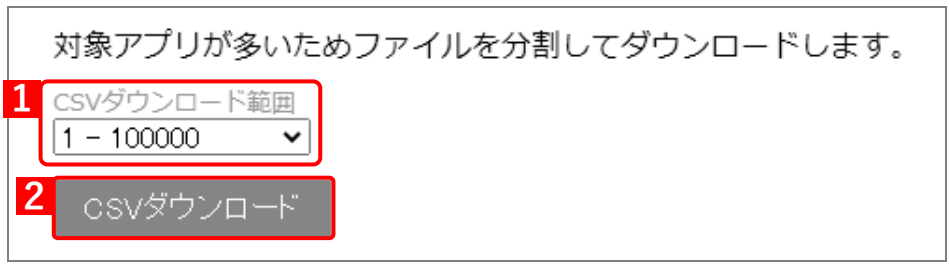
◆画面（出力範囲選択）

対象のアプリが 100,000 件を超える場合は、出力範囲選択画面が表示されます。範囲を分割して CSV ファイルに出力します。

タイミングによっては、出力データに増減が発生することがあります。

- 100,000 件を超える場合は、範囲を変更している間に同期などにより、データが増減すると出力されるデータにずれが発生する可能性があります。
- 表示されるはずのデータが表示されない場合は、再度他の範囲のファイルをダウンロードし直してください。
- 同じデータが複数の CSV ファイルに表示されていても、重複してデータが保存されているわけではありません。別途操作は必要ありません。
- 出力されたデータが予想と異なっていた場合は、再度「アプリケーションレポート（高速版）」からダウンロードし直すと解消されます。

表示操作　**［機器］→［CSV をダウンロード］→［アプリケーションレポート（高速版）］→［CSV ダウンロード］**



項番	項目	説明
1	CSV ダウンロード範囲	抽出結果から CSV ファイルにダウンロードしたい範囲（行数）を選択します。
2	［CSV ダウンロード］	クリックすると、項番 1「CSV ダウンロード範囲」で選択した範囲の CSV ファイルがダウンロードされます。 CSV ファイルの文字コードは、日本語環境で Shift-JIS（CP932）、その他の環境で UTF-8 です。

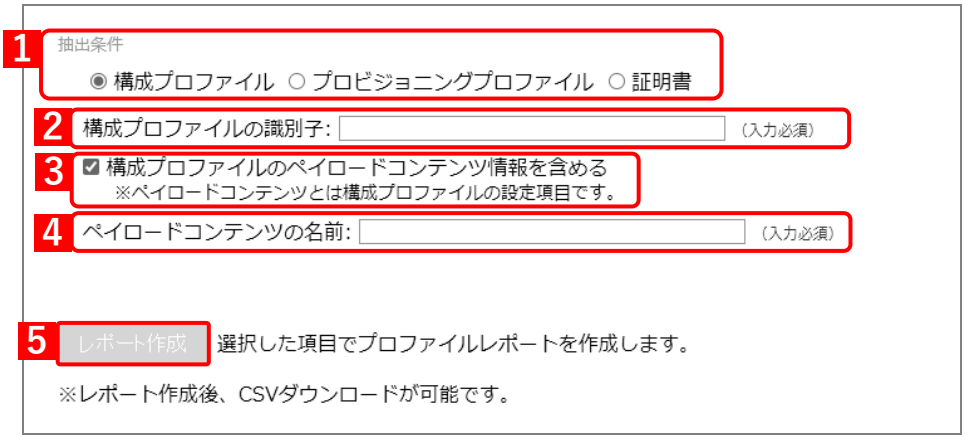
4.11.4 プロファイルレポート

iOS 端末にインストールされている構成プロファイル、プロビジョニングプロファイル、証明書を一覧で確認します。作成したプロファイルレポートは、CSV ファイルとして出力することができます。

画面（［構成プロファイル］選択時）
画面（［プロビジョニングプロファイル］選択時）
画面（［証明書］選択時）
画面（レポート作成結果）

◆画面（［構成プロファイル］選択時）

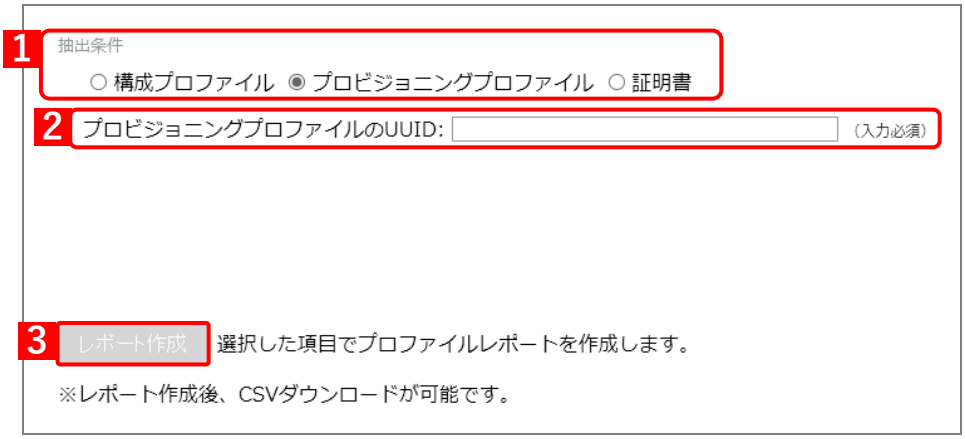
表示操作　［機器］→［CSV をダウンロード］→［プロファイルレポート］



項番	項目	説明
1	抽出条件	［構成プロファイル］を選択します。
2	構成プロファイルの識別子	対象の iOS 端末の構成プロファイル詳細画面に表示される UUID の値を入力します。 「画面（構成プロファイルの詳細）」163 ページ 構成プロファイル識別子を入力していないと、項番 5［レポート作成］がクリックできません。
3	［構成プロファイルのペイロードコンテンツ情報を含める］	構成プロファイルのペイロードコンテンツ情報を含める場合は、チェックを入れます。 チェックを入れると、項番 4「ペイロードコンテンツの名前」が表示されます。
4	ペイロードコンテンツの名前	対象の iOS 端末の構成プロファイル詳細画面に表示されるペイロードコンテンツの名前の値を入力します。 「画面（構成プロファイルの詳細）」163 ページ ペイロードコンテンツの名前を入力していないと、項番 5［レポート作成］がクリックできません。 項番 3［構成プロファイルのペイロードコンテンツ情報を含める］にチェックを入れると表示されます。
5	［レポート作成］	クリックすると、レポート作成が開始します。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 「画面（レポート作成結果）」251 ページ レポート作成に時間がかかる場合があります。

◆画面（［プロビジョニングプロファイル］選択時）

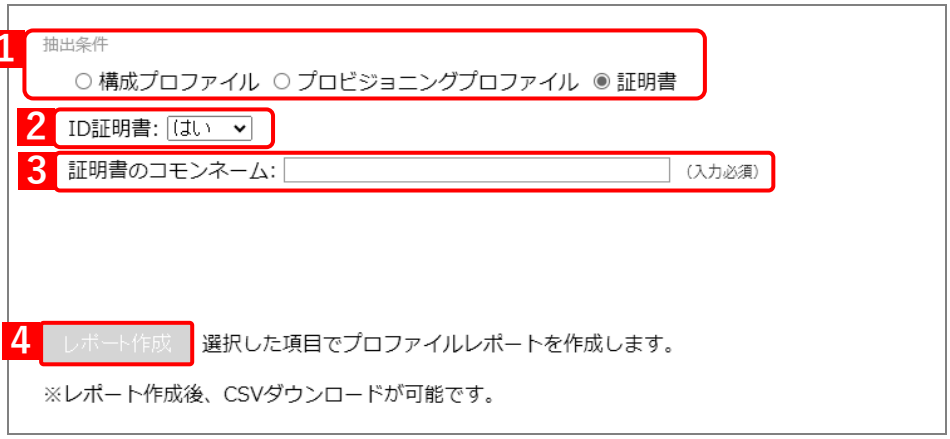
表示操作　［機器］→［CSV をダウンロード］→［プロファイルレポート］→抽出条件から［プロビジョニングプロファイル］を選択



項番	項目	説明
1	抽出条件	［プロビジョニングプロファイル］を選択します。
2	プロビジョニングプロファイルの UUID	対象の iOS 端末のプロビジョニングプロファイル詳細画面に表示される UUID の値を入力します。 ☞「画面（プロビジョニングプロファイルの詳細）」164 ページ プロビジョニングプロファイルの UUID を入力していないと、項番 3［レポート作成］がクリックできません。
3	［レポート作成］	クリックすると、レポート作成が開始します。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 ☞「画面（レポート作成結果）」251 ページ レポート作成に時間がかかる場合があります。

◆画面（［証明書］選択時）

表示操作　［機器］→［CSV をダウンロード］→［プロファイルレポート］→抽出条件から［証明書］を選択



項番	項目	説明
1	抽出条件	［証明書］を選択します。
2	ID 証明書	リストボックスから［はい］または［いいえ］を選択します。

項番	項目	説明
3	証明書のコモンネーム	対象の iOS 端末のプロファイル画面に表示される証明書のコモンネームの値を入力します。 ☞「（情報－iOS）プロファイル」162 ページ 証明書のコモンネームを入力していないと、項番 4［レポート作成］がクリックできません。
4	［レポート作成］	クリックすると、レポート作成が開始します。レポート作成が完了すると、レポート結果が画面下部に一覧表示されます。 ☞「画面（レポート作成結果）」251 ページ レポート作成に時間がかかる場合があります。

◆画面（レポート作成結果）

表示操作　［機器］→［CSV をダウンロード］→［プロファイルレポート］→［レポート更新］

項番	項目	説明
1	［レポート更新］	抽出条件を変更してからクリックすると、変更した条件でレポートを再作成できます。
2	［CSV ダウンロード］	クリックすると、現在のレポート作成結果の CSV ファイルをダウンロードします。 CSV ファイルの文字コードは、日本語環境で Shift-JIS（CP932）、その他の環境で UTF-8 です。
3	機器数	レポートした機器の件数が表示されます。
4	更新日時	レポートの更新日時が表示されます。
5	（レポート作成結果）	対象のプロファイルレポートの一覧が表示されます。 レポートに表示される項目は設定された条件によって異なります。

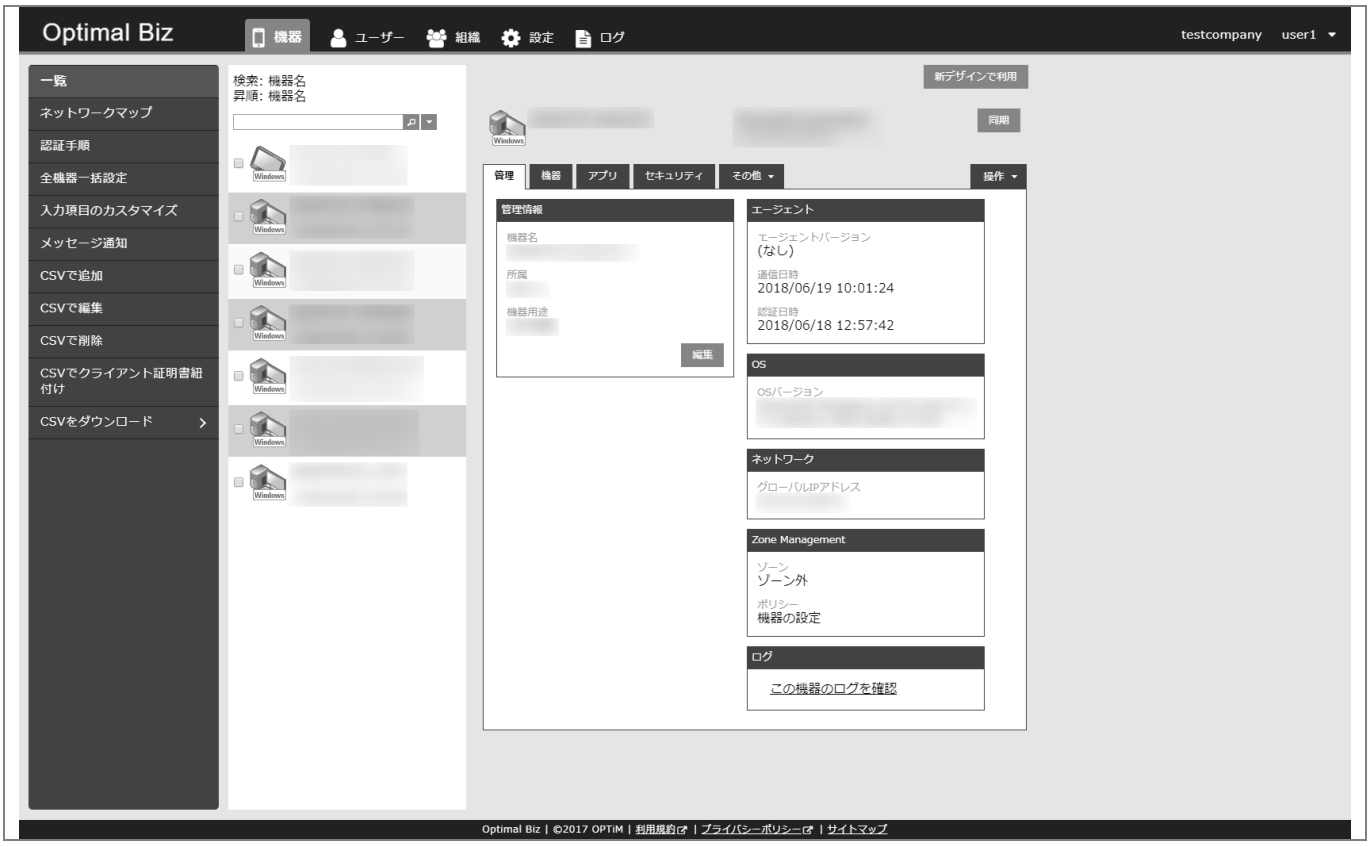
4.12 旧デザイン

注意

- ［機器］の［一覧］を旧デザインで表示して使用できますが、今後は使用できなくなる予定です。また、新しい機能が表示されない場合もあります。なるべく使用しないでください。

◆画面

表示操作　**［機器］→［一覧］→［旧デザインで利用］**



5 ユーザー

この章では、ヘッダーメニューの［ユーザー］画面に表示される、各種の設定について説明します。

5.1 一覧

［ユーザー］の［一覧］画面では、ユーザーの新規作成、情報確認、編集、削除のほか、ユーザーに対する「App とブック」ライセンスの付与や、アクセス制限、Android 端末へのアプリケーション配信の設定などを行うことができます。

ユーザーアカウントのユーザー種別が「管理者」権限を持つ場合は、「管理者」本人のユーザー種別を変更できません。また「操作者」権限を持つ場合は上位の「管理者」権限を持つユーザーの編集はできません。

◆画面

表示操作［ユーザー］→［一覧］

項番	名称	説明
1	検索／並び替え	● （A） 検索の対象項目が表示されます。 ● （B） 並び替えの対象項目が表示されます。 ● （C） 検索する場合は、検索するキーワードを（C）に入力し、をクリックします。検索後、すべてのユーザーを再表示するにはブラウザーを再読み込みする、または（C）を空欄にし、あらためて をクリックします。
2	［新規作成］	をクリックすると、項番【5】「ユーザー情報」に入力欄が表示されます。ユーザーの新規作成方法については、以下を参照してください。 ☞「［管理］タブ」257 ページ

項番	名称	説明
3	（その他の操作）	をクリックすると、以下のメニューを選択できます。 ●全てにチェックを入れる すべてのチェックボックスにチェックが入ります。 ●全てのチェックをはずす すべてのチェックボックスからチェックを外します。 ●検索対象 選択した以下の項目から検索を行います。 ・「ユーザー名」、「フリガナ」、「ユーザーID」、「メールアドレス」、「ユーザー種別」、「組織」、「登録した入力項目のカスタマイズ」 ●並び替え 昇順 選択した項目でユーザー一覧を昇順に並び替えます。 ・「ユーザー名」、「ユーザーID」、「メールアドレス」 ●並び替え 降順 選択した項目でユーザー一覧を降順に並び替えます。 ・「ユーザー名」、「ユーザーID」、「メールアドレス」 ●一括削除（※1） クリックして、確認画面で［OK］をクリックするとユーザー一覧にチェックボックスにチェックが入っているユーザーをまとめて削除します。
4	ユーザー一覧	登録されているユーザーの一覧が表示されます。 ●（D） 一括削除の対象にするユーザーにする場合にチェックを入れます。 ●（E） 「名前」が表示されます。 ●（F） 検索対象のユーザー情報（検索対象がユーザー名の場合はユーザー種別が表示されます）が表示されます。 ●（G） 並び替え対象のユーザー情報（並び替え対象がユーザー名の場合はメールアドレスが表示されます）が表示されます。
5	ユーザー情報	ユーザー一覧で選択したユーザーの情報が表示されます。
6	［操作］	クリックすると、以下のメニューが表示されます。 ●ロックアウト解除 このメニューは、ロックアウトしている（ログインに複数回失敗しログインできない状態）ユーザーだけに表示されます。クリックすると、ロックアウトの解除が行われ、ログインできるようになります。 なお、ロックアウトされたユーザーのアイコンは鍵付きの状態で表示されます。 「［操作］タブ」261 ページ 「アカウントポリシー」639 ページ ●削除（※1） 表示されているユーザーを削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。
7	［編集］	クリックすると、管理情報、パスワードの編集ができます。編集項目については、以下を参照してください。 「［管理］タブ」257 ページ

項番	名称	説明
8	［設定削除］	2 段階認証の設定を削除するとき、クリックします。 実行確認画面が表示されます。 ●OK 2 段階認証の設定を削除します。 ●キャンセル 2 段階認証の設定の削除を中止します。 ユーザーが 2 段階認証で使用する端末を紛失したときは、本画面で設定を削除してください。ユーザーは次回のログイン時に新しい端末で 2 段階認証の設定をしてください。

※1：ログイン中のユーザーは削除できません。また、チェックボックスも表示されません。

5.1.1 ［管理］タブ

ユーザーを新規に作成します。作成したユーザーは、端末の管理情報として利用されます。

また、ユーザーにはすべての操作ができる［管理者］から、管理サイトへのログインをできなくする［一般］まで、多様な権限を付与することができます。

画面（新規作成）

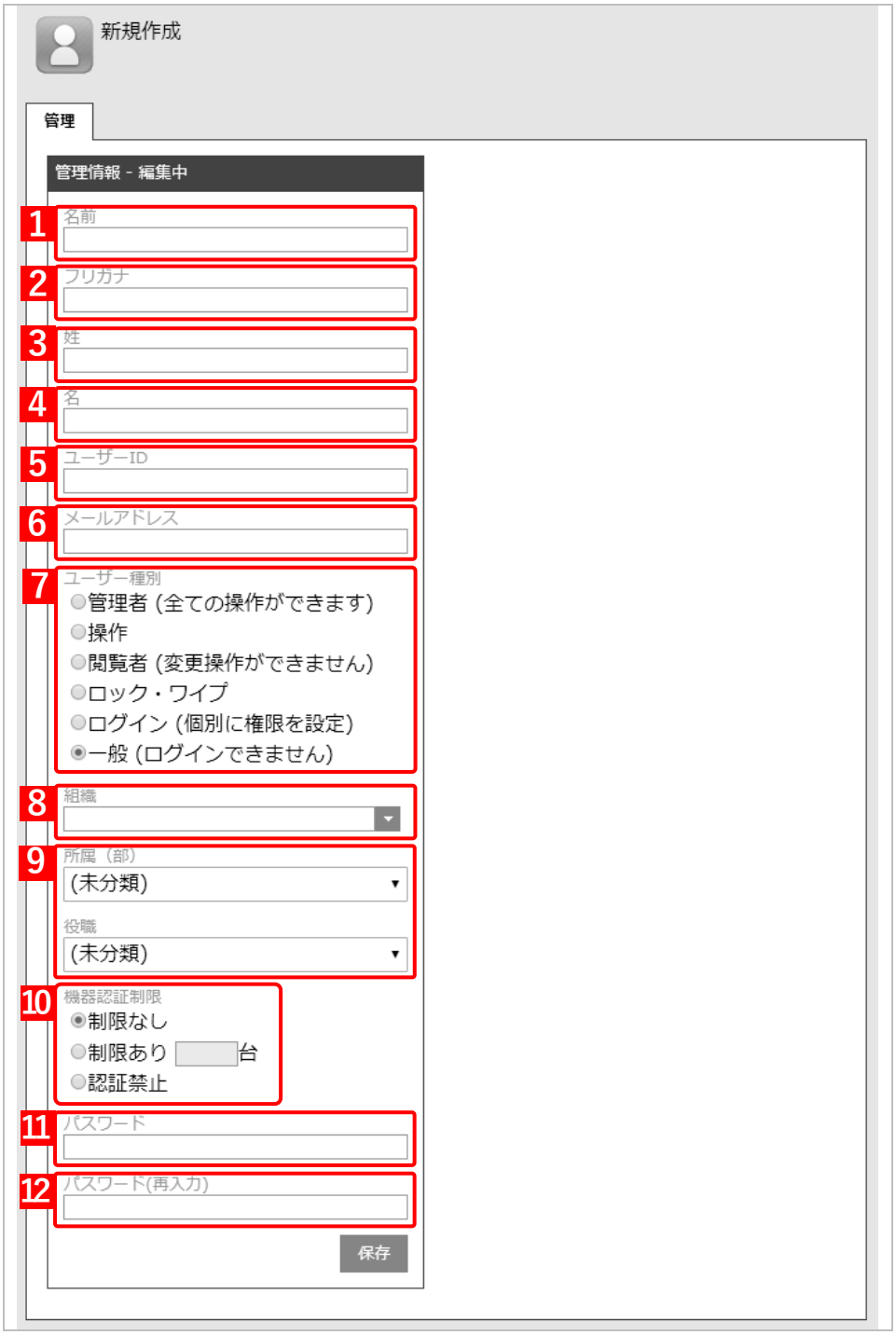
画面（編集）

ユーザーを作成すると、［「App とブック」設定］タブ、［アクセス制御］タブ、［その他］タブが表示されます。

◆画面（新規作成）

表示操作　［ユーザー］→［一覧］→ ＋

作成できるユーザー数は、契約によって異なります。



項番	名称	説明
1	名前	ユーザーの名称を 30 文字以内で入力します。重複はできません。名前を入力していない状態で［保存］をクリックすると「姓」と「名」に入力されている情報が「名前」に自動的に反映されます。そのとき、姓と名の間に半角スペースが入ります。 「名前」に入力がなく、「姓」と「名」にも入力がない場合、「名前」の入力を求められます。
2	フリガナ	フリガナを 30 文字以内で入力します。 半角カタカナで入力しても全角カタカナに変換され、全角空白は半角空白に変換されます。 「名前」、「姓」、「名」を入力しても、「フリガナ」は自動的に反映されません。手動で入力します。
3	姓	姓を 20 文字以内で入力します。
4	名	名を 20 文字以内で入力します。
5	ユーザーID	ユーザーID を 255 文字以内の半角英数字、半角記号で入力します。重複するユーザーID は登録できません。
6	メールアドレス	メールアドレスを 255 文字以内の半角英数字、半角記号で入力します。 「@」の前後にそれぞれ 1 文字以上入力してください。重複するメールアドレスは登録できません。
7	ユーザー種別	ユーザーに付与する権限を以下から選択します。 ユーザー種別により管理サイトの操作範囲が異なります。 編集時は、ログイン中のユーザーのユーザー種別は変更できません。 ●管理者 管理サイトのすべての操作を行えます。 ●操作 ロック・ワイプの操作およびロック・ワイプ設定内容の閲覧以外、管理サイトのすべての操作を行えます。 ●閲覧者 管理サイトの閲覧のみ行えます。新規作成、編集、削除などの変更操作はできません。 ●ロック・ワイプ ロック・ワイプの操作およびロック・ワイプ設定内容の閲覧、ユーザー情報の閲覧（位置情報を含む）、機器の管理情報の編集のみ行えます。ロック・ワイプ以外の機能についての情報の閲覧および編集は行えません。 ●ログイン 「ダッシュボード」と「個人設定」の閲覧、編集のみ行えます。主に「入力項目のカスタマイズ」を用いて追加権限を付与する場合に指定します。 「ダッシュボード」と「個人設定」の詳細については、以下を参照してください。 「ダッシュボード」37 ページ 「個人設定」49 ページ 「入力項目のカスタマイズ」271 ページ ●一般 管理サイトへのログインはできません。
8	組織	ユーザーに所属させる組織がある場合は、リストボックスから登録されている組織を選択します。 リストボックスで表示される組織は 100 までとなり、100 を超える（リストに表示されない）組織にユーザーを割り当てる場合の手順については、以下を参照してください。 「CSV で編集」279 ページ

項番	名称	説明
9	（カスタマイズ項目）	「入力項目のカスタマイズ」で分類や自由入力の項目を登録している場合に表示されます。 カスタマイズ項目の作成方法については、以下を参照してください。 「入力項目のカスタマイズ」271 ページ
10	機器認証制限	ユーザーが認証できる機器の制限を以下から選択します。 ●制限なし すべての機器を認証できます。 ●制限あり 選択した場合は、機器の台数は入力必須です。最大機器台数は 0 から 50,000 の間を半角数字で指定してください。すでにユーザーに紐づいている機器がある場合は、その台数以上の値を指定してください。 ●認証禁止 機器の認証はできません。
11	パスワード	ログインユーザーとして利用する場合には、パスワードを 4 文字から 32 文字以内の半角英数字、半角記号で入力します。 入力を省略するとランダムなパスワードが設定されますがパスワードは確認できないため、ログインユーザーとして利用する場合は、パスワードを設定してください。
12	パスワード(再入力)	確認のため、パスワードを再入力します。

◆画面（編集）

表示操作　**［ユーザー］→［一覧］→一覧から対象を選択→［管理］タブ→「管理情報」の［編集］**

表示操作　**［ユーザー］→［一覧］→一覧から対象を選択→［管理］タブ→「パスワード」の［編集］**

項番	名称	説明
1	管理情報	管理情報を編集します。詳細については、以下を参照してください。 ☞「画面（新規作成）」257 ページ
2	パスワード	パスワードを編集します。詳細については、以下を参照してください。 ☞「画面（新規作成）」257 ページ

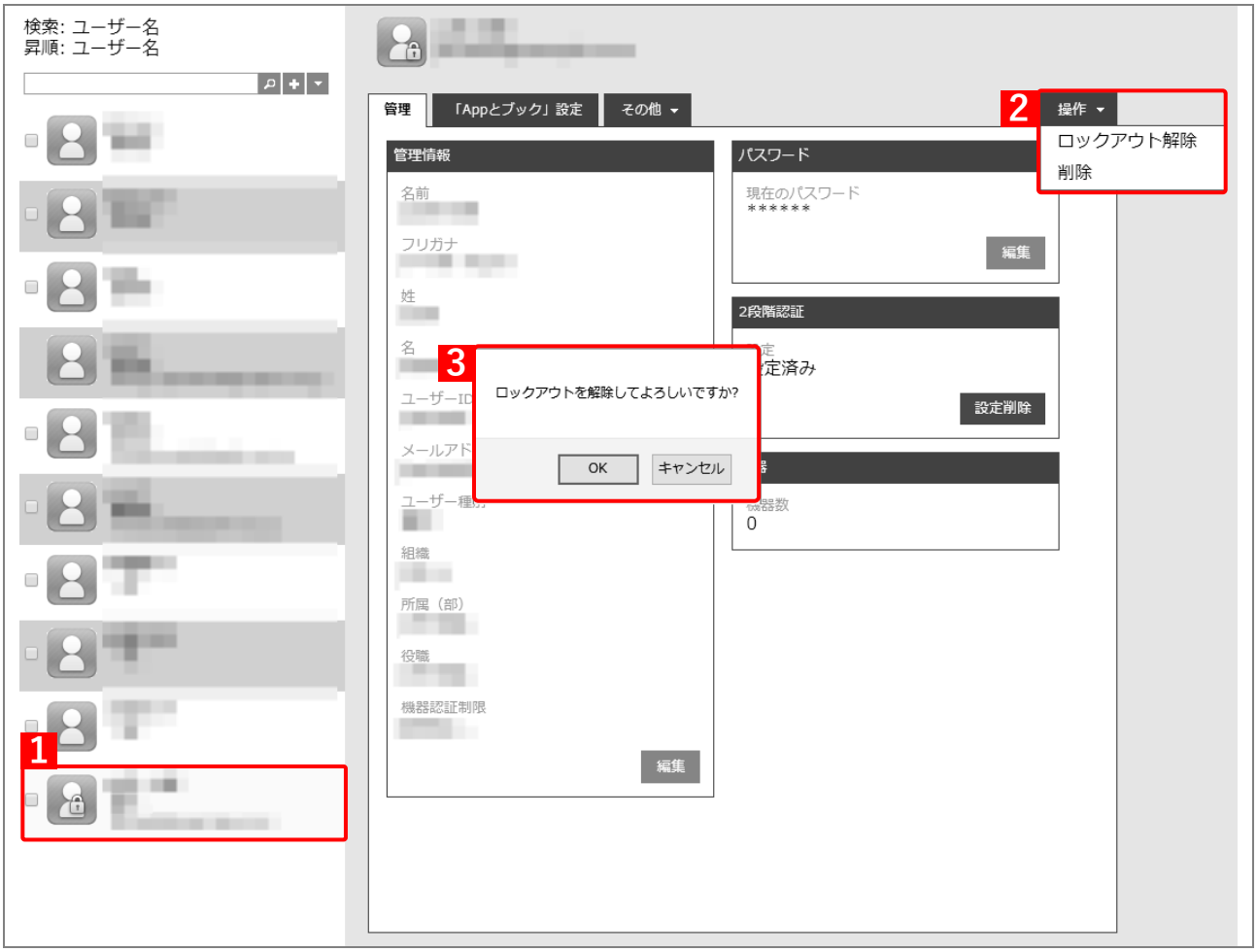
5.1.2 ［操作］タブ

ロックアウト状態（ログインに複数回失敗しログインできない状態）の解除や、ユーザーの削除を行うことができます。

ロックアウトの解除は、ロックアウトされたユーザー以外のユーザーがログインして操作してください。

◆画面（ロックアウトされたユーザーの解除）

表示操作 ［ユーザー］→［一覧］→一覧から対象（ロックアウト中のユーザー）を選択→［操作］→［ロックアウト解除］



項番	名称	説明
1	ユーザー一覧	対象とするユーザーをクリックします。
2	［操作］	クリックし、表示されたリストメニューから「ロックアウト解除」を選択します。 ロックアウトしていないユーザーは、「ロックアウト解除」は表示されません。
3	―	ロックアウトされたユーザーの解除について確認する画面です。 ●OK ユーザーのロックアウトを解除します。 ●キャンセル ユーザーのロックアウト解除を中断します。

5.1.3 ［「App とブック」設定］タブ

ユーザーに対する「App とブック」ライセンスの付与設定や、設定状況などを確認することができます。

［「App とブック」設定］タブでは、状態によって表示される項目が異なります。

- 画面（新規作成）
- 画面（App ライセンスの付与）
- 画面（ブックライセンスの付与）
- 画面（状況確認）
- 画面（ユーザー個別設定）
- 画面（機器の Apple ID 変更による再度参加依頼）

［「App とブック」設定］タブは、ユーザーを作成すると表示されます。

構成プロファイルアップロードで App Store を表示させないようにする制限項目（「App のインストールを許可」または「App Store からの App インストールを許可」）を有効にしていると、「App とブック」の参加依頼を完了できませんのでご注意ください。

◆画面（新規作成）

ユーザーに対する「App とブック」ライセンスの付与を行うための設定画面を、新規に表示します。

［「App とブック」ライセンス］のアカウント登録が必要です。

「「App とブック」ライセンス」514 ページ

ユーザーが所属している組織に、すでに「App とブック」設定が適用されている場合は、「App とブック」設定画面に組織で設定した「App とブック」の設定が表示されます。

「画面（ユーザー個別設定）」268 ページ

表示操作　［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ

項番	名称	説明
1	［新規作成］	クリックすると、ライセンス付与の画面が表示されます。ライセンス付与は、App ライセンスとブックライセンスがあります。それぞれの詳細については、以下を参照してください。 「画面（App ライセンスの付与）」263 ページ 「画面（ブックライセンスの付与）」265 ページ

◆画面（App ライセンスの付与）

ユーザーに対する App ライセンス付与の設定を行います。

本設定でユーザーに割り当てた App ライセンスは、「「App とブック」ライセンス」の［アプリケーション］タブで、「未割当数」としてカウントされます。

この状態では実際にライセンスは、付与されていません。ライセンスの付与については、以下を参照してください。

「アプリケーション配信」530 ページ

表示操作　**［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ→［新規作成］または［編集］→［アプリケーション］**

項番	名称	説明
1	テンプレート	「App とブック」設定のテンプレートを適用する場合は、リストボックスからテンプレートを選択して［適用］をクリックすると、テンプレートの内容が適用されて、「App とブック」設定が完了します。
2	「App とブック」管理配布登録	「App とブック」ライセンスと参加依頼の方法を設定します。 ●「App とブック」ライセンス 「App とブック」アカウントを選択します。 ●参加依頼 「App とブック」のアプリや書籍を配布するには、ユーザーの参加が必要です。「App とブック」への参加を求める確認画面をユーザーの端末に表示します。参加依頼の送信方法を以下の項目から選択します。 ・自動送信 自動で送信します。 ・手動送信 選択した場合、「参加依頼を送付する機器」に参加依頼を送付するデバイスをリストボックスから選択します。 ユーザーに機器が紐づいていない場合、「手動送信」は表示されません。 選択した送信方法は、変更することができません。
3	App ライセンス付与	（A）［アプリケーション］をクリックすると表示されます App ライセンスを割り当てるアプリを設定します。 ●アプリケーション名 をクリックして、リストボックスからアプリを選択します。 「App とブック」ライセンスに登録しているアプリが設定できます。画面に表示される件数は、「App とブック」ライセンスに登録しているアプリの数です。 「App とブック」設定が保存されたあとは、アプリの名前のリンクをクリックすると、iTunes Store の該当アプリの紹介ページを表示します。 ABM で購入したアプリの件数が表示されます。アプリは最大 300 件まで購入できます。

◆画面（ブックライセンスの付与）

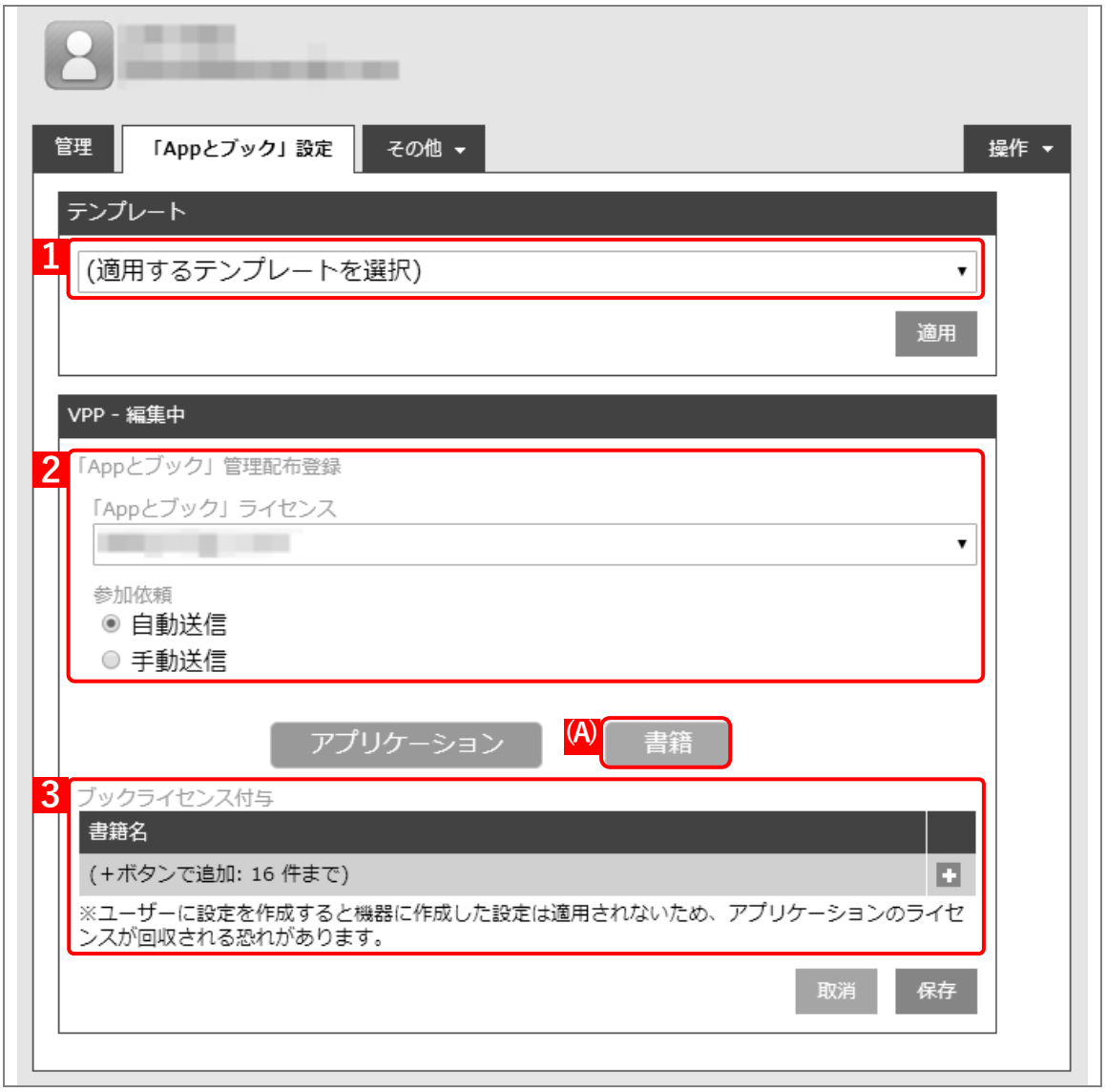
ユーザーに対するブックライセンス付与の設定を行います。

本画面でユーザーに割り当てたブックライセンスは、「「App とブック」ライセンス」の［書籍］タブで、「未割当数」としてカウントされます。

この状態では実際にライセンスは、付与されていません。ライセンスの付与については、以下を参照してください。

「［書籍］タブ」519 ページ

表示操作　**［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ→［新規作成］または［編集］→［書籍］**

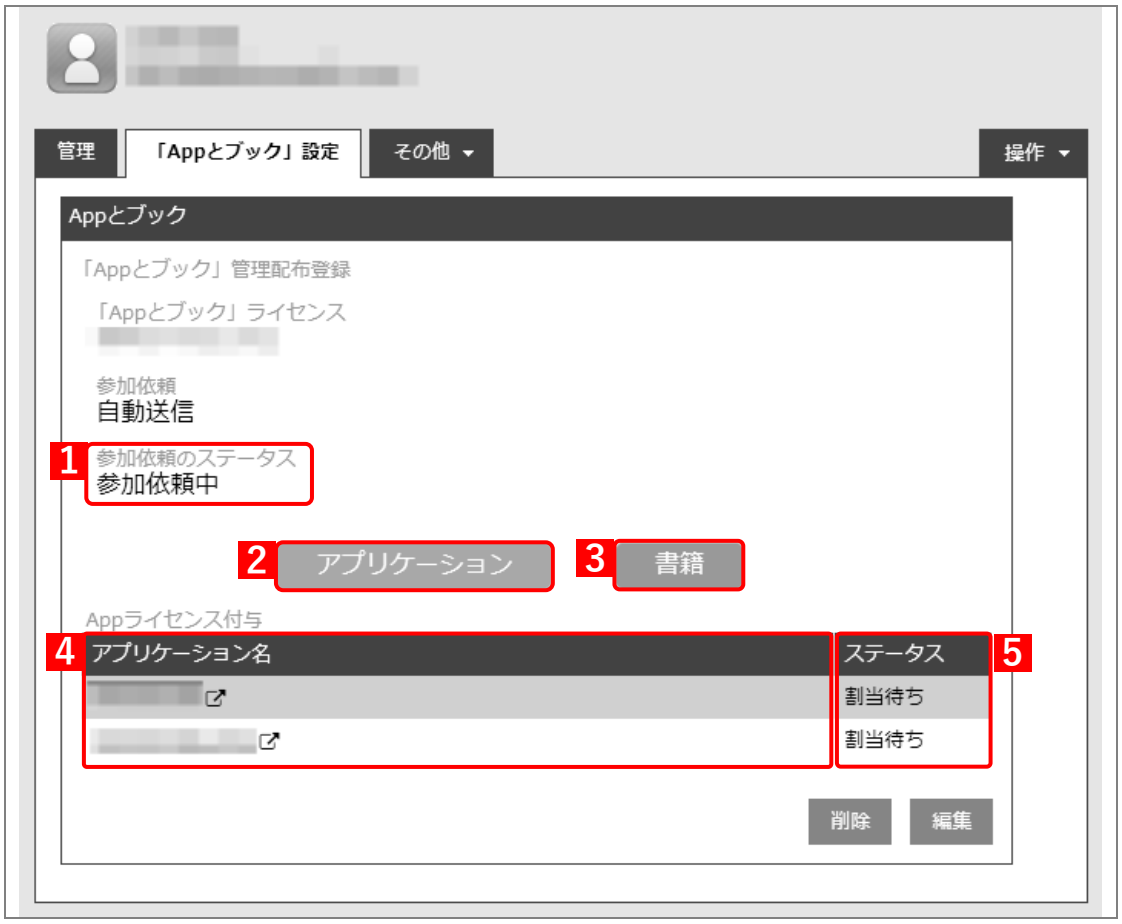


項番	名称	説明
1	テンプレート	ユーザーに「App とブック」テンプレートを適用します。
2	「App とブック」管理配布登録	「App とブック」ライセンスと参加依頼の方法を設定します。 ●「App とブック」ライセンス 「App とブック」アカウントを選択します。 ●参加依頼 「App とブック」のアプリや書籍を配布するには、ユーザーの参加が必要です。「App とブック」への参加を求める確認画面をユーザーの端末に表示します。参加依頼の送信方法を以下の項目から選択します。 ・自動送信 自動で送信します。 ・手動送信 選択した場合、「参加依頼を送付する機器」に参加依頼を送付するデバイスをリストボックスから選択します。 ユーザーに機器が紐づいていない場合、「手動送信」は表示されません。
3	ブックライセンス付与	（A）［書籍］をクリックすると表示されます。 ブックライセンスを割り当てる書籍を設定します。 ●書籍名 をクリックして、リストボックスから書籍を選択します。 「App とブック」ライセンスに登録している書籍が設定できます。画面に表示される件数は、「App とブック」ライセンスに登録している書籍の数です。 「App とブック」設定が保存されたあとは、書籍の名前のリンクをクリックすると、iTunes Store の該当書籍の紹介ページを表示します。 ABM で購入した書籍の件数が表示されます。書籍は最大 300 件まで購入できます。

◆画面（状況確認）

「App とブック」設定の参加依頼のステータス、ライセンス付与したアプリや書籍のステータスを確認できます。

表示操作　［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ



項番	名称	説明
1	参加依頼のステータス	参加依頼の現在のステータスが表示されます。
2	［アプリケーション］	クリックすると App ライセンス付与の割り当て状況を確認できます。
3	［書籍］	クリックすると書籍ライセンス付与の割り当て状況を確認できます。
4	アプリケーション名／書籍名	アプリ名や書籍名をクリックすると、iTunes Store の該当アプリや書籍の紹介ページを開くことができます。
5	ステータス	現在のライセンス付与の割り当て状況が表示されます。 ●割当済 ライセンスが割り当てられている ●割当待ち ライセンスが割り当てられていない ●ライセンス残数 0 ライセンスが割り当てられておらず、ライセンスの残数が 0 になっている ABM で「App とブック」ライセンスを購入するか、不要な「App とブック」ライセンスを機器、ユーザー、組織から外して、再度割り当てを行ってください。

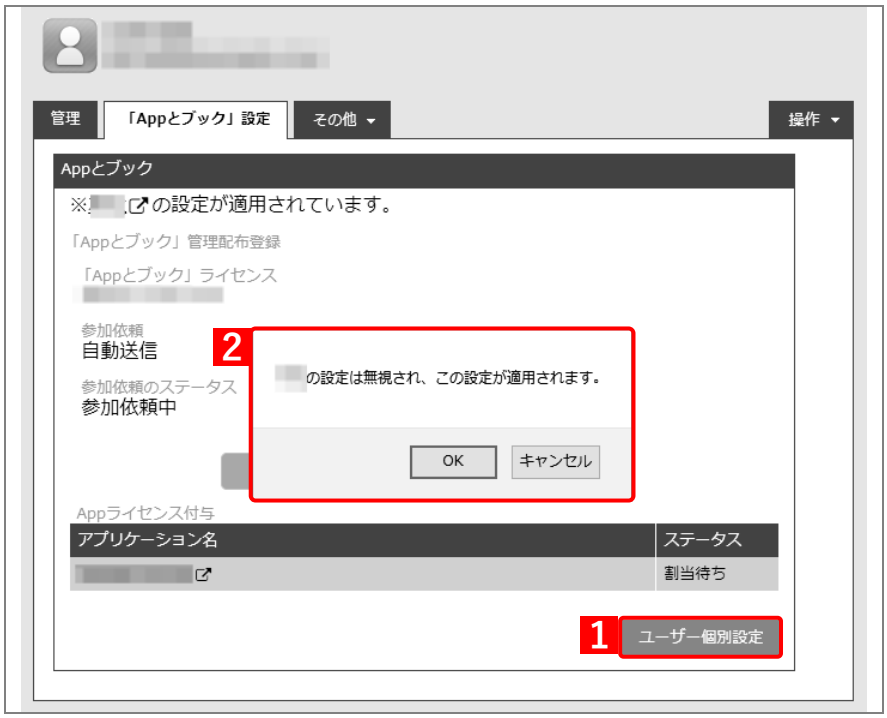
◆画面（ユーザー個別設定）

ユーザーが所属している組織で「App とブック」の設定が行われている場合は、組織で設定した「App とブック」設定が表示されます。

そのため、組織の設定を無視してユーザー個別の「App とブック」を設定したい場合は、本設定を行います。

［ユーザー個別設定］は、ユーザーが所属している組織で「App とブック」設定が行われている場合に表示されます。

表示操作　［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ



項番	名称	説明
1	［ユーザー個別設定］	組織の設定を無視してユーザー個別の設定を行う場合にクリックします。クリックすると、確認画面が表示されます。
2	メッセージボックス	ユーザー個別設定について確認する画面です。 ●OK ユーザー個別設定の画面に移動します。［OK］をクリックしたあとは、「App とブック」アプリおよび書籍のライセンスを付与します。詳細については、以下を参照してください。 ☞「画面（App ライセンスの付与）」263 ページ ☞「画面（ブックライセンスの付与）」265 ページ ●キャンセル ユーザー個別設定を中断します。

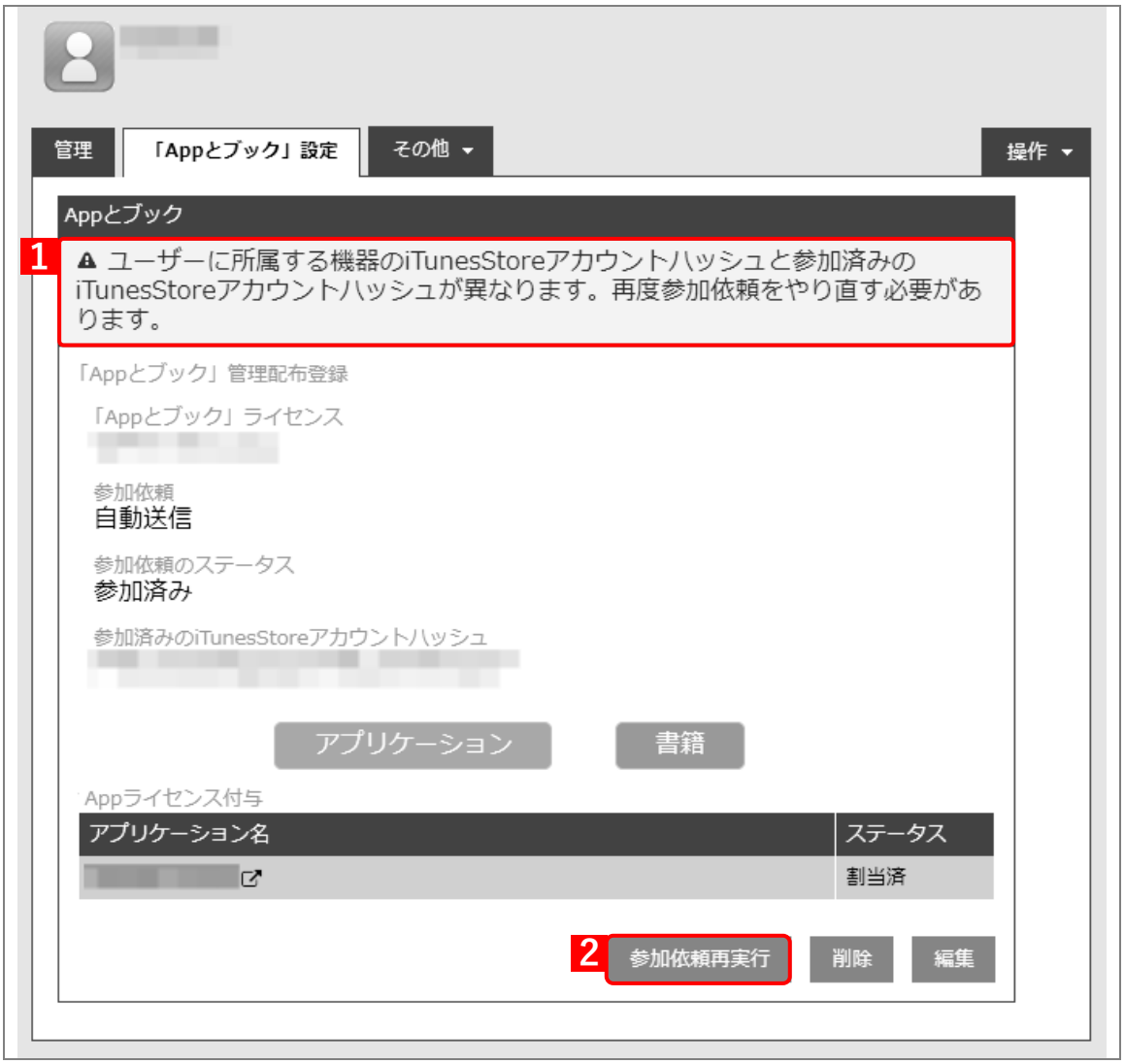
◆画面（機器の Apple ID 変更による再度参加依頼）

ユーザーに所属する端末の Apple ID が変更されると、ユーザーに所属する端末の iTunes Store アカウントハッシュと、参加済みの iTunes Store アカウントハッシュが異なるため、参加依頼をやり直すメッセージを表示します。

このメッセージが表示されると、「App とブック」アプリの追加配信ができなくなるため、［参加依頼再実行］をクリックして再度参加依頼を行い、あらためて iOS 端末側で「App とブック」アプリの割り当てを許可してください。

☞「［アプリケーション］タブ」518 ページ
☞「［書籍］タブ」519 ページ

表示操作　［ユーザー］→［一覧］→一覧から対象を選択→［「App とブック」設定］タブ



項番	名称	説明
1	警告メッセージ	端末に設定されている iTunes Store アカウントハッシュと参加済みの iTunes Store アカウントハッシュが異なる場合に表示されます。
2	［参加依頼再実行］	対象の iOS 端末に参加依頼を再度通知します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。

◆エラー一覧

文言	発生契機	対処方法
⚠ アプリケーションは重複しないものを入力してください。	「App ライセンス付与」欄で［+］でアプリを追加するときに、アプリ名が重複している。	重複しているアプリを設定から削除し、[保存] をクリックしてください。
⚠ 書籍は重複しないものを入力してください。	「ブックライセンス付与」欄で[+]で書籍を追加するときに書籍名が重複している。	重複している書籍を設定から削除し、[保存] をクリックしてください。

5.1.4 ［その他▼］タブ／設定

Android Enterprise 機能を利用したアプリの配信設定を、ユーザー単位で作成することができます。

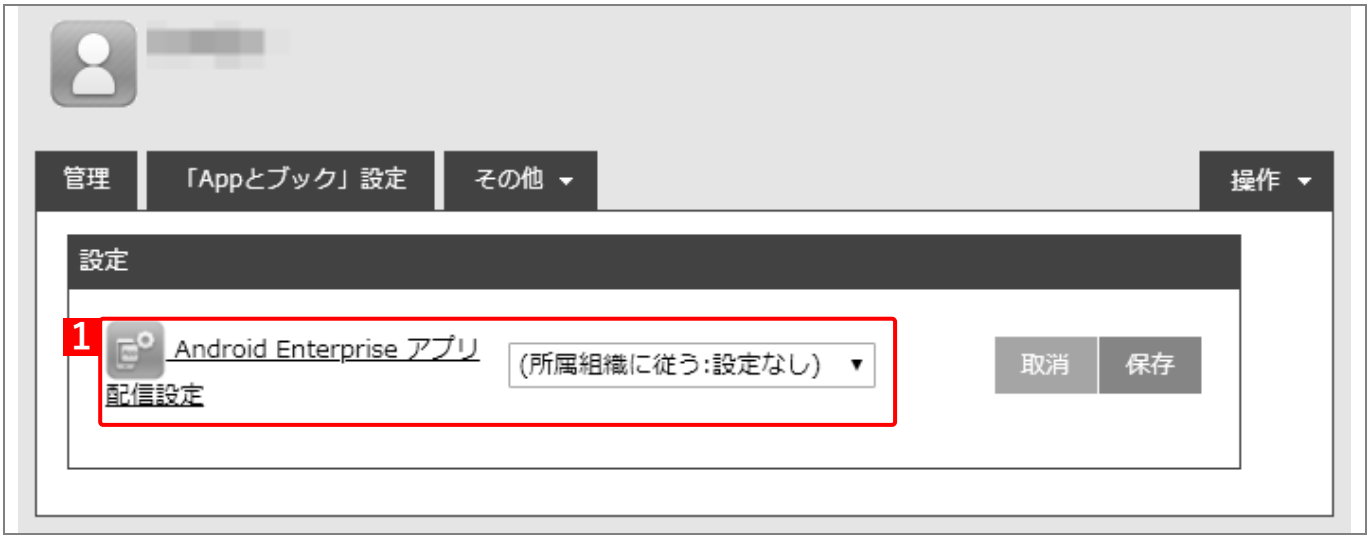
Android Enterprise の「アプリケーション配信」で、あらかじめ設定セットを作成してください。

「Android Enterprise／アプリケーション配信」327 ページ

本機能は Android Enterprise 機能を利用した Android 端末に利用できます。

◆画面

表示操作［ユーザー］→［一覧］→一覧から対象を選択→［その他▼］→［設定］→［編集］



項番	名称	説明
1	Android Enterprise アプリ配信設定	●Android Enterprise を利用する機器にアプリケーション配信の設定をリストボックスから選択します。

5.2 入力項目のカスタマイズ

ユーザーの［管理］タブに表示される管理情報に、任意の項目を追加することができます。

☞「［管理］タブ」257 ページ

追加できる項目には、リストボックスから項目を選択する［分類］と、テキストボックスに文字を直接書き込む［自由入力］があります。

また、［分類］で追加した項目は、ユーザーと機器を紐づけすると［全機器一括設定］画面に表示され、対象機器の選択条件として使用することもできます。

☞「機器の管理情報」67 ページ

☞「全機器一括設定」200 ページ

●追加した入力項目で一括設定を行う使用例

① ［分類］タブで、項目名に「社員種別」、グループ名に「正社員」と「契約社員」を設定して新規作成します。

☞「画面（新規作成）」273 ページ

② ユーザーの［管理］タブの管理情報に表示される「社員種別」の項目で、「正社員」と「契約社員」のいずれかを選択して保存します。

☞「［管理］タブ」257 ページ

③ 各機器の管理情報に表示されるラジオボタンから［ユーザー］を選択し、リストボックスから②で作成したユーザーを選択して、ユーザーと機器を紐づけます。

☞「機器の管理情報」67 ページ

④ 全機器一括設定で、「ユーザーの社員種別」をクリックして表示されるメニューから「正社員」または「契約社員」を選択し、機能を一括適用します。

☞「全機器一括設定」200 ページ

5.2.1 ［分類］タブ

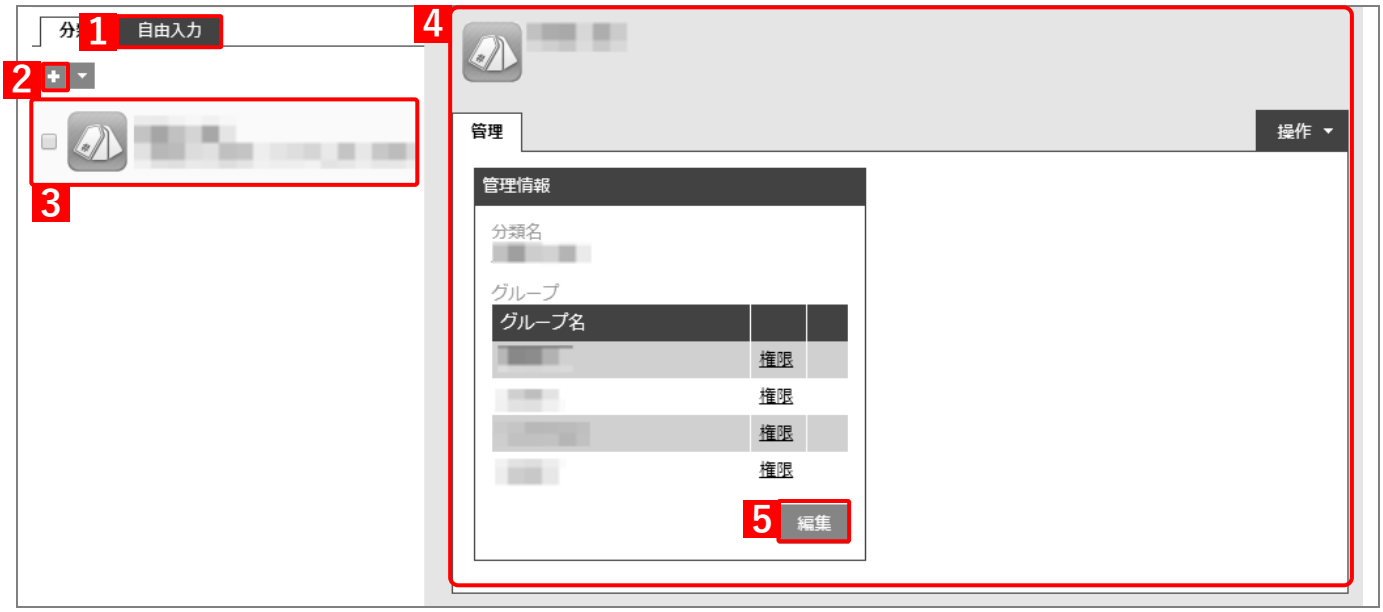
［入力項目のカスタマイズ］画面の［分類］タブ画面について説明します。

画面

画面（新規作成）

◆画面

表示操作　**［ユーザー］→［入力項目のカスタマイズ］→［分類］タブ**



項番	名称	説明
1	［自由入力］タブ	クリックすると、自由入力画面が表示されます。詳細については、以下を参照してください。 「［自由入力］タブ」275 ページ
2	✚	クリックすると、分類の新規作成画面が表示されます。分類は最大 50 件まで作成できます。カスタマイズ項目の新規作成については、以下を参照してください。 「画面（新規作成）」276 ページ
3	分類一覧	登録されているカスタマイズ項目の分類名が表示されます。
4	管理情報	分類一覧から選択した分類の登録内容が表示されます。
5	［編集］	クリックすると、登録されている入力項目のカスタマイズ情報を編集できます。編集できる項目は、新規作成時と同じです。

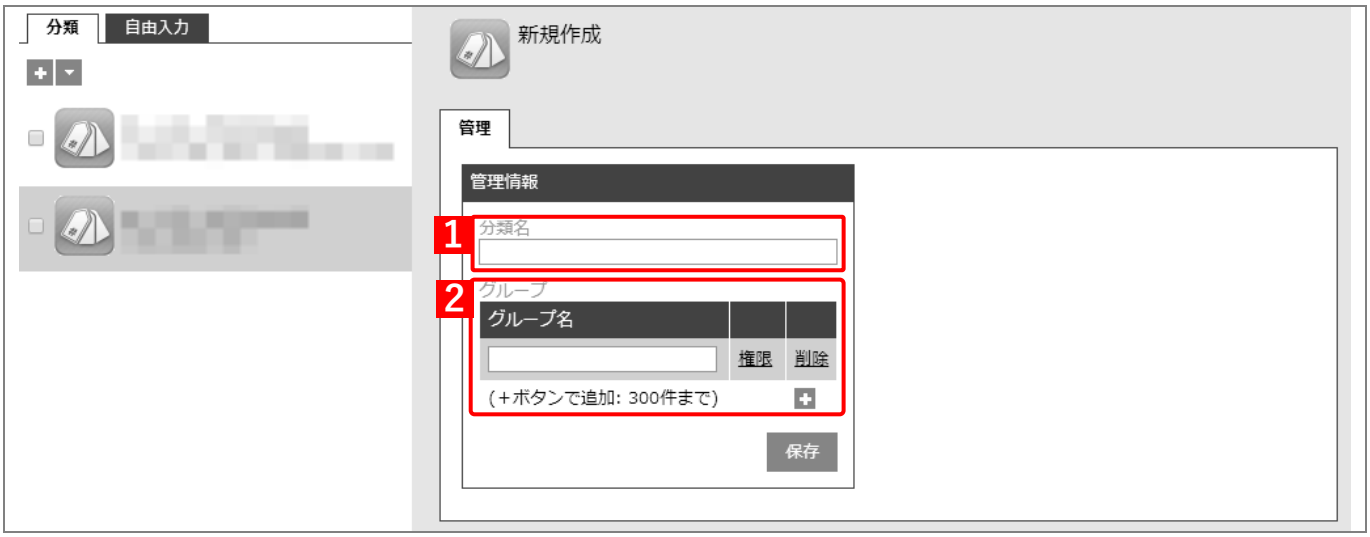
◆画面（新規作成）

表示操作［ユーザー］→［入力項目のカスタマイズ］→［分類］タブ→ ＋

［分類］タブ画面でカスタマイズできる項目について説明します。

作成した項目の利用方法については、以下を参照してください。

「入力項目のカスタマイズ」271 ページ



項番	名称		説明
1	分類名		分類の名称を 30 文字以内で入力します。重複する分類名は登録できません。 例）所属事業部
2	グループ		分類の下にグループを作成します。 ＋ をクリックして最大 300 件指定できます。
		グループ名	グループの名称を 30 文字以内で入力します。重複する分類名は登録できません。 例）営業部、システム部、総務部
		権限	ユーザーに追加権限を付与する場合に指定します。権限を追加する必要がない場合は指定する必要はありません。 クリックすると、権限設定用の画面が表示されます。 この画面では、ユーザーの管理情報の「ユーザー種別」で付与された権限では行えない操作ができます。追加する権限は「組織」、「ユーザー所有の機器」、「アプリ」ごとに指定します。 ●組織 「組織」に追加する権限を指定します。 ＋ をクリックして、リストボックスから組織を選択し、付与する権限を選択します。 例えばユーザー種別「閲覧者」のユーザーに、営業部に対してだけ「管理者」権限を付与できます。権限は「管理者」、「操作」、「閲覧者」、「ロック・ワイプ」のいずれかを指定します。 各権限の詳細については、以下を参照してください。 「［管理］タブ」257 ページ

項番	名称		説明
			●ユーザー所有の機器 ユーザー所有の機器に対して追加する権限を「管理者」、「操作」、「閲覧者」、「ロック・ワイプ」、「なし」のいずれかから選択します。 例えばユーザー種別「閲覧者」のユーザーに、自身が所有する機器に対してだけ「管理者」権限を付与できます。「なし」を選択した場合はユーザー所有の機器に対して権限の追加を行いません。 その他の権限の詳細については、以下を参照してください。 ☞「［管理］タブ」257 ページ ●アプリ アプリに追加する権限を指定します。表示されるアプリは、オプションの契約によって異なります。
		削除	クリックすると、該当のグループの行が削除されます。

5.2.2 ［自由入力］タブ

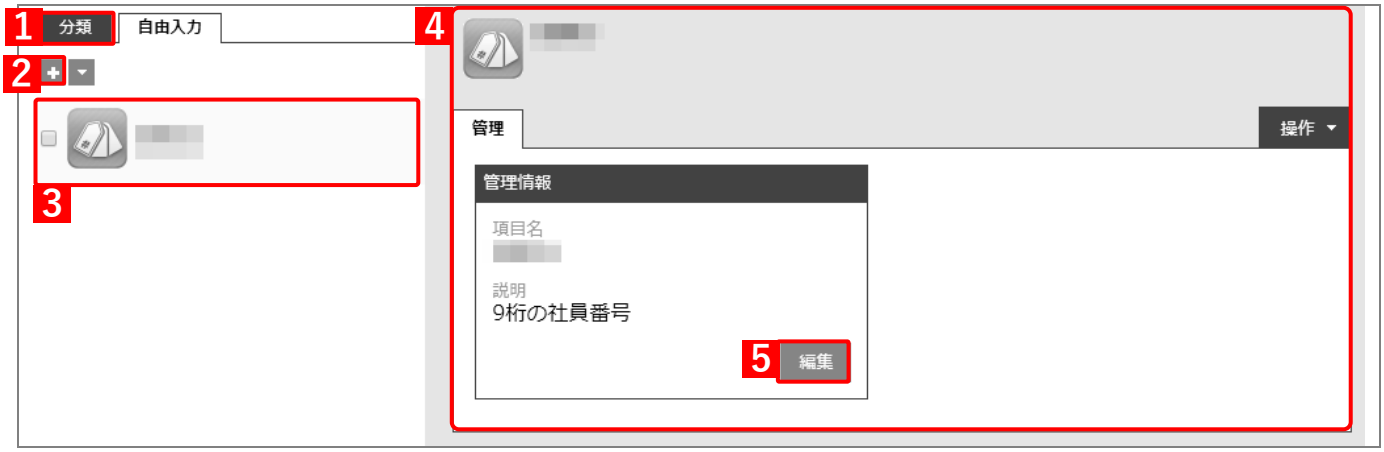
［入力項目のカスタマイズ］画面の［分類］タブ画面について説明します。

画面

画面（新規作成）

◆画面

表示操作　**［ユーザー］→［入力項目のカスタマイズ］→［自由入力］タブ**



項番	名称	説明
1	［分類］タブ	クリックすると、ユーザー分類画面が表示されます。詳細は、以下を参照してください。 「［分類］タブ」272 ページ
2	✚	クリックすると、自由入力の新規作成画面が表示されます。自由入力は最大 50 件まで作成できます。カスタマイズ項目の新規作成については、以下を参照してください。 「画面（新規作成）」276 ページ
3	自由入力一覧	登録されている自由入力の項目名が表示されます。
4	管理情報	自由入力一覧から選択した自由入力の登録内容が表示されます。
5	［編集］	クリックすると、表示されている入力項目の管理情報を編集できます。 編集できる項目は、新規作成時と同じです。

◆画面（新規作成）

表示操作［ユーザー］→［入力項目のカスタマイズ］→［自由入力］タブ→ ✚

［自由入力］タブ画面でカスタマイズできる項目について説明します。

作成した項目の利用方法については、以下を参照してください。

☞「入力項目のカスタマイズ」271 ページ

項番	名称	説明
1	項目名	入力欄の項目の名称を 30 文字以内で入力します。重複する項目名は登録できません。 例）社員番号、生年月日
2	説明	入力欄についての説明などがあれば、100 文字以内で入力します。 入力した説明文は、各機器の管理情報の該当項目の入力欄の下に「※」付きで表示されます。

5.3 CSV で追加

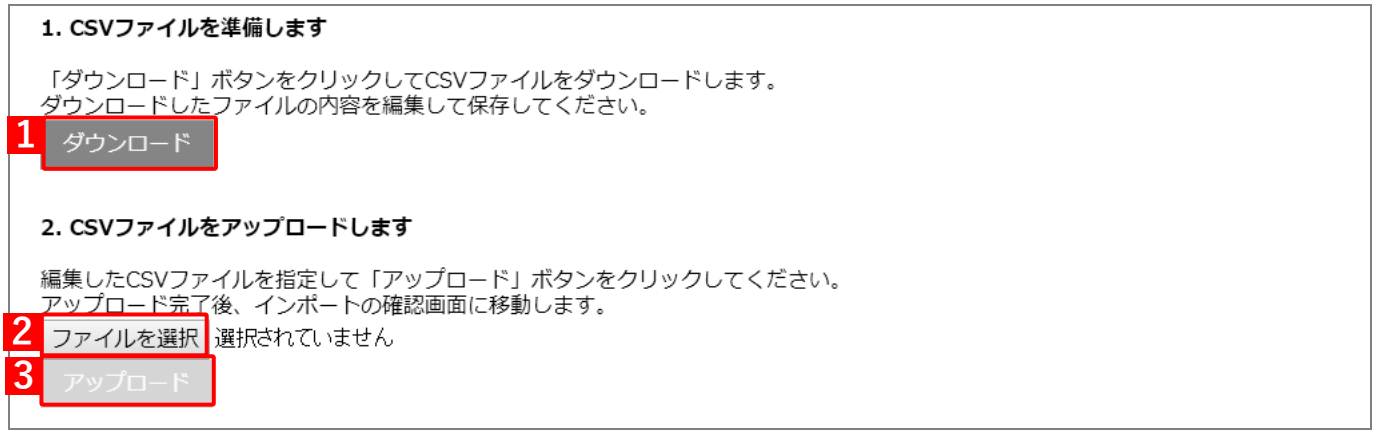
CSV ファイルを利用して、複数のユーザー情報を一括で管理サイトに登録できます。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

◆画面

表示操作［ユーザー］→［CSV で追加］



項番	項目	説明
1	［ダウンロード］	項目名のみが記載されたインポート用の CSV ファイルをダウンロードします。ダウンロードした CSV ファイルへのユーザー情報の入力方法については、以下を参照してください。 「インポート用の CSV ファイルの項目」278 ページ
2	［ファイルを選択］	ユーザー情報を入力したインポート用の CSV ファイルを選択します。
3	［アップロード］	ユーザー情報をアップロードします。アップロードが完了すると、インポート画面が表示されます。

◆インポート用の CSV ファイルの項目

ユーザー情報を CSV ファイルからインポートして追加、編集する場合、CSV ファイルに以下の項目を入力、編集して作成します。

CSV ファイルの 1 行目に項目名が表示されています。登録する情報は、2 行目以降に入力してください。

変更に使用する CSV ファイルには、登録されているユーザーの情報が表示されています。列と行の追加や削除は行わず、内容の修正のみ行ってください。

CSV ファイルの構造については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

項目名	入力方法
GUID	変更しないでください。 この項目は「CSV で編集」でダウンロードした CSV ファイルに表示されます。
[S]ユーザー種別	以下のいずれかの種別を入力します。 ・「管理者」、「操作」、「閲覧者」、「ロック・ワイプ」、「ログイン」、「一般」
[F]パスワード	新規データの場合は、4 文字から 20 文字以内の半角英数字で入力します。変更データの場合は、「*」で表示されていますが、変更はできます。4 文字から 20 文字以内の半角英数字で入力してください。 また、「*」を 8 個入力した場合は、変更されません。
その他の[F]から始まる項目	項目名に該当する値を自由に入力します。
[G]から始まる項目	「入力項目のカスタマイズ」の「分類」で登録した項目です。項目に該当する内容を入力します。 「入力項目のカスタマイズ」271 ページ 「入力項目のカスタマイズ」の「分類」で何も登録していない場合は、項目は表示されません。

5.4 CSV で編集

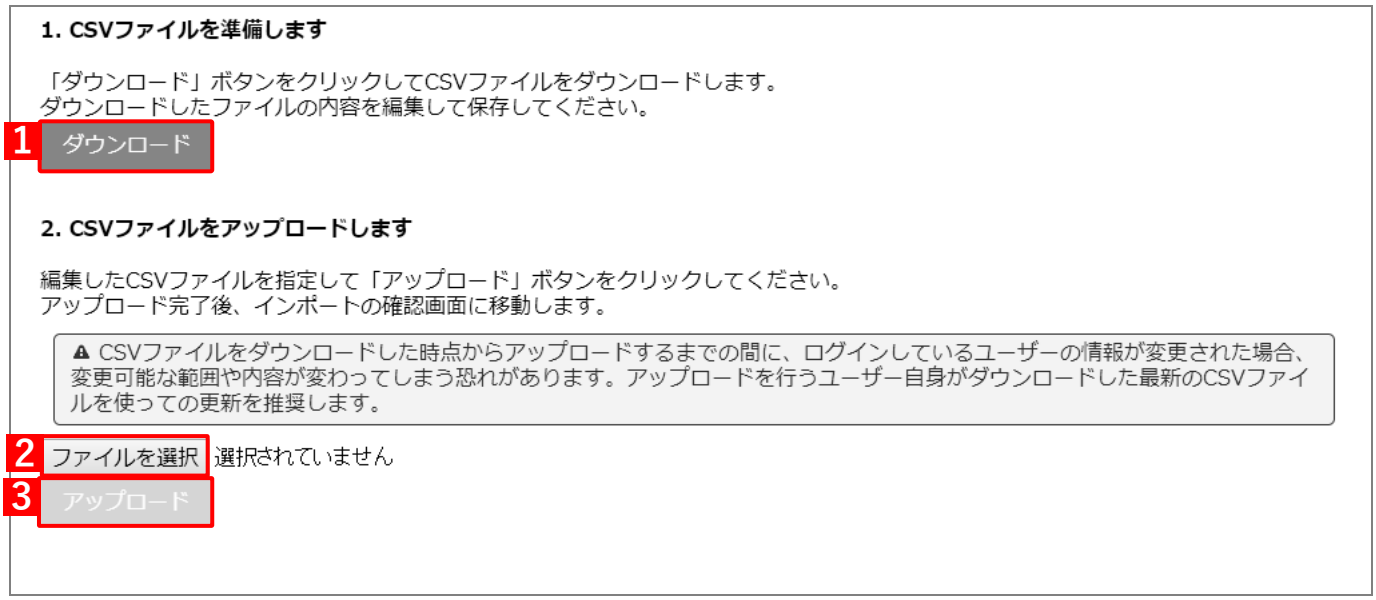
登録されているユーザーの情報をまとめて編集（変更）したい場合に使用します。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

◆画面

表示操作［ユーザー］→［CSV で編集］



項番	項目	説明
1	［ダウンロード］	ユーザー情報を記入するインポート用の CSV ファイルをダウンロードします。ダウンロードした CSV ファイルの編集方法については、以下を参照してください。 「インポート用の CSV ファイルの項目」278 ページ
2	［ファイルを選択］	ユーザー情報を入力したインポート用の CSV ファイルを選択します。
3	［アップロード］	ユーザー情報をアップロードします。アップロードが完了すると、インポート画面が表示されます。

5.5 CSV をダウンロード

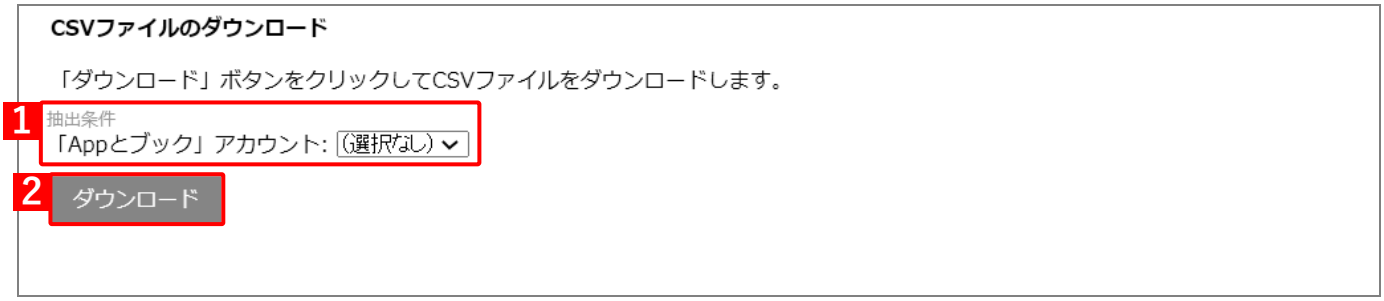
登録されているすべてのユーザー情報が記載されている CSV ファイルをダウンロードできます。
CSV ファイルへ出力されるときの文字コードは日本語環境では Shift-JIS（CP932）、その他の環境では UTF-8 です。

ダウンロードできる CSV ファイルは、「CSV で編集」でダウンロードできるファイルと同じです。

「CSV で編集」279 ページ

◆画面

表示操作［ユーザー］→［CSV をダウンロード］



項番	名称	説明
1	抽出条件	●「App とブック」アカウント 「App とブック」アカウントを選択すると、以下の条件を満たすユーザーのアプリまたは書籍ライセンスの割り当て状況がユーザーごとに CSV 出力されます。 ・ユーザーまたはユーザーが所属する組織に、選択した「App とブック」アカウント（「App とブック」場所のトークン）が紐づいている アプリまたは書式のライセンス割り当て状況には、以下のいずれかが表示されます。 ・割当済 ライセンスが割り当てられている ・割当待ち ライセンスが割り当てられていない ・ライセンス残数 0 ライセンスが割り当てられていなく、ライセンスの残数が 0 になっている ABM で「App とブック」ライセンスを購入するか、不要な「App とブック」ライセンスを機器から外して、ライセンス数を確保し、再度割り当てを行ってください。
2	［ダウンロード］	クリックすると、抽出条件に一致したユーザー情報が記載されている CSV ファイルをダウンロードできます。

6 組織

この章では、ヘッダーメニューの［組織］画面に表示される、各種の設定について説明します。

6.1 一覧

［機器］の［一覧］画面では、組織の新規作成や組織単位の機器設定、Android Enterprise アプリ配信設定の割り当てのほか、「App とブック」の付与状況確認などを行うことができます。

作成した組織に「機器」や「ユーザー」を所属させると、設定テンプレートや設定セットの適用が組織単位で行えるようになります。

組織単位での機器設定については、以下を参照してください。

☞「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」286 ページ

また、［ユーザー］の［入力項目のカスタマイズ］で「ユーザー種別」を「閲覧者」に設定しているユーザーが特定の組織に所属している場合は［操作］の権限を与えるなど、組織別の権限を所属ユーザーに追加することもできます。

詳細については、以下を参照してください。

☞「入力項目のカスタマイズ」271 ページ

機器やユーザーを組織に所属させる操作は、「機器」や「ユーザー」の新規作成画面、または編集画面で行います。

☞「機器」53 ページ
☞「ユーザー」253 ページ

組織は、最大 3,000 件まで作成できます。

◆画面

表示操作　［組織］→［一覧］

項番	名称	説明
1	［新規作成］	＋ をクリックすると項番 4 の「組織情報」に入力欄が表示されます。組織の新規作成方法については、以下を参照してください。 ☞「［管理］タブ」284 ページ

項番	名称	説明
2	［その他の操作］	をクリックすると以下のメニューが表示されます。 ●全てにチェックを入れる すべてのチェックボックスにチェックが入ります。 ●全てのチェックをはずす すべてのチェックボックスからチェックを外します。 ●一括削除 チェックボックスにチェックの入った組織をまとめて削除します。詳細については、以下を参照してください。 ☞「一括削除」32 ページ
3	組織一覧	登録されている組織の一覧が表示されます。 ●（A） 登録されている「組織名」が表示されます。 ●（B） 登録されている「上位組織」が表示されます。
4	組織情報	項番 3 の「組織一覧」から選択した組織の詳細な情報が表示されます。
5	［機器設定］タブ	組織単位での機器設定を行うタブです。各タブの概要は以下のとおりです。 ●［Android 設定］タブ Android 端末に組織単位での機器設定を行います。 ●［iOS 設定］タブ iOS 端末に組織単位での機器設定を行います。 ●［Windows 設定］タブ Windows 端末に組織単位での機器設定を行います。 ●［その他］タブ ・ユーザー設定 Android Enterprise のアプリケーション配信設定の割り当てを行います。詳細については、以下を参照してください。 ☞「Android Enterprise」327 ページ ・「App とブック」設定 企業に対する「App とブック」ライセンスの配布状態を確認・編集します。本画面で割り当てたライセンスは、「「App とブック」ライセンス」の［アプリケーション］タブで、「未割当数」としてカウントされます。この状態では実際にライセンスは付与されていません。詳細については、以下を参照してください。 ☞「「App とブック」ライセンス」514 ページ 「App とブック」トークンがアップロードされていない場合は、本画面に「(「App とブック」ライセンスがありません)」というメッセージのみ表示されます。 機器オプションパッケージを機器に割り当てていない場合は、設定を適用しません。
6	［操作］	クリックすると以下のメニューが表示されます。 ●削除 表示されている組織を削除します。詳細については、以下を参照してください。 ☞「削除」31 ページ

6.1.1 ［管理］タブ

組織名や組織の位置づけを設定します。

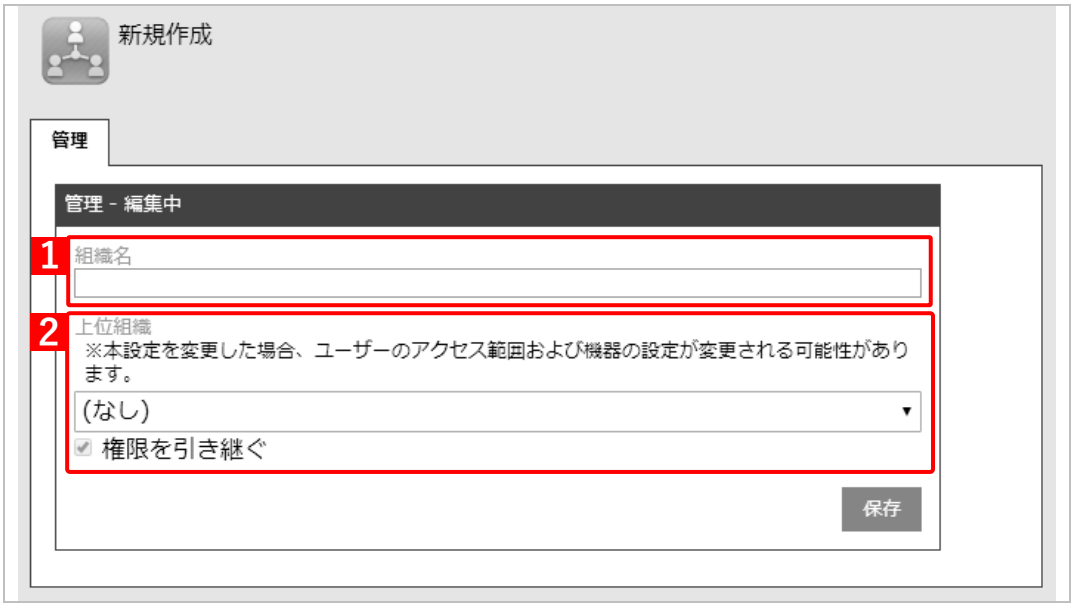
画面（新規作成）

画面

◆画面（新規作成）

表示操作　［組織］→［一覧］→ ＋

「機器」や「ユーザー」を所属させるための組織を新規に作成します。作成した組織は、機器およびユーザーの作成や編集時に入力項目として表示されます。



項番	名称	説明
1	組織名	組織名を 100 文字以内で入力します。同一上位組織内での重複はできません。例えば、「本社」や「支社名」「部署名」などを入力します。
2	上位組織	作成する組織を「組織図」のどこに配置するかを指定します。指定した組織の直下に紐づきます。最上位の組織とする場合は「(なし)」を指定します。また、上位組織を「(なし)」以外に指定したときは、あわせて権限を引き継ぐかどうかを指定します。ここで指す権限は「入力項目のカスタマイズ」を用いてユーザーに付与する追加権限を意味します。権限を引き継いだ場合は上位の組織に対して所有する追加権限をそのまま行使できます。 「サイトマップ―組織図を表示する」を例にあげます。“支社 1”を作成するときに権限を引き継ぐとした場合は、“本社”に追加権限［管理者］を持つユーザーは“支社 1”にも追加権限［管理者］を持つことになります。権限を引き継がない場合は、“本社”に追加権限［管理者］を持つユーザーでも“支社 1”については追加権限を持ちません。 ☞「組織図」651 ページ 選択肢には、以下の項目があります。 ●権限を引き継ぐ 上位組織の権限を引き継ぐ場合はチェックボックスにチェックを入れます。 例えば、「本社」と「支社」の関係を構築する場合は、「本社」「支社」の順番で作成します。「支社」を作成するときに「上位組織」を「本社」に設定すると、本社の下に支社がある関係となります。 本設定を変更した場合、ユーザーのアクセス範囲および機器の設定が変更される可能性があります。

◆画面

表示操作［組織］→［一覧］→一覧から対象を選択→［管理］タブ

項番	名称	説明
1	［編集］	クリックすると、表示されている組織を編集できます。編集内容は新規作成と同じです。詳細については、以下を参照してください。 ☞「画面（新規作成）」284 ページ
2	権限を共有する機器	クリックすると機器一覧を表示します。 ☞「機器一覧」54 ページ

◆エラー一覧

文言	発生契機	対処方法
⚠ 配下の組織、機器またはユーザーが存在するため削除できません。	削除しようとしている組織にユーザー、機器、下位組織が紐づけられている。	紐づけを解除したうえで再度削除してください。
⚠ 配下の組織、機器またはユーザーが存在するため一括削除できません。	一括削除しようとしている組織のいずれかにユーザー、機器、下位組織が紐づけられている。	紐づけを解除したうえで再度削除してください。

6.1.2 ［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ

設定セットを OS ごとに組織単位で端末に反映することができます。

テンプレートを作成している場合は、テンプレートの設定内容を反映することもできます。

また、Android Enterprise のアプリケーション配信設定や「App とブック」テンプレートの適用、App ライセンスとブックライセンスの付与などを、組織単位で行うことができます。

画面（設定テンプレートの適用）
画面（設定セットの適用）

本設定は、各機能の設定の割り当てで「(所属組織に従う)」が設定されている場合に、機器に反映されます。
設定セットの割り当てについては、以下を参照してください。

「(設定－Android）設定の割り当て」75 ページ
「(設定－iOS）設定の割り当て」83 ページ
「(設定－Windows）設定セットの割り当て」103 ページ

機器オプションパッケージを機器に割り当てていない場合は、設定を適用しません。

◆画面（設定テンプレートの適用）

表示操作　**［組織］→［一覧］→一覧から対象を選択→［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ**

OS 別に設定したテンプレートを選択した組織に適用します。

ここでは、［iOS 設定］タブ画像を例に使用しています。

項番	名称	説明
1	テンプレート	リストボックスから適用する設定テンプレートを選択します。
2	［適用］	クリックすると、選択したテンプレートが適用されます。

◆画面（設定セットの適用）

表示操作　**［組織］→［一覧］→一覧から対象を選択→［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ→［編集］**

OS 別に機能ごとの設定セットを設定し、選択した組織に保存します。

ここでは、［iOS 設定］タブ画像を例に使用しています。

項番	名称	説明
1	設定	リストボックスから適用する設定セットを選択します。必要事項を選択後に、［保存］をクリックして保存します。編集をキャンセルする場合は［取消］をクリックします。 「(所属組織に従う：設定なし)」を選択した場合、上位組織の設定が継承されます。 上位組織が設定されていない場合に「(所属組織に従う：設定なし)」を選択した場合、「(設定なし)」を選択した場合と同じ動きとなります。

6.1.3 ［その他▼］タブ／ユーザー設定

組織に Android Enterprise アプリ配信設定を割り当てます。

Android Enterprise の「アプリケーション配信」で、あらかじめ設定セットを作成してください。

「Android Enterprise／アプリケーション配信」327 ページ

本機能は、Android Enterprise 機能を利用した Android 端末に利用できます。

◆画面

表示操作　**［組織］→［一覧］→一覧から対象を選択→［その他▼］→「ユーザー設定」**

項番	名称	説明
1	Android Enterprise アプリ配信設定	組織に適用する Android Enterprise アプリ配信設定をリストボックスから選択します。 「(所属組織に従う：設定なし)」を選択した場合、上位組織の設定が継承されます。 上位組織が設定されていない場合に「(所属組織に従う：設定なし)」を選択した場合、「(設定なし)」を選択した場合と同じ動きとなります。

6.1.4 ［その他▼］タブ／「App とブック」設定

組織に「App とブック」設定テンプレートや「App とブック」ライセンス、アプリや書籍の付与などを設定します。

画面（「App とブック」設定テンプレートの適用）

画面（App ライセンスの付与）

画面（ブックライセンスの付与）

◆画面（「App とブック」設定テンプレートの適用）

表示操作　**［組織］→［一覧］→一覧から対象を選択→［その他▼］→「「App とブック」設定」→［新規作成］または［編集］**

設定した「App とブック」設定テンプレートを選択した組織に適用します。

項番	名称	説明
1	テンプレート	組織に適用する「App とブック」テンプレートをリストボックスから選択します。「App とブック」設定テンプレートの詳細については、以下を参照してください。 「「App とブック」設定テンプレート」520 ページ
2	「App とブック」ライセンス付与対象	「App とブック」ライセンスを付与する対象を以下から選択します。 ●「ユーザー」、「機器」
3	［適用］	クリックすると、選択したテンプレートが適用されます。

◆画面（App ライセンスの付与）

表示操作　**［組織］→［一覧］→一覧から対象を選択→［その他▼］→「［App とブック］設定」→［新規作成］または［編集］**

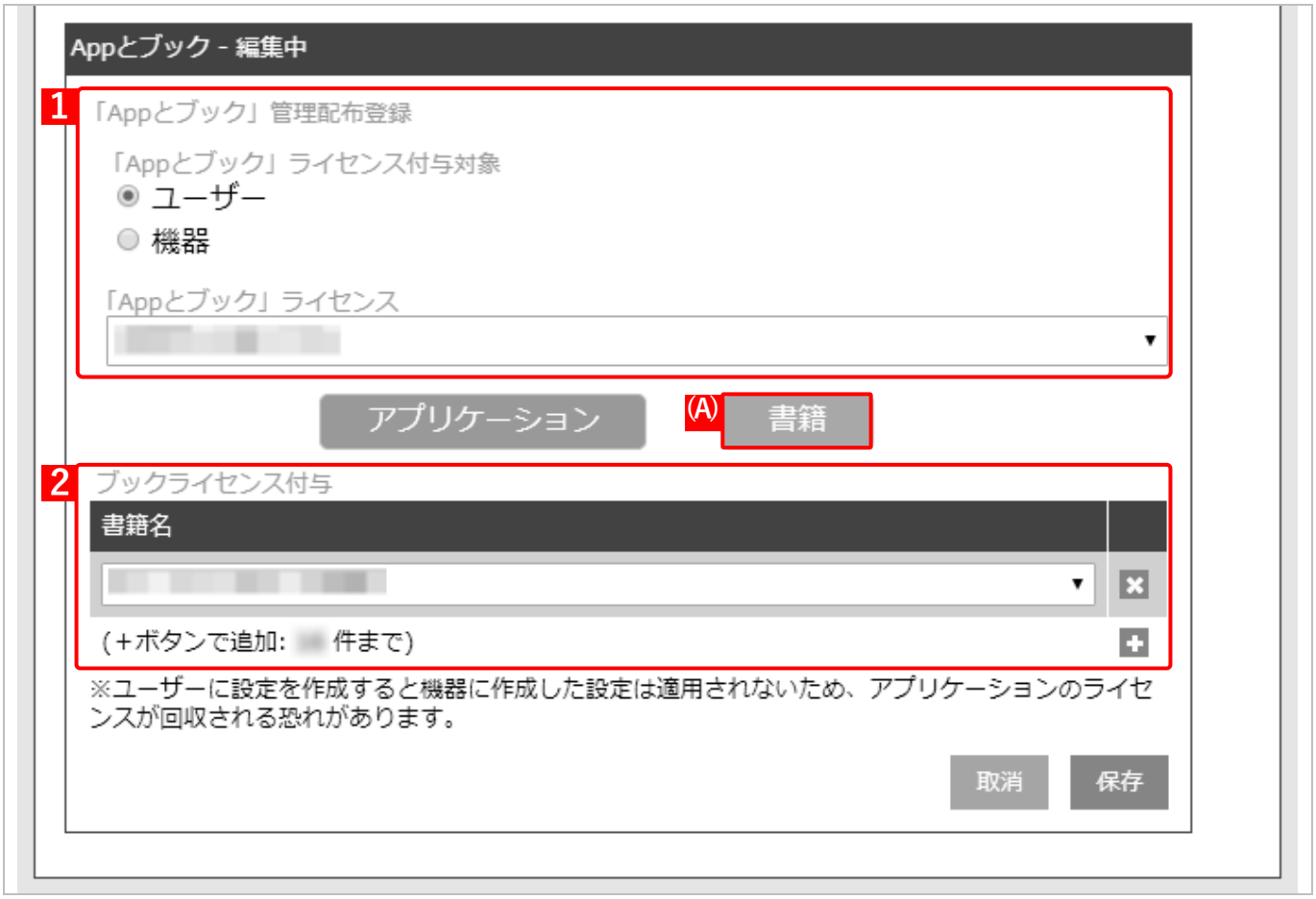
App ライセンスを選択した組織に付与します。

項番	名称	説明
1	「App とブック」管理配布登録	以下の項目を設定します。 ●「App とブック」ライセンス付与対象 「App とブック」ライセンスを付与する対象を以下から選択します。 ・「ユーザー」、「機器」 ●「App とブック」ライセンス 「App とブック」アカウントをリストボックスから選択します。詳細については、以下を参照してください。 ☞「［App とブック」ライセンス」514 ページ
2	App ライセンス付与	（A）［アプリケーション］をクリックすると、表示されます。 ライセンスの付与情報を確認・編集します。リストボックスからライセンスを付与するアプリを選択します。「App ライセンス付与」に、ライセンスが付与されたアプリの名前が表示されます。この名前をクリックすると、iTunes Store の該当アプリの紹介ページを表示します。 ＋ をクリックすると、入力欄が追加されます。 × をクリックすると、アプリが削除されます。 「App とブック」ライセンスに登録しているアプリが設定できます。画面に表示される件数は、「App とブック」ライセンスに登録しているアプリの数です。 ABM で購入したアプリの件数が表示されます。アプリは最大 300 件まで購入できます。

◆画面（ブックライセンスの付与）

表示操作　**［組織］→［一覧］→一覧から対象を選択→［その他▼］→「［App とブック］設定」→［新規作成］または［編集］**

書籍のライセンスを選択した組織に付与します。



項番	名称	説明
1	「App とブック」管理配布登録	以下の項目を設定します。 ●「App とブック」ライセンス付与対象 「App とブック」ライセンスを付与する対象を「ユーザー」に指定します。 ●「App とブック」ライセンス 「App とブック」アカウントをリストボックスから選択します。詳細については、以下を参照してください。 ☞「［App とブック」ライセンス」514 ページ

項番	名称	説明
2	ブックライセンス付与	（A）［書籍］をクリックすると、表示されます。 ライセンスの付与情報を確認・編集します。リストボックスからライセンスを付与する書籍を選択します。「ブックライセンス付与」に、ライセンスが付与された書籍の名前が表示されます。この名前をクリックすると、iTunes Store の該当書籍の紹介ページを表示します。 をクリックすると、入力欄が追加されます。 をクリックすると、アプリが削除されます。 「App とブック」ライセンスに登録している書籍が設定できます。画面に表示される件数は、「App とブック」ライセンスに登録している書籍の数です。 ABM で購入した書籍の件数が表示されます。書籍は最大 300 件まで購入できます。

◆エラー一覧

文言	発生契機	対処方法
⚠ アプリケーションは重複しないものを入力してください。	「App ライセンス付与」欄で［+］でアプリを追加するときに、追加するアプリ名が重複している。	重複しているアプリを設定から削除し、[保存] をクリックしてください。
⚠ 書籍は重複しないものを入力してください。	「ブックライセンス付与」欄で[+]で書籍を追加するときに、書籍名が重複している。	重複している書籍を設定から削除し、[保存] をクリックしてください。

6.2 CSV で追加

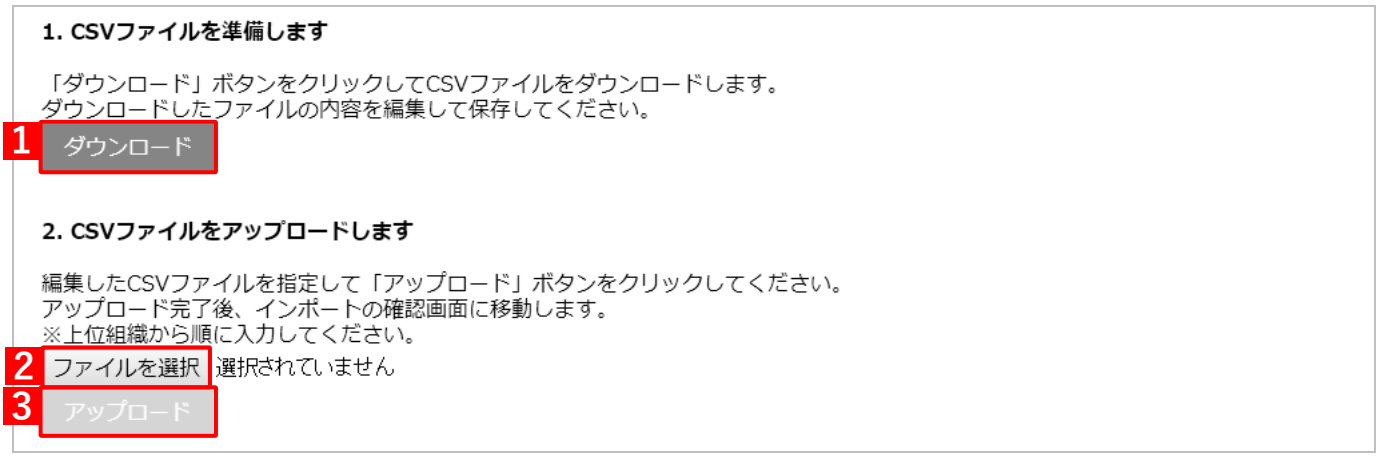
CSV ファイルを利用して、複数の組織情報を一括で管理サイトに登録できます。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

◆画面

表示操作［組織］→［CSV で追加］



項番	名称	説明
1	［ダウンロード］	項目名のみが記載されているインポート用の CSV ファイルをダウンロードします。ダウンロードした CSV ファイルへの組織情報の入力方法については、以下を参照してください。 「インポート用の CSV ファイルの項目」294 ページ
2	［ファイルを選択］	組織情報を入力したインポート用の CSV ファイルを選択します。
3	［アップロード］	組織情報をアップロードします。アップロードが完了すると、インポート画面が表示されます。

◆インポート用の CSV ファイルの項目

組織情報を CSV ファイルからインポートして追加、編集する場合、CSV ファイルに以下の項目を入力、編集して作成します。

CSV ファイルの 1 行目に項目名が表示されています。登録する情報は、2 行目以降に入力してください。

変更に使用する CSV ファイルには、登録されている組織の情報が表示されています。列と行の追加や削除は行わず、内容の修正のみ行ってください。

CSV ファイルの構造については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」－「インポート用の CSV ファイルの構造」

項目名	入力方法
GUID	変更しないでください。この項目は「CSV で編集」でダウンロードした CSV ファイルに表示されます。
[F]組織名	100 文字以内で入力してください。同一の上位組織内で重複はできません。
[S]上位組織	登録済みの上位組織の名称を入力してください。
[S]権限の引き継ぎ	上位組織の権限を引き継ぐ場合は、「ON」を入力してください。引き継がない場合は、空欄にしてください。
[S:OS 名]設定セット名もしくは設定テンプレート 例）[S:Android]設定テンプレート [S:iOS]ローミング設定	設定セットの名称を入力してください。 設定テンプレートの設定と競合している場合は、設定テンプレートが優先されます。各 OS の設定テンプレートの詳細については、以下を参照してください。 Android：「設定テンプレート」300 ページ iOS：「設定テンプレート」387 ページ Windows：「設定テンプレート」564 ページ 上位組織の設定を継承する場合は、空欄にしてください。
[S:OS 名]設定セット名(継承) 例)[S:Android]アプリケーション禁止(継承) [S:iOS]ローミング設定(継承)	上位組織の設定を継承する場合は、「ON」を入力してください。 継承せずに設定セットをあてる場合は、空欄にしてください。

6.3 CSV で編集

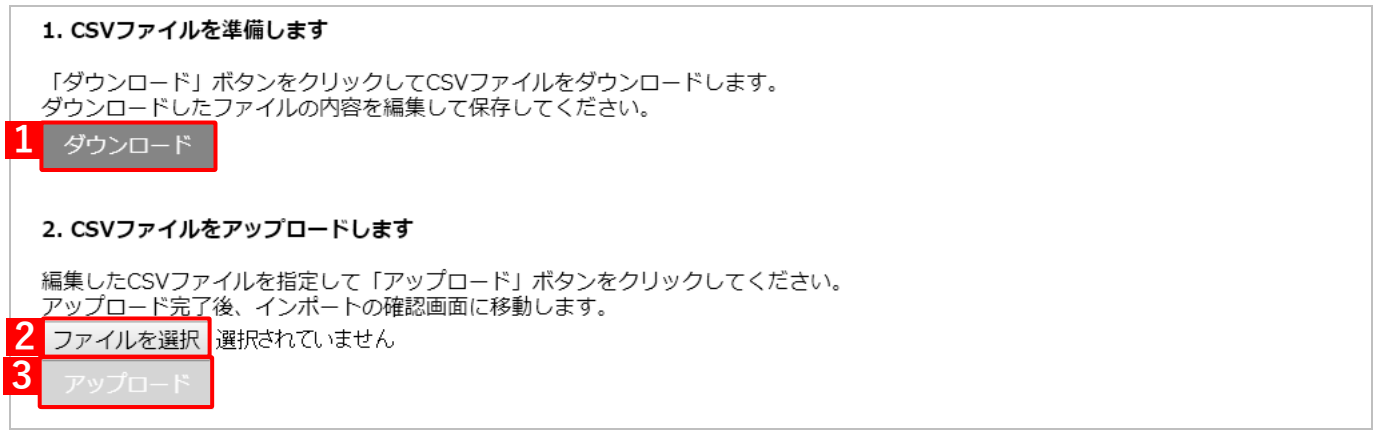
登録されている組織の情報をまとめて編集（変更）したい場合に使用します。

操作手順については、以下を参照してください。

『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

◆画面

表示操作［組織］→［CSV で編集］



項番	名称	説明
1	［ダウンロード］	組織情報を記入するインポート用の CSV ファイルをダウンロードします。
2	［ファイルを選択］	組織情報を入力したインポート用の CSV ファイルを選択します。
3	［アップロード］	組織情報をアップロードします。アップロードが完了すると、インポート画面が表示されます。

6.4 CSV をダウンロード

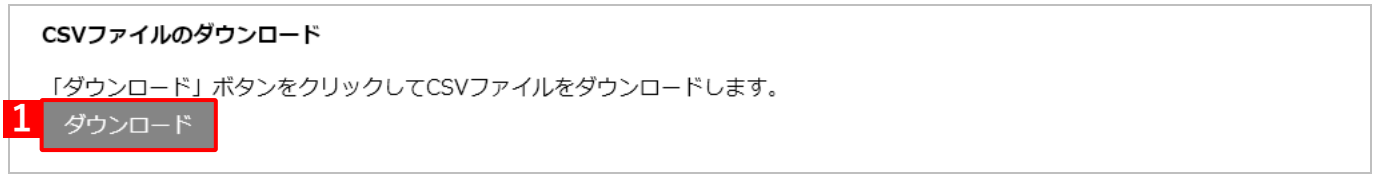
登録されているすべての組織情報が記載されている CSV ファイルをダウンロードできます。CSV ファイルへ出力されるときの文字コードは日本語環境では Shift-JIS（CP932）、その他の環境では UTF-8 です。

ダウンロードできる CSV ファイルは、「CSV で編集」でダウンロードできるファイルと同じです。

「CSV で編集」295 ページ

◆画面

表示操作　［組織］→［CSV をダウンロード］



項番	名称	説明
1	［ダウンロード］	クリックすると、登録されているすべての組織情報が記載されている CSV ファイルのダウンロードが開始されます。任意の場所に CSV ファイルを保存してください。ダウンロードした CSV ファイルは Excel やメモ帳などで開けます。

7 設定－Android

この章では、サブヘッダーメニューの［Android］画面に表示される、各種の設定について説明します。

注意

●作成した各設定の設定セットは、ヘッダーメニューの［機器］から割り当てることができます。
●設定を反映するには、端末と同期を行う必要があります。

7.1 管理アプリの通信と動作

管理サイトに登録されているすべての Android 端末に、共通する以下の操作を適用します。

●管理サーバーとの通信間隔
　管理サイトと Android エージェントアプリが行う定期的な同期の間隔を設定します。

●管理サーバーと通信できなかった場合
　管理サーバーと通信できなかった場合に、端末画面をロックするまでの時間を設定します。

●リモートロックの解除コード
　ロックした端末画面の解除用コードを設定します。

●端末でのエージェント停止・ライセンス解除・アンインストールの制限
　エージェントアプリを停止、ライセンス解除を行うときに必要なパスワードを設定します。

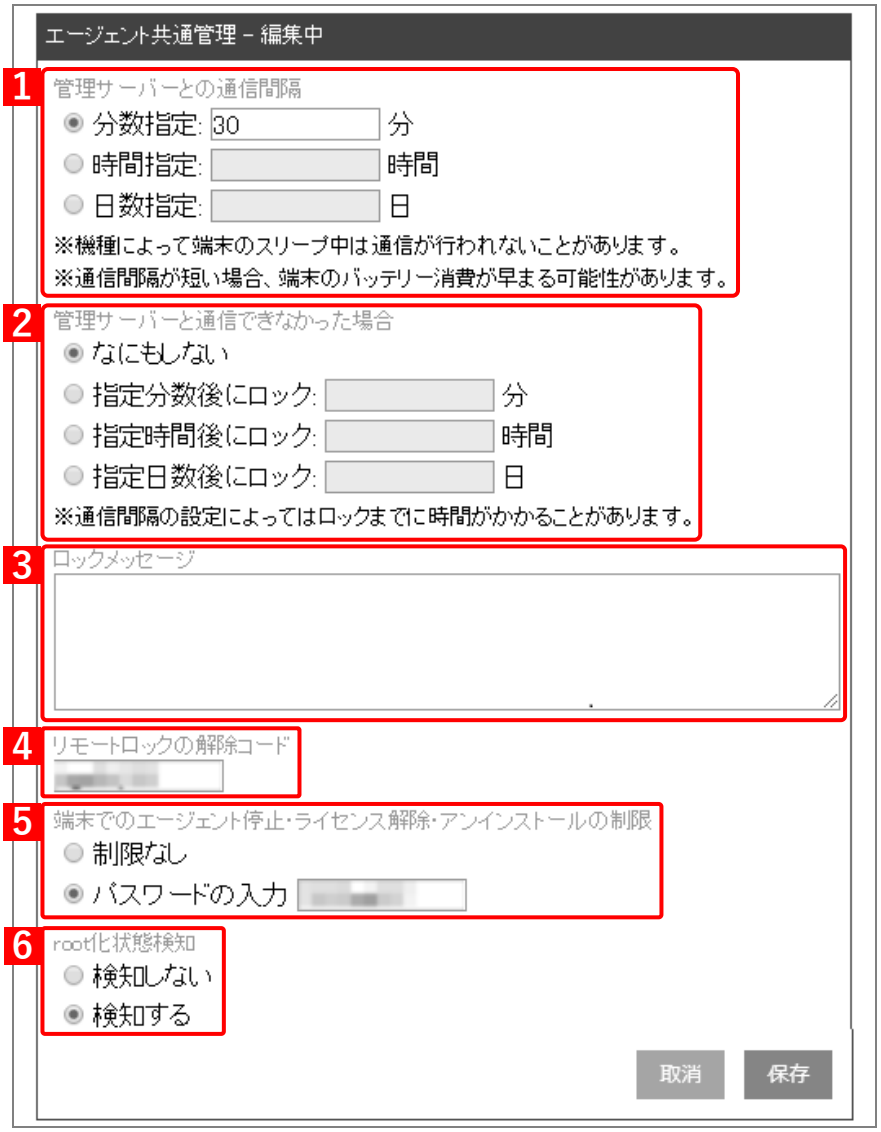
●root 化状態検知
　利用者が Android 端末を root 化した場合に検知します。

設定を保存した時点で、すべての Android 端末に適用されます。ただし、設定が端末に反映されるまでの時間は、サーバーや機器の通信状態に依存します。

サーバーとの通信間隔や端末の通信状態などによりバッテリー消費に影響があります。

◆画面

表示操作　［設定］→［Android］→［管理アプリの通信と動作］→［編集］



項番	対象	説明
1	管理サーバーとの通信間隔	機器が管理サーバーと定期的に同期する間隔を以下から選択して設定します。初期設定では、「分数指定」の「30 分」に設定されています。 ●分数指定 指定した分数間隔で同期を行います。10 から 59 の半角数字を入力します。 ●時間指定 指定した時間間隔で同期を行います。1 から 23 の半角数字を入力します。 ●日数指定 指定した日数間隔で同期を行います。1 から 365 の半角数字を入力します。 機種によって端末のスリープ中は通信が行われないことがあります。 通信間隔が短い場合、端末のバッテリー消費が早まる可能性があります。
2	管理サーバーと通信できなかった場合	管理サーバーと Android 端末が通信ができなくなった場合、Android 端末をロックするタイミングを以下から選択して設定します。初期設定では「なにもしない」に設定されています。 ●なにもしない リモートロックを行いません。 ●指定分数後にロック 指定した分数経過するとリモートロックを行います。10 から 59 の半角数字を入力します。 ●指定時間後にロック 指定した時間経過するとリモートロックを行います。1 から 23 の半角数字を入力します。 ●指定日数後にロック 指定した日数経過するとリモートロックを行います。1 から 365 の半角数字を入力します。 通信間隔の設定によってはロックまでに時間がかかることがあります。
3	ロックメッセージ	ロック中の Android 端末の画面にメッセージを表示したい場合に、1 文字から 200 文字で入力します。 ロック画面上では入力したメッセージの前後にある空白は削除されます。
4	リモートロックの解除コード	リモートロックによるロック画面および管理サーバーと通信ができなかった場合のロック画面で使用する解除コードを 4 文字から 20 文字の半角英数字で設定します。ロック画面から解除コードを入力すると、ロックを解除できます。 管理サイトからもリモートロックを解除できます。 初期設定ではランダムな 8 文字のパスワードが設定されています。 Android 5.0 以上の端末は「使用履歴にアクセスできるアプリ」が許可されていない場合は、端末に解除コードを入力してもリモートロックを解除できません。その場合は、管理サイトでリモートロック解除をしてください。
5	端末でのエージェント停止・ライセンス解除・アンインストールの制限	エージェントアプリからライセンスを解除する場合や、アンインストールする場合に、パスワードを要求する設定ができます。 ●制限なし パスワードを入力せずにライセンス解除やアンインストールできます。 ●パスワードの入力 ライセンス解除やアンインストールするときにパスワードを入力します。パスワードは 4 文字から 20 文字の半角英数字で入力します。 初期設定ではランダムな 8 文字のパスワードが設定されています。
6	root 化状態検知	Android 端末が root 化したこと、または root 化するアプリがインストールされている場合に検知する設定ができます。 ●「検知しない」、「検知する」

7.2 設定テンプレート

各機能で設定した設定セットの内容を、設定テンプレートとして保存します。

複数の Android 端末に同じ設定内容を繰り返し設定したい場合や、用途に応じて設定内容を切り替えたいときにテンプレートを使用すると、簡単に設定内容を適用することができます。

本機能では、設定テンプレートの作成や作成したテンプレートをデフォルトに設定するなどの操作を行うことができます。

画面

画面（設定テンプレートの作成）

設定テンプレートを一括で複数の Android 端末に適用できません。

テンプレートとして登録したい各機能の設定セットを、あらかじめ作成してください。

作成した設定テンプレートは、Android 端末ごと、または組織ごとに適用することができます。

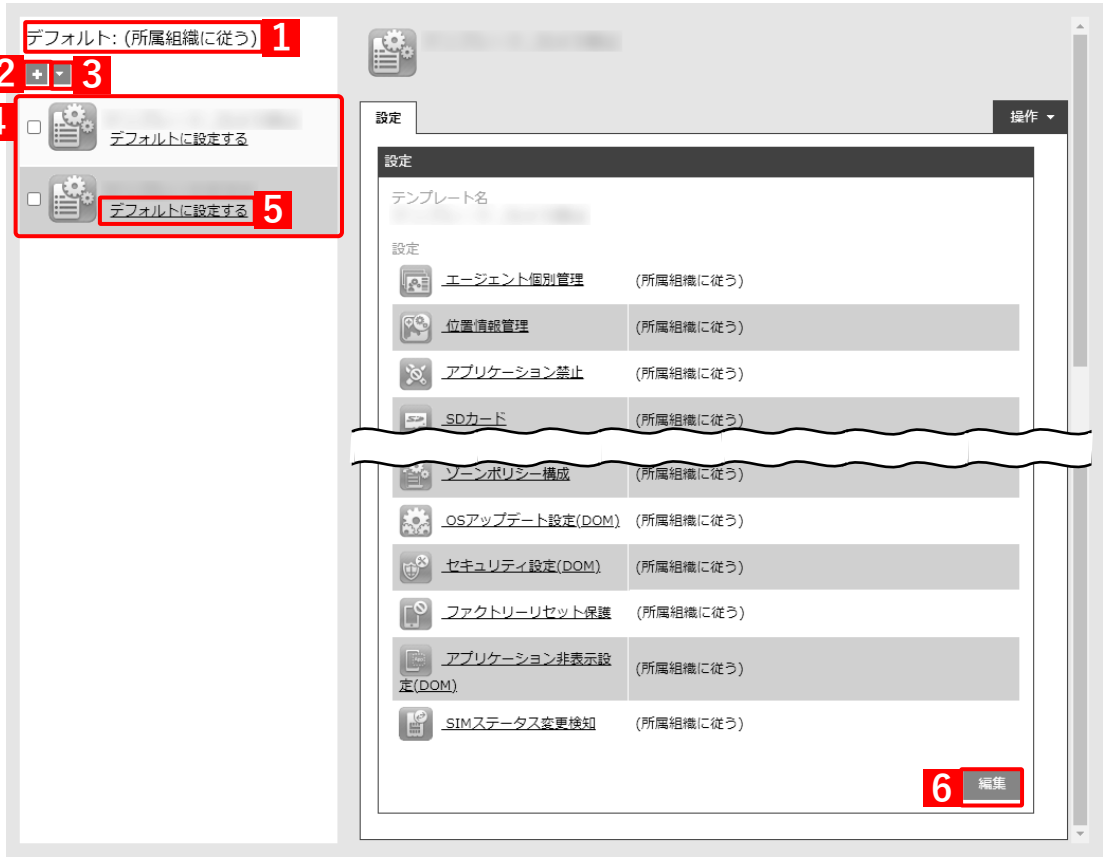
「（設定－Android）設定テンプレートの割り当て」77 ページ

「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」286 ページ

設定テンプレートは、最大 51 件まで作成できます。

◆画面

表示操作 ［設定］→［Android］→［設定テンプレート］

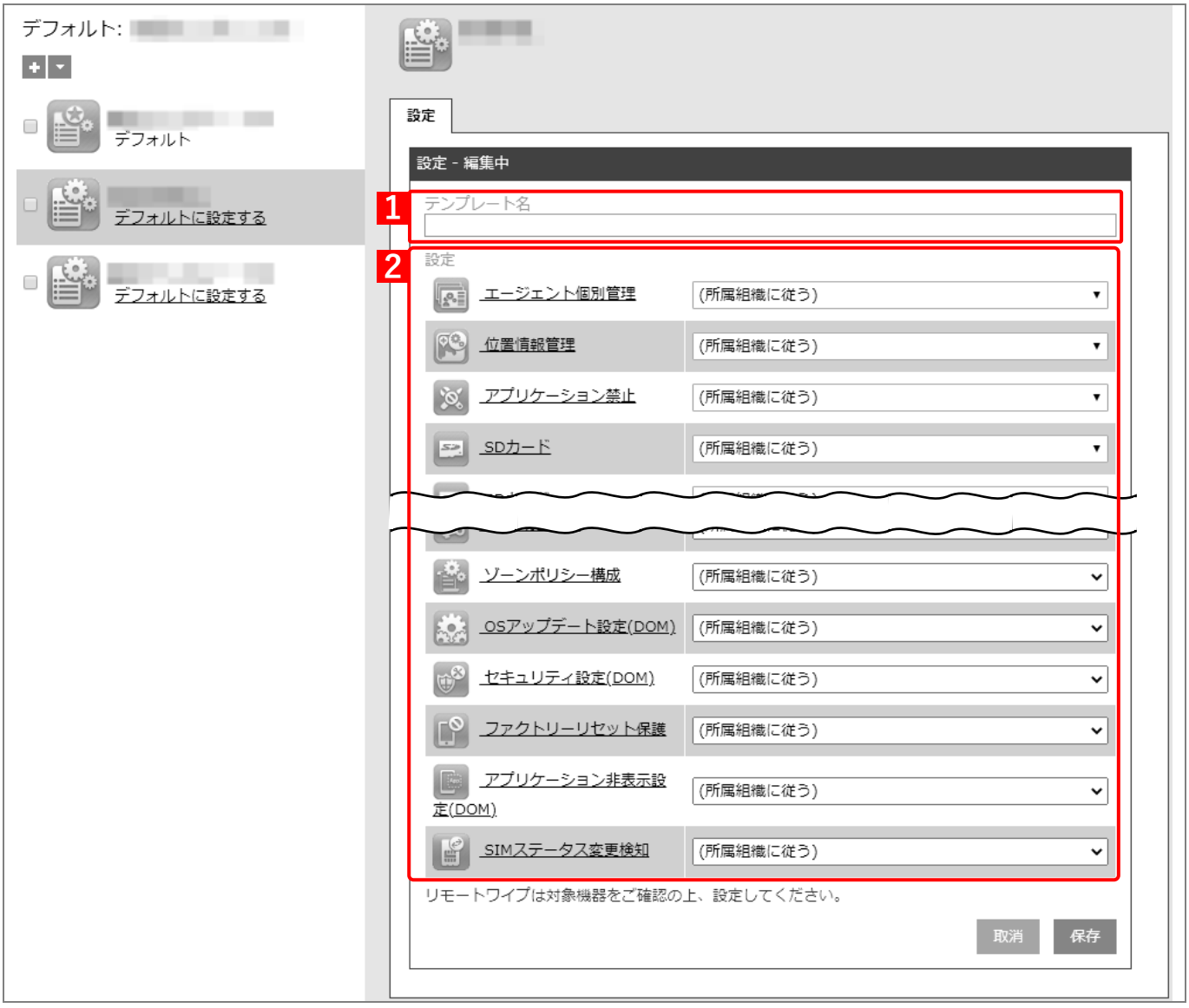


項番	項目	説明
1	デフォルトテンプレート表示	デフォルトに設定したテンプレートの名称が表示されます。 デフォルトに設定したときは、「(所属組織に従う)」が表示されます。 「(所属組織に従う)」は設定テンプレートの初期設定値です。

項番	項目	説明
2	＋	設定テンプレートを新規に作成します。 ☞「画面（設定テンプレートの作成）」301 ページ
3	▼	設定テンプレートのチェックや、チェックした設定テンプレートの一括削除のほか、デフォルトに設定した設定テンプレートを初期設定値の「(所属組織に従う)」に戻します。 ☞「(所属組織に従う)をデフォルトに設定する」303 ページ
4	設定テンプレート一覧	＋で作成した設定テンプレートが表示されます。
5	［デフォルトに設定する］	作成した設定テンプレートをデフォルトにします。 ☞「設定テンプレートをデフォルトに設定する」302 ページ
6	［編集］	設定テンプレートを編集します。 ☞「画面（設定テンプレートの作成）」301 ページ

◆画面（設定テンプレートの作成）

表示操作［設定］→［Android］→［設定テンプレート］→ ＋ または［編集］



項番	項目	説明
1	テンプレート名	設定テンプレートの名称を 1 文字から 30 文字で入力します。
2	設定	各機能に設定する内容を以下から選択します。 ●各機能の設定名 各機能で作成した設定の名称を指定します。指定した設定名に対する編集および削除が行われた場合、設定テンプレートにも反映されます。 ●(所属組織に従う) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(変更しない) 機器ごとに適用している設定に変更を行いません。 ●(設定なし) 各機能の設定を外します。 リモートワイプは対象機器を確認してから、設定してください。

設定テンプレートをデフォルトに設定する

作成した設定テンプレートをデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が設定テンプレートの内容に設定されます。

管理サイトに登録する端末を同じ設定にしたい場合に便利です。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［Android］→［設定テンプレート］→デフォルトにするテンプレートの「デフォルトに設定する」

項番	項目	説明
1	デフォルト	デフォルトに設定しているテンプレート名が表示されます。また、デフォルトになっているテンプレート名の下に「デフォルト」と表示されます。(A)の箇所に記載されます。
2	［デフォルトに設定する］	クリックすると、そのテンプレート名の設定をデフォルトにできます。
3	メッセージボックス	選択したテンプレートをデフォルトにすることを確認する画面です。 ●OK 選択したテンプレートをデフォルトに設定します。 ●キャンセル 選択したテンプレートをデフォルトに設定することを中断します。

(所属組織に従う)をデフォルトに設定する

「(所属組織に従う)」をデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が「(所属組織に従う)」に設定されます。

初期設定では、デフォルトに「(所属組織に従う)」が設定されています。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［Android］→［設定テンプレート］→ ▼ →［(所属組織に従う)をデフォルトにする］

項番	項目	説明
1	(所属組織に従う)をデフォルトにする	各種設定内容が「(所属組織に従う)」になるテンプレートをデフォルトにします。
2	メッセージボックス	デフォルトに設定することを確認する画面です。 ●OK 「(所属組織に従う)」をデフォルト設定します。 ●キャンセル 設定を行いません。

7.3 セキュリティ

本機能では、スクリーンロックのパスワード設定、位置情報の取得、Secure Shield の設定、カメラの禁止項目、SD カードの禁止項目、Bluetooth の禁止項目の設定セットを作成します。

7.3.1 画面ロック

Android 標準のロック画面設定に制限を追加する、スクリーンロックの設定セットを作成します。パスワードの文字数や英数字利用の指定、パスワードの有効期限、スクリーンロック解除の失敗に応じてワイプを行う設定などが追加されます。

「ロック画面の制限」は、Device Owner Mode 化されたストア版エージェントでのみ利用可能です。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

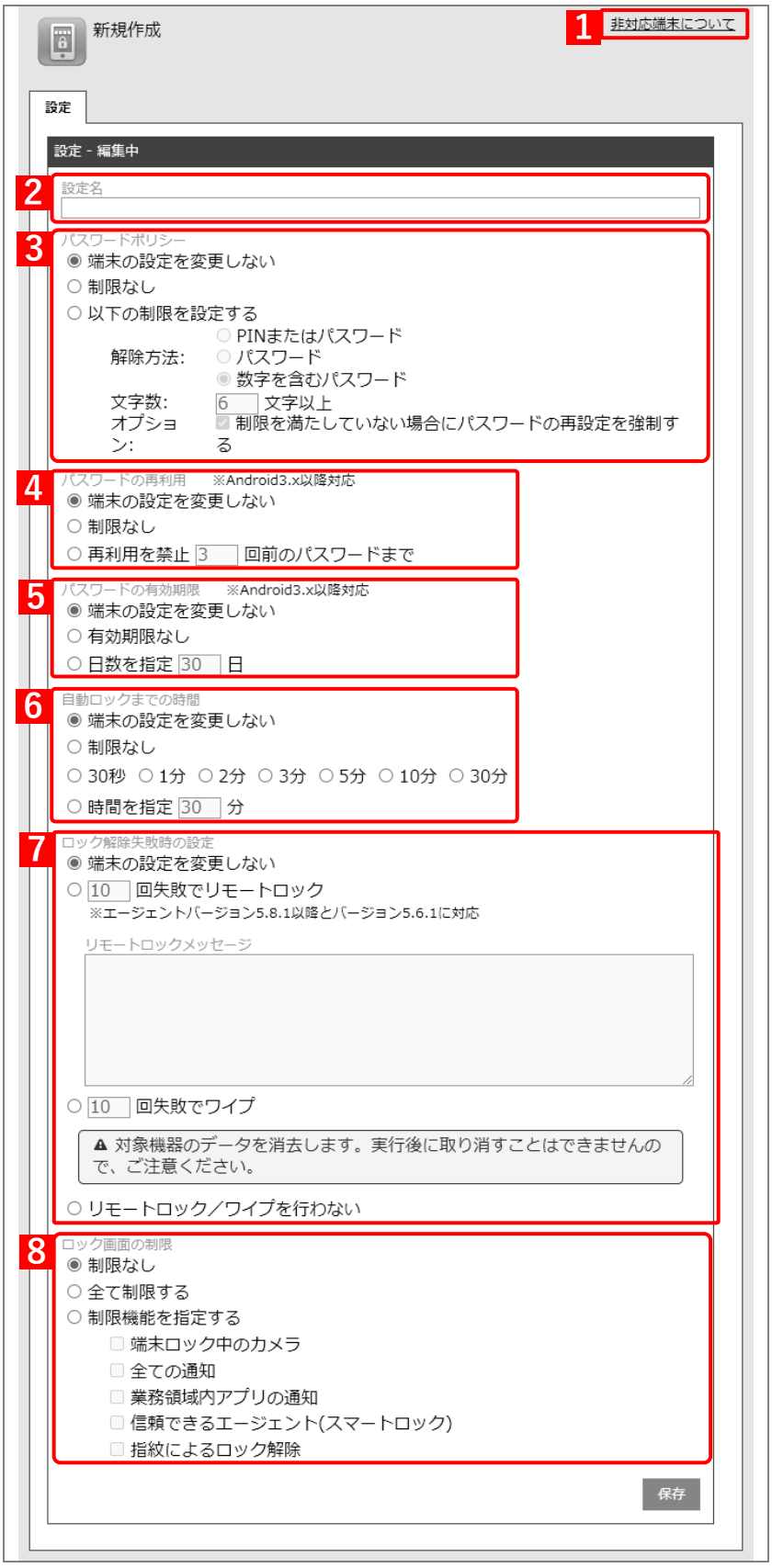
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［セキュリティ］→［画面ロック］→ ✚



項番	項目	説明
1	非対応端末について	クリックすると非対応の Android 端末名が表示されます。 『Android エージェント対応端末表』

項番	項目	説明
2	設定名	設定の名称を 1 文字から 30 文字で入力します。
3	パスワードポリシー	ロック画面で入力するパスワードの制限を選択します。
	端末の設定を変更しない	現在の設定を変更しません。
	制限なし	パスワードの入力を不要にします。
	以下の制限を設定する	以下から選択します。 ●解除方法 以下から選択します。 ・PIN またはパスワード PIN（数字）またはパスワード（英字のみ）で解除します。 ・パスワード 英字のみのパスワードで解除します。 ・数字を含むパスワード 数字と英字の両方を含むパスワードで解除します。 ●文字数 パスワードの最小の入力文字数を 4 文字から 16 文字の半角数字で入力します。例えば、文字数に「5」を指定した場合は、5 文字以上のパスワードを入力します。 ●オプション 指定した制限を満たしていないパスワードが入力された場合、パスワードの再設定画面を端末に表示したいときは、「制限を満たしていない場合にパスワードの再設定を強制する」にチェックを入れます。 Device Owner Mode の状態が「有効」になっている Android 7.0 以上の端末で、スクリーンロックパスワード設定画面が表示されたとき、スクリーンロックパスワードを設定せずに端末の電源を OFF にすると、電話などの通知が表示されなくなります。スクリーンロックパスワード設定画面が表示された場合、電源を OFF にする前にスクリーンロックパスワードを設定してください。 Device Owner Mode の状態が「有効」になっている端末で、スクリーンロックパスワード設定画面が表示されたとき、「あとで」をタップするとホーム画面のアプリがグレー表示され利用できなくなります。その場合は、端末でパスワードポリシーを満たしたパスワードを設定すると、再びアプリが利用できるようになります。 電話などの通知が表示されなくなった場合は、端末でアプリの設定のリセットを行ってください。 ・端末の設定アプリを起動 ・端末の［設定］→［通知］→［ミ］→［アプリの設定をリセット］する ・確認画面が表示されますのでリセットを行ってください。 一度リセットをすると、すべてのアプリ設定がデフォルト値に戻ります。十分に注意してください。 ・本製品の設定が促されるため、許可してください。
4	パスワードの再利用	パスワードの有効期限が切れた場合、同じパスワードを再度利用できるか設定します。 ●制限なし パスワードの再利用回数を制限しません。 ●再利用を禁止 指定した回数以降は、新たなパスワードを利用するように使用します。指定は 1 から 10 の半角数字で入力します。 ●端末の設定を変更しない 現在の設定を変更しません。 Android 3.0 以上に対応しています。

項番	項目	説明
5	パスワードの有効期限	パスワードの有効期限の設定を以下から選択します。 ●有効期限なし 有効期限を設定しません。 ●日数を指定 有効期限日数を 1 から 365 の半角数字で入力します。 ●端末の設定を変更しない 現在の設定を変更しません。 Android 3.0 以上に対応しています。
6	自動ロックまでの時間	自動的に端末にロックをかける契機を以下から選択します。 ●端末の設定を変更しない 現在の端末の設定を変更しません。 ●制限なし 自動ロックまでの時間を制限しません。 ●「30 秒」、「1 分」、「2 分」、「3 分」、「5 分」、「10 分」、「30 分」 端末を何も操作しない状態が続いた場合、端末にロックをかけるまでの経過時間を選択します。例えば、「5 分」を選択した場合は、端末の操作をしない時間が 5 分経過すると、自動的に端末がロックされるようになります。 ●時間を指定 端末にロックをかけるまでの時間を 1 から 30 の半角数字で入力します。 自動ロックまでの上限時間を設定できます。設定した時間以内であれば、Android 端末で設定時間を変更することができます。本設定以内の時間を Android 端末で設定している場合は、本設定ではなく、端末で設定したロック時間が優先されます。 本設定の自動ロック時間は、Android 端末では「画面消灯時間」が設定されます。
7	ロック解除失敗時の設定	ロック解除に失敗した場合の設定を以下から選択します。 ●端末の設定を変更しない 現在の設定を変更しません。 ●○回失敗でリモートロック スクリーンロックの解除に指定回数失敗した場合は、自動的にリモートロックするように設定します。回数は 2 から 50 の半角数字で入力します。 ・リモートロックメッセージ 200 文字以内で入力してください。 この設定は、エージェントバージョン 5.8.1 以上とバージョン 5.6.1 の端末で利用できます。 ●○回失敗でワイプ スクリーンロックの解除に指定回数失敗した場合、自動的にワイプするように設定します。回数は 2 から 50 の半角数字で入力します。 対象機器のデータを消去します。実行後に取り消すことはできません。 ●リモートロック／ワイプを行わない スクリーンロックの解除に失敗した場合、リモートロック、ワイプを行いません。 端末でロック解除方法に「パターン」を使用していて、3 つ以下の点をなぞってパターンの入力に失敗しても解除失敗の回数としてカウントされません。 4 つ以上の点をなぞってパターンの入力に失敗すると解除失敗の回数としてカウントされます。

<table>
<tr><th>項番</th><th colspan="2">項目</th><th>説明</th></tr>
<tr><td>8</td><td colspan="2">ロック画面の制限</td><td>端末でロック画面が設定されている場合は、制限する機能の範囲について選択します。
本機能をご利用いただくには、端末のエージェントで新たな権限（画面ロックの一部の機能を無効化）の許可を行う必要があります。詳細については、以下のマニュアルを参照してください。
『Android クライアント リファレンスマニュアル』の「管理サイトからの指示による動作」－「管理外通知画面が表示された場合」
端末のパスワードロックが未設定またはスワイプに設定していた場合は、ロック画面の制限ができません。「PIN」「パターン」「パスワード」などを設定してください。
「（操作－Android）スクリーンロックパスワード変更」109 ページ
『Android クライアント リファレンスマニュアル』の「管理サイトからの指示による動作」－「パスワードポリシーが変更された場合」</td></tr>
<tr><td></td><td>制限なし</td><td>機能を制限しません。</td></tr>
<tr><td></td><td>全て制限する</td><td>ロック画面上のすべての機能を制限します。
「リモートロック」で解除方法を「スクリーンロックパスワード」に設定して実行すると、管理サイトで指定した通知領域のメッセージは表示されません。
「（操作－Android）リモートロック」ページ</td></tr>
<tr><td></td><td>制限機能を指定する</td><td>以下から選択します。
●端末ロック中のカメラ
端末ロック中のカメラボタン（画面上）からのカメラ起動を制限します。
物理ボタンからのカメラ起動については、端末によって制限されない場合があります。
本機能を利用していない場合でも、設定＞Android＞機能制限＞カメラにおいてカメラを禁止している場合は、ロック画面上に表示されません。
●全ての通知
スクリーンロック画面に表示されるすべての通知が制限されます。
●業務領域内アプリの通知
スクリーンロック画面に表示される業務領域内アプリの通知が制限されます。
●信頼できるエージェント（スマートロック）
スマートロック機能によるスクリーンロックの解除を制限できます。
スマートロックは、Android 5.0 以上に、OS 標準機能として搭載された 信頼できる場所、顔、声、端末などによるロック画面を解除する機能です。
●指紋によるロック解除
指紋によるロック画面解除を制限します。</td></tr>
</table>

7.3.2 位置情報管理

Android 端末で位置情報を測位する契機を指定するための設定セットを作成します。
取得した位置情報を確認する場合は、以下を参照してください。

「（情報－Android）位置」146 ページ

端末の位置情報機能を有効にしてください。

本製品のエージェントアプリの位置情報取得を端末側で許可してください。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

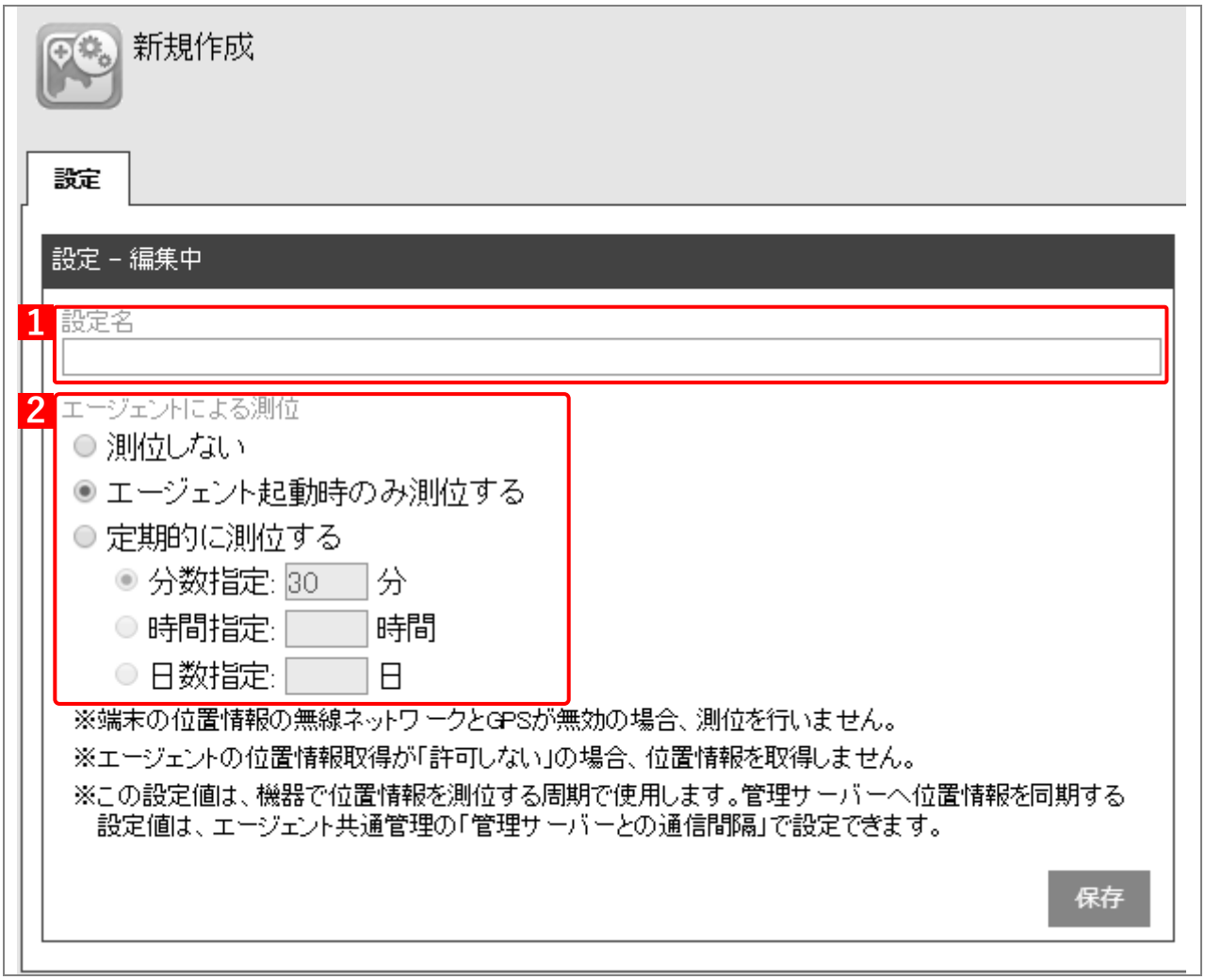
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［セキュリティ］→［位置情報管理］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	エージェントによる測位	エージェント側の位置情報の測位の契機を以下から選択します。 ●測位しない エージェント側では、位置情報を測位しません。 ただし、管理サイトから「同期」を指示した場合は、端末の位置情報を測位します（契機 1）。 ●エージェント起動時のみ測位する 以下のときに測位します（契機 2）。 ・端末を起動したとき ・エージェントを起動または終了したとき ・エージェントが停止したあと、自動で再開したとき ユーザー、アプリ、OS の仕様などで停止することもあります。 ●定期的に測位する 契機 1・2 に加え、定期的に測位する契機を分数指定、時間指定、日数指定から選択できます。 ・分数指定 指定した分数間隔で測位する場合に選択します。分数は 10 から 59 の半角数字で入力します。 ・時間指定 指定した時間間隔で測位する場合に選択します。時間は 1 から 23 の半角数字で入力します。 ・日数指定 指定した日数間隔で測位する場合に選択します。日数は 1 から 365 の半角数字で入力します。 端末の位置情報の無線ネットワークと GPS が無効の場合、測位を行いません。 エージェントの位置情報取得が「許可しない」の場合、位置情報を取得しません。 この設定値は、機器で位置情報を測位する周期で使用します。管理サーバーへ位置情報を同期する設定値は、「管理アプリの通信と動作」の「管理サーバーとの通信間隔」で設定できます。 「管理アプリの通信と動作」298 ページ Android 12 以上は、正確な位置情報を取得するために、端末の設定で「正確な位置情報を使用」を有効にしてください。

7.3.3 Secure Shield

Secure Shield は、端末の設定アプリの利用範囲を制限する機能です。各項目を設定し、端末へ Secure Shield による制限を端末に行うための設定セットを作成します。
Secure Shield を有効にすると、［設定］をタップしたときに Secure Shield の画面が表示されます。

端末の OS をアップデートすると、Secure Shield が機能しなくなることがあります。OS をアップデートする前に、Secure Shield の OS 対応状況を確認してください。OS が未対応のバージョンの場合は、設定が割り当てられていても Secure Shield を利用できません。
Secure Shield の対応機種については、以下を参照してください。

『Android エージェント Secure Shield 動作状況』

エージェント側での Secure Shield の使用方法については、以下を参照してください。

『Android クライアント リファレンスマニュアル』の「管理サイトからの指示による動作」－「Secure Shield が有効に設定された場合」

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

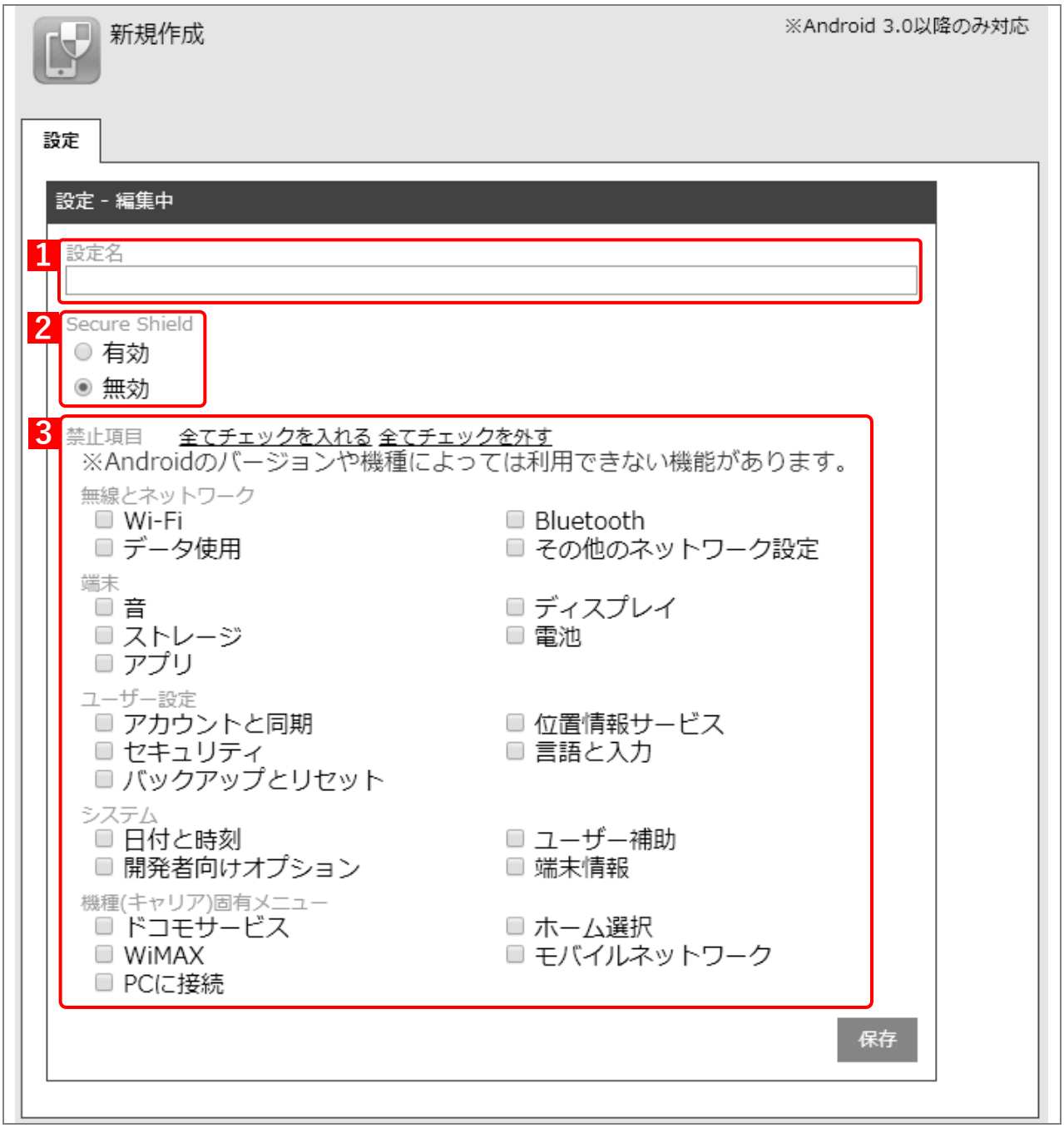
「全機器一括設定」200 ページ

通知領域から変更できてしまう内容は、Secure Shield では防げません。
「セキュリティ設定（DOM）」で「ステータスバー」の無効化の併用をご検討ください。

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［セキュリティ］→［Secure Shield］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	Secure Shield	Secure Shield の有効／無効を以下から選択します。 ●有効 Secure Shield を有効にし、禁止項目で指定した端末の設定アプリ機能を制限します。 ●無効 Secure Shield を無効にし、禁止項目の制限を解除します。
3	禁止項目	Secure Shield で禁止する項目を設定します。 Android のバージョンや機種によっては利用できない機能があります。対応機種については、以下を参照してください。 『Android エージェント対応端末表』

項番	項目		説明
		［全てチェックを入れる］	クリックすると、禁止項目のすべての項目にチェックを入れます。
		［全てチェックを外す］	クリックすると、禁止項目のすべての項目のチェックを外します。
		無線とネットワーク	禁止する項目にチェックを入れます。 ●Wi-Fi Wi-Fi の ON／OFF の切り替えを行います。 ●Bluetooth Bluetooth の ON／OFF の切り替えを行います。 Android 12 以上は、端末の設定で「付近のデバイス」権限を許可するに設定している場合は、Bluetooth の切り替えが行えます。 ●データ使用 端末のデータ通信量の確認や、データの制限設定などを行います。 ●その他のネットワーク設定 機内モード、VPN 設定など、その他のネットワークの設定を行います。
		端末	禁止する項目にチェックを入れます。 ●音 着信音やマナーモードの設定を行います。 ●ディスプレイ ディスプレイの明るさ、ロック画面の表示設定を行います。 ●ストレージ 本体メモリや microSD、メモリカードの空き容量を確認できます。また、microSD、メモリカードのマウント／マウント解除やデータ消去などもできます。 ●電池 電池残量を確認したり、電池を使用しているアプリを確認したりできます。 ●アプリ アプリの管理を行います。
		ユーザー設定	禁止する項目にチェックを入れます。 ●アカウントと同期 アカウントの追加や設定の変更を行います。 ●位置情報サービス 位置情報サービスや GPS 機能などの ON／OFF の切り替えを行います。 ●セキュリティ 画面ロックの認証設定や、パスワードの設定などを行います。 ●言語と入力 表示言語や文字入力について設定します。 ●バックアップとリセット 端末のバックアップについて設定したり、端末の初期化したりできます。
		システム	禁止する項目にチェックを入れます。 ●日付と時刻 日付と時刻の表示形式やタイムゾーンを設定します。 ●ユーザー補助 ユーザー補助サービスの設定を行います。 ●開発者向けオプション 端末の開発者向け機能です。 ●端末情報 端末のバージョン情報の確認やソフトウェアの更新などを行います。

項番	項目		説明
		機種(キャリア)固有メニュー	禁止する項目にチェックを入れます。 ●ドコモサービス ドコモが固有で設定しているサービスの設定を行います。 ●ホーム選択 ホームアプリの切り替えを行います。 ●WiMAX WiMAX の設定を行います。 ●モバイルネットワーク データローミングやエリア設定などを行います。 ●PC に接続 USB で PC に接続するときの接続タイプの設定を行います。

7.3.4 機能制限

カメラ、SD カード、Bluetooth の各機能を制限します。

本機能では、カメラや SD カードなどの使用を制限する設定セットを作成することができます。

7.3.5 機能制限／カメラ

端末のカメラ起動を禁止するための設定セットを作成します。

本機能でカメラ機能を禁止にした場合、端末でカメラを起動するとメッセージが表示され、カメラ機能を利用できなくなります。

カメラを利用するアプリでは、アプリの起動はできますが、カメラ機能を利用することはできなくなります。

アプリがカメラの利用を試みたタイミングで禁止メッセージが表示されます。その後、アプリが継続して利用できるかどうかは各アプリの仕様に依存します。

Android 12 以上では、端末の設定で「カメラへのアクセス」を有効に設定していない場合、カメラは使用できません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

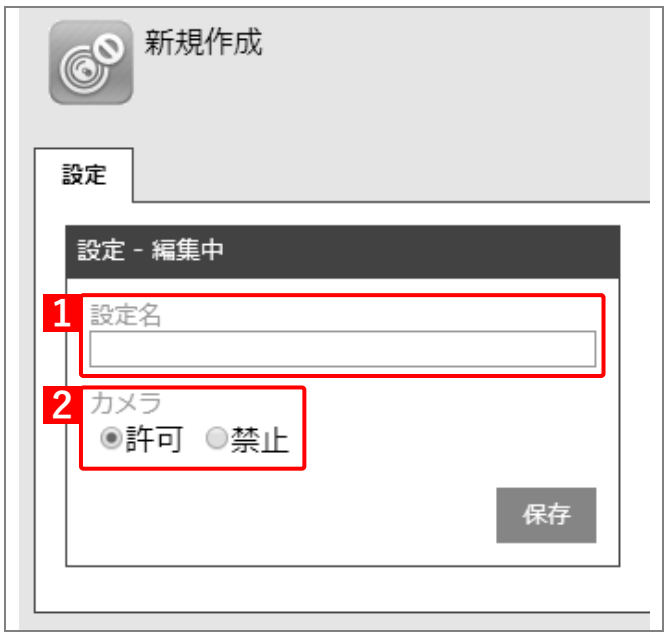
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［セキュリティ］→［機能制限］→［カメラ］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	カメラ	カメラの禁止／許可を以下から選択します。 ●許可 カメラ機能を利用できます。 ●禁止 カメラ機能を利用できません。

7.3.6 機能制限／SD カード

端末の SD カードをアンマウントし、SD カードの利用を禁止するための設定セットを作成します。本機能で SD カードの利用を禁止した場合、アプリから SD カードが利用できなくなります。

Android 4.2 以上では、SD カードの利用を制限できます。
なお、OS によって挙動が異なるため、ご利用のときは注意ください。

- Android 4.2 の場合、SD カード内のデータを初期化します。
- Android 4.3～4.4 のバージョンで、エージェントバージョン 7.1 以上の場合、SD カード挿入時にロック画面が表示されます。また、一部の Android 4.3 の端末では SD カードのワイプに対応しています。

本機能に対応している対応している端末の詳細については、以下を参照してください。

『Android エージェント対応端末表』

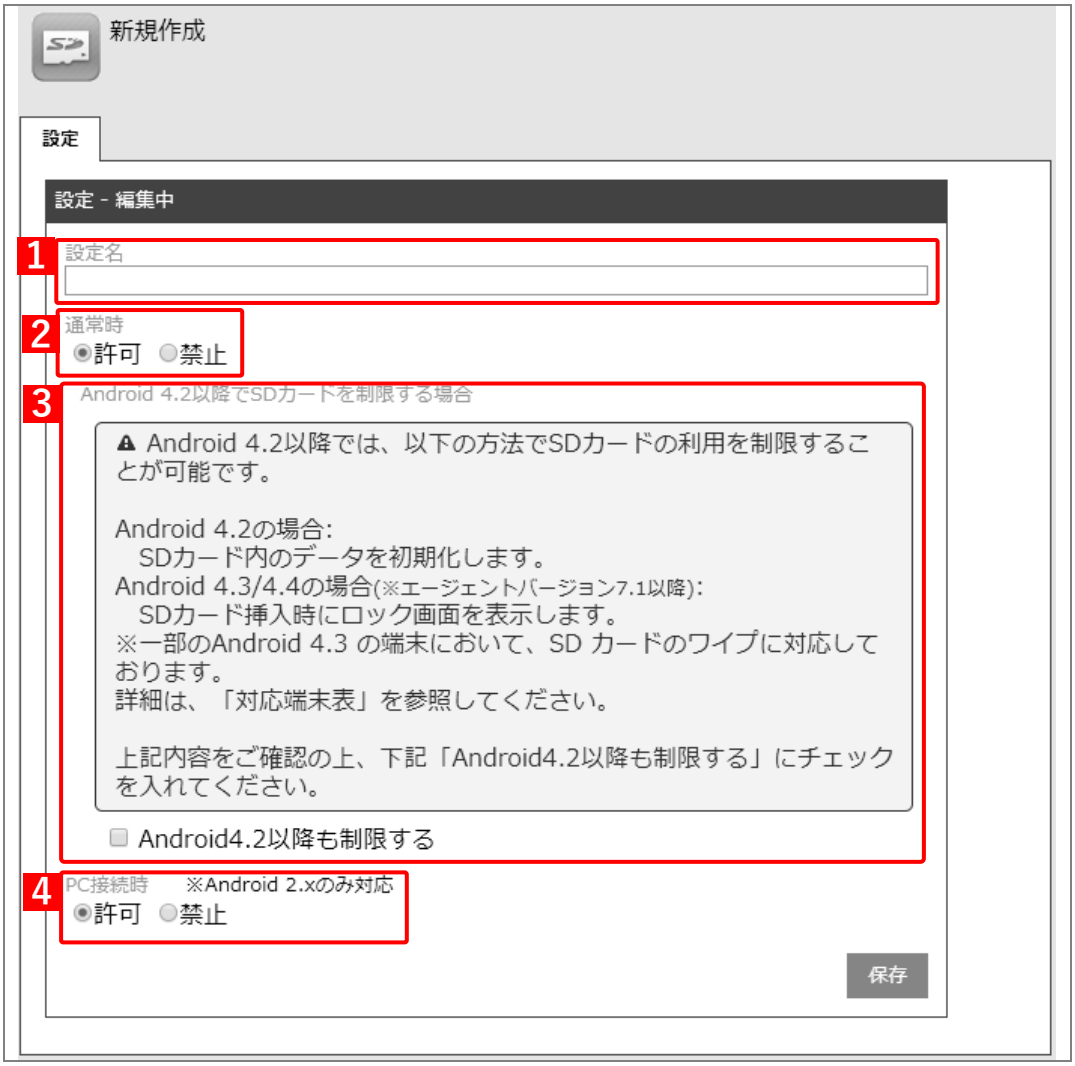
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ
「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［セキュリティ］→［機能制限］→［SD カード］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	通常時	通常時の SD カード利用の許可／禁止を以下から選択します。 ●許可 SD カードを利用できます。 ●禁止 SD カードを利用できません。
3	Android 4.2 以降で SD カードを制限する場合	Android 4.2 以上の端末でも SD カードの利用制限をする場合に設定します。 ●Android 4.2 以上も制限する 利用制限をする場合は、チェックを入れます。 Android 4.2 以上の場合は、バージョンによって SD カードの利用制限の内容が異なります。表示された制限の内容を確認してください。
4	PC 接続時	端末をパソコンに接続している場合の SD カード利用の許可／禁止を以下の項目から選択します。 ●「許可」、「禁止」 Android 2.x のみに対応しています。

7.3.7 機能制限／Bluetooth

端末の Bluetooth 機能を制限するための設定セットを作成します。

端末の Bluetooth 機能を有効または無効に設定します。また、各機器で設定された Bluetooth 機能設定のままにすることもできます。

端末を機内モードに設定していると、本機能は端末に反映されません。

端末の Bluetooth が ON/OFF どちらの場合でも、本設定が優先されます。

端末で Bluetooth の使用を禁止する場合は、以下で設定を行ってください。

「セキュリティ設定（DOM）」364 ページ

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［セキュリティ］→［機能制限］→［Bluetooth］→ ✚

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	Bluetooth 機能	Bluetooth 機能の利用の有効／無効を以下から選択します。 ●変更しない 各機器によって設定されている設定を変更しません。 ●有効にする 端末の Bluetooth 機能を有効にします。 ●無効にする 端末の Bluetooth 機能を無効にします。 Android 8.x の場合は、「無効にする」を選択した設定を端末に適応し、端末で Bluetooth 機能を有効にすると、通知領域の簡易設定画面のスイッチが ON（有効）になります。ただし、実際に「無効にする」の設定が適応されるため、Bluetooth 機能は利用できません。 Android 12 以上は、端末の設定で「付近のデバイス」権限を許可するに設定している場合は、Bluetooth の切り替えが行えます。

7.4 アプリケーション

Android 端末のアプリに関連する設定、および設定セットを作成します。

本機能では、特定のアプリの使用禁止や端末にインストールされた特定のアプリの検知を行うことができます。

また、Android Enterprise を利用したアプリの配信、アプリ権限ポリシーを設定することができます。

7.4.1 アプリケーション禁止

アプリの使用を禁止するための設定セットを作成します。

本画面では、以下の禁止ルールを設定することができます。

また、CSV ファイルを利用して、許可または禁止するアプリを一括で管理サイトに登録することもできます。

●許可するアプリケーションを指定してルールを作成（ホワイトリスト形式）

・アプリケーション名とパッケージ名を指定して、アプリの利用を許可する。

●禁止するアプリケーションを指定してルールを作成（ブラックリスト形式）

・アプリケーション名とパッケージ名を指定して、アプリの利用を禁止する。

●すべてのアプリケーションのインストールを禁止

●指定した画面の表示を禁止

禁止するアプリにより、OS の動作に支障をきたす（エージェント停止、OS 強制再起動を繰り返す、Android Recovery 画面になるなど）場合があります。システムアプリを禁止するときは、特に注意してください。システムアプリを禁止した場合、どのような挙動になるかについては、ご利用の端末や OS に依存するため、弊社ではご案内はできかねます。

禁止対象のアプリは起動できません。

Android 4.0 以上の端末の場合、カメラ機能を含むアプリは、カメラ機能の画面で「許可」を選択していなくても起動することができます。

「アプリケーション禁止」機能は、起動した画面を検知して禁止する機能です、そのため、バックグラウンドで動作するアプリは禁止できません。

カメラや Bluetooth などの使用を禁止する場合は、「機能制限」を利用してください。詳細については、以下を参照してください。

☞「機能制限」315 ページ

Web アプリ（ショートカット）は禁止できません。

本製品のエージェントアプリを禁止することはできません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

☞「(設定－Android) 設定の割り当て」75 ページ

☞「全機器一括設定」200 ページ

本機能を設定した場合、端末の挙動は以下のとおりです。

・ホームとアプリ一覧での表示：表示される

・アプリ画面の表示：停止

・バックグラウンドでの挙動：実行

アプリケーション非表示を設定した場合は、以下を参照してください。

☞「アプリケーション非表示」369 ページ

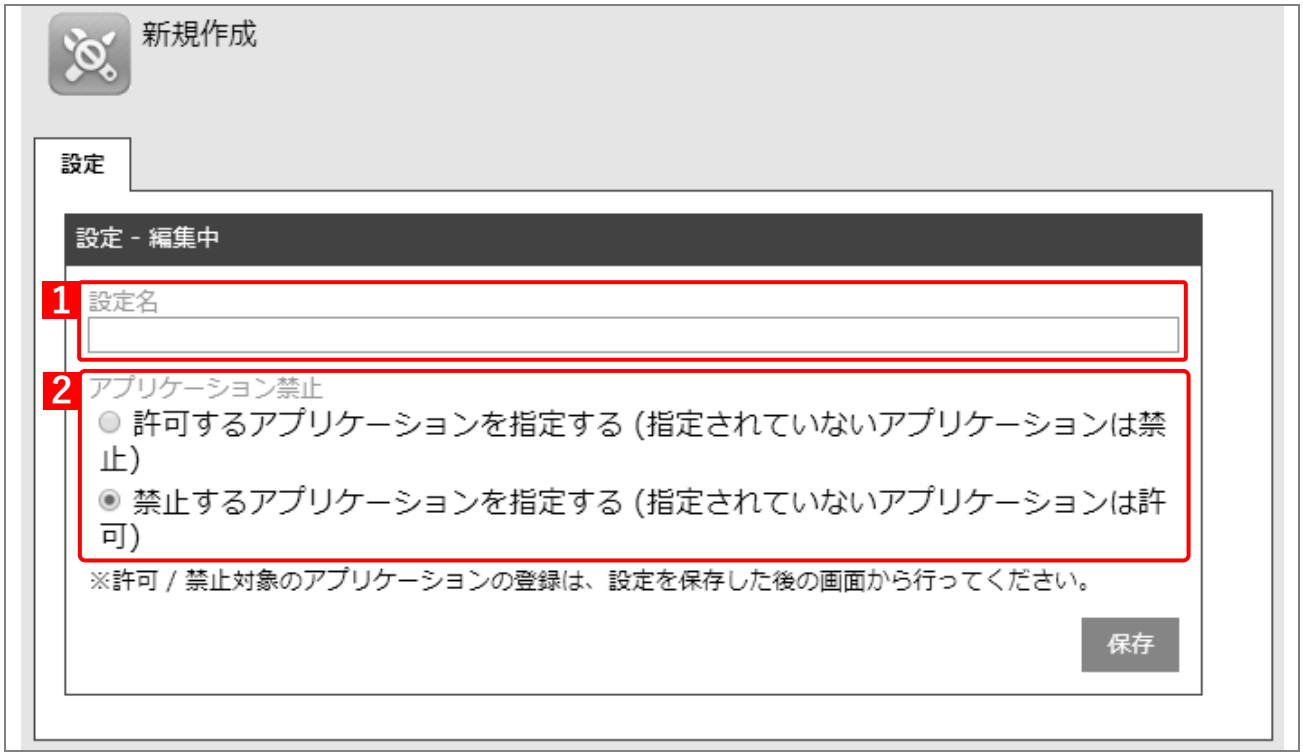
設定セットは、最大 50 件まで作成できます。

7.4.1.1 ［設定］タブ

画面（新規作成）
画面（編集）

◆画面（新規作成）

表示操作［設定］→［Android］→［アプリケーション］→［アプリケーション禁止］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	アプリケーション禁止	アプリの禁止方法を以下から選択します。 ●許可するアプリケーションを指定する(指定されていないアプリケーションは禁止) 指定されたアプリのみ使用できます。 ●禁止するアプリケーションを指定する(指定されていないアプリケーションは許可) 指定されたアプリは使用できません。

◆画面（編集）

表示操作［設定］→［Android］→［アプリケーション］→［アプリケーション禁止］→一覧から対象を選択

項番	項目	説明
1	インポート・エクスポート	CSV ファイルを利用して、許可または禁止するアプリを一括で管理サイトに登録できます。また、現在設定されているアプリの一覧を、CSV ファイルとして保存することもできます。 操作手順については、以下を参照してください。 『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」 本項目は、設定セットの作成後に表示されます。 ●対象アプリケーション一覧を CSV ファイルからインポート クリックすると、CSV ファイルのインポート画面が表示されます。 ●対象アプリケーション一覧を CSV ファイルでエクスポート 禁止している対象アプリの一覧を、CSV ファイルとしてダウンロードします。

項番	項目	説明
2	対象アプリケーション	アプリケーション名とパッケージ名を指定して、対象アプリを登録します。1 つの設定セットにつき、1000 件まで登録できます。 （追加）、（削除）、（編集）、（保存）、（取り消し）を使って操作します。 この項目は、設定を作成したあとに表示されます。 アプリを 31 個以上登録した場合は、端末によって本設定が有効になるまでに時間がかかることがあります。 ●アプリケーション名 アプリ名を入力します。機器が登録されている場合は、入力された文字を機器に登録されているすべてのアプリの中から関連するアプリケーションを表示します。 ●パッケージ名 アプリのパッケージ名を入力します。 パッケージ名は、対象端末にインストールされているアプリの一覧から確認できます。詳細については、以下を参照してください。 「（情報－Android）アプリケーション」141 ページ
3	［メモから追加］	各端末のアプリ一覧で、「メモ」列に が表示されているアプリが追加されます。アプリ一覧については、以下を参照してください。 「（情報－Android）アプリケーション」141 ページ

◆エラー一覧

文言	発生契機	対処方法
⚠ メモに存在する全てのアプリはインストールされていません。	メモに1つもアプリが登録されていない状態で「メモから追加」をクリックしている。 もしくは、すでにアプリケーション禁止に設定されているアプリを「メモから追加」で追加しようとしている。	メモに何も登録されていない場合は、禁止したいアプリをメモに登録してください。 すでにアプリケーション禁止設定に、メモに登録されているアプリが含まれている場合は「メモから追加」を押さずに［保存］してください。

7.4.1.2 ［高度な設定］タブ

注意

●本機能は、従来版エージェントのみに対応しています。従来版エージェントのサポートは終了したので、ストア版エージェントを利用してください。ストア版エージェントでのアプリ配信については、以下を参照してください。

「Android Enterprise」327 ページ

『Android Enterprise アプリケーション配信 手順書』

◆画面

表示操作 ［設定］→［Android］→［アプリケーション］→［アプリケーション禁止］→一覧から対象を選択→［高度な設定］タブ→［編集］

7.4.2 アプリケーション検知

端末にインストールされたアプリの一覧から、指定した条件に一致するものを検知し、結果をログに表示する設定セットを作成します。

アプリの検知は、端末ごとに 1 日に 1 回ランダムなタイミングで実行されます。

本機能は、設定セットを適用する前に端末にインストールされていたアプリに対しても有効です。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

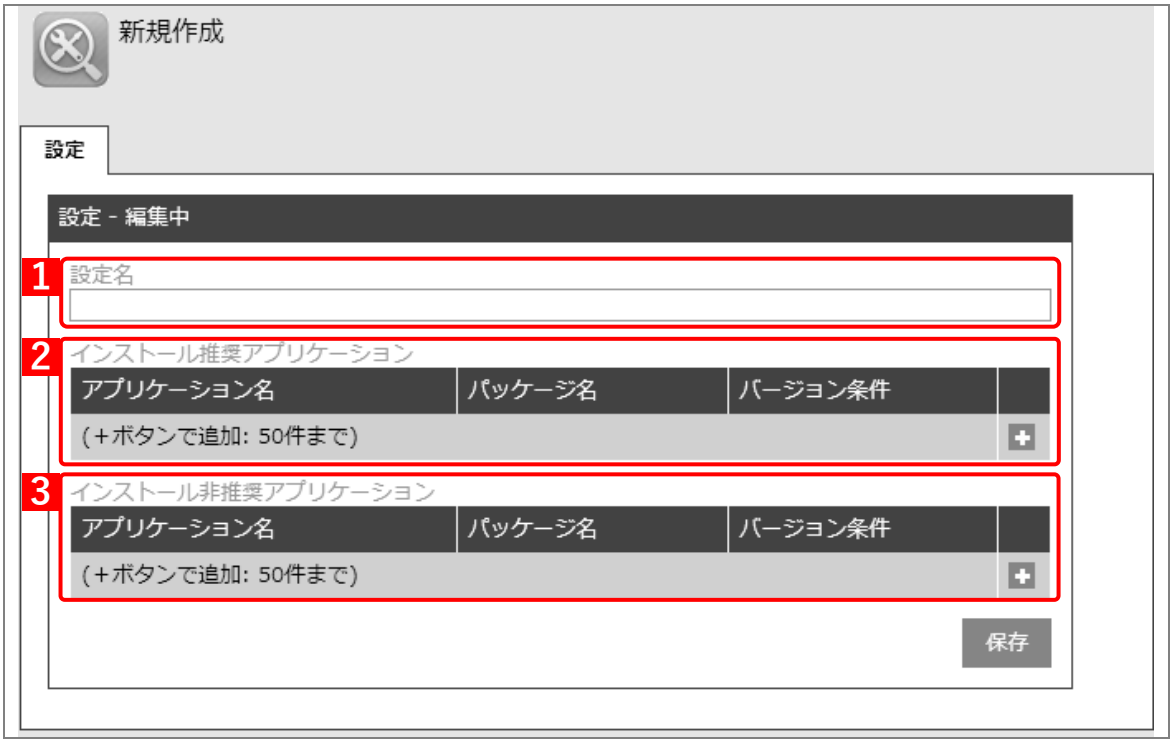
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［アプリケーション］→［アプリケーション検知］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	インストール推奨アプリケーション	インストールを推奨するアプリケーションを指定します。指定したアプリが端末にインストールされていない場合は、検知されます。1 つの設定セットにつき、50 件まで登録できます。 ●アプリケーション名 アプリ名を 60 文字以内で入力します。入力必須です。アプリ名は端末のアプリ情報で確認できます。 ●パッケージ名 パッケージの名称を 255 文字以内の半角英数字、「.」、「_」、「$」で入力します。入力必須です。パッケージ名は端末のアプリ情報から確認できます。 ●バージョン条件 ・以下の項目から選択します。 ・「全て」、「≧」、「＞」、「≦」、「＜」、「＝」 ・バージョン情報を 0 から 2147483647 の半角数字と「.」、「-」で入力します。入力必須です。 入力例 ABC アプリのバージョン 2.0 以上を推奨アプリケーションにする場合 アプリケーション名：ABC アプリ パッケージ名：com.xxxx.xxxx バージョン条件：≧2.0
3	インストール非推奨アプリケーション	インストールを推奨しないアプリケーションを指定します。指定したアプリが端末にインストールされている場合は、検知されます。1 つの設定セットにつき、50 件まで登録できます。 ●アプリケーション名 アプリ名を 60 文字以内で入力します。入力必須です。アプリ名は端末のアプリケーション情報から確認できます。 ●パッケージ名 パッケージの名称を 255 文字以内の半角英数字、「.」、「_」、「$」で入力します。入力必須です。パッケージ名は端末のアプリ情報から確認できます。 ●バージョン条件 ・以下の項目から選択します。 ・「全て」、「≧」、「＞」、「≦」、「＜」、「＝」 ・バージョン情報を 0 から 2147483647 の半角数字と「.」、「-」で入力します。入力必須です。 入力例 ABC アプリのバージョン 2.0 未満を非推奨アプリケーションにする場合 アプリケーション名：ABC アプリ パッケージ名：com.xxxx.xxxx バージョン条件：＜2.0

7.4.3 Android Enterprise

Android Enterprise を利用して、managed Google Play ストアのアプリケーションを配信します。

本機能は、アプリケーション配信のための各種設定や、アプリ権限ポリシーを設定します。

あらかじめ Android Enterprise アカウントを登録してください。アカウントが登録されていない場合は、表示されるメッセージ画面で［アカウント登録］をクリックし、Android Enterprise アカウントを登録してください。Android Enterprise アカウントの登録については、以下を参照してください。

「Android Enterprise（企業アカウント登録）」643 ページ

『Android キッティングマニュアル』

Android 端末で、ストア版エージェントを Device Owner Mode 化してください。

Android Enterprise では、有料アプリの配信はできません。「アプリ内課金あり」のアプリを配信した場合は、追加機能の購入などはできません。

7.4.4 Android Enterprise／アプリケーション配信

Android Enterprise に対応した端末に、managed Google Play ストアのアプリを配信するための設定セットを作成します。

画面（新規作成：［全てのアプリをインストール可能］を選択した場合）

画面（新規作成：［企業許可アプリのみインストール可能］を選択した場合）

画面（新規作成：［指定アプリのみインストール可能］を選択した場合）

画面（一括配信）

企業で許可したアプリだけを配信する場合は、事前に「企業許可アプリ」でアプリを登録してください。

「Android Enterprise／企業許可アプリ」338 ページ

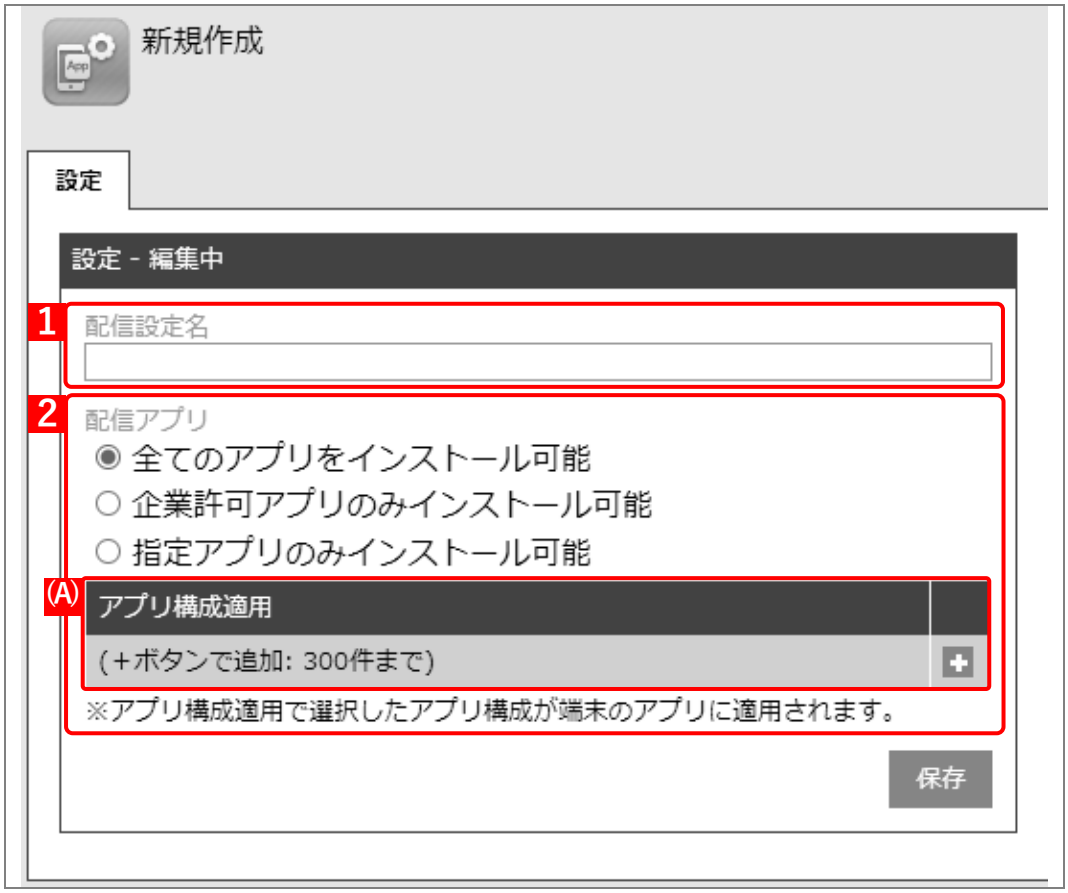
作成した設定セットは、ユーザーまたはユーザーの所属組織に割り当てることで、機器に適用されます。
ユーザーの所属組織に割り当てる場合は、ユーザーの「Android Enterprise アプリ配信設定」を「(所属組織に従う:設定なし)」に設定してください。

「［その他▼］タブ／設定」270 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成：［全てのアプリをインストール可能］を選択した場合）

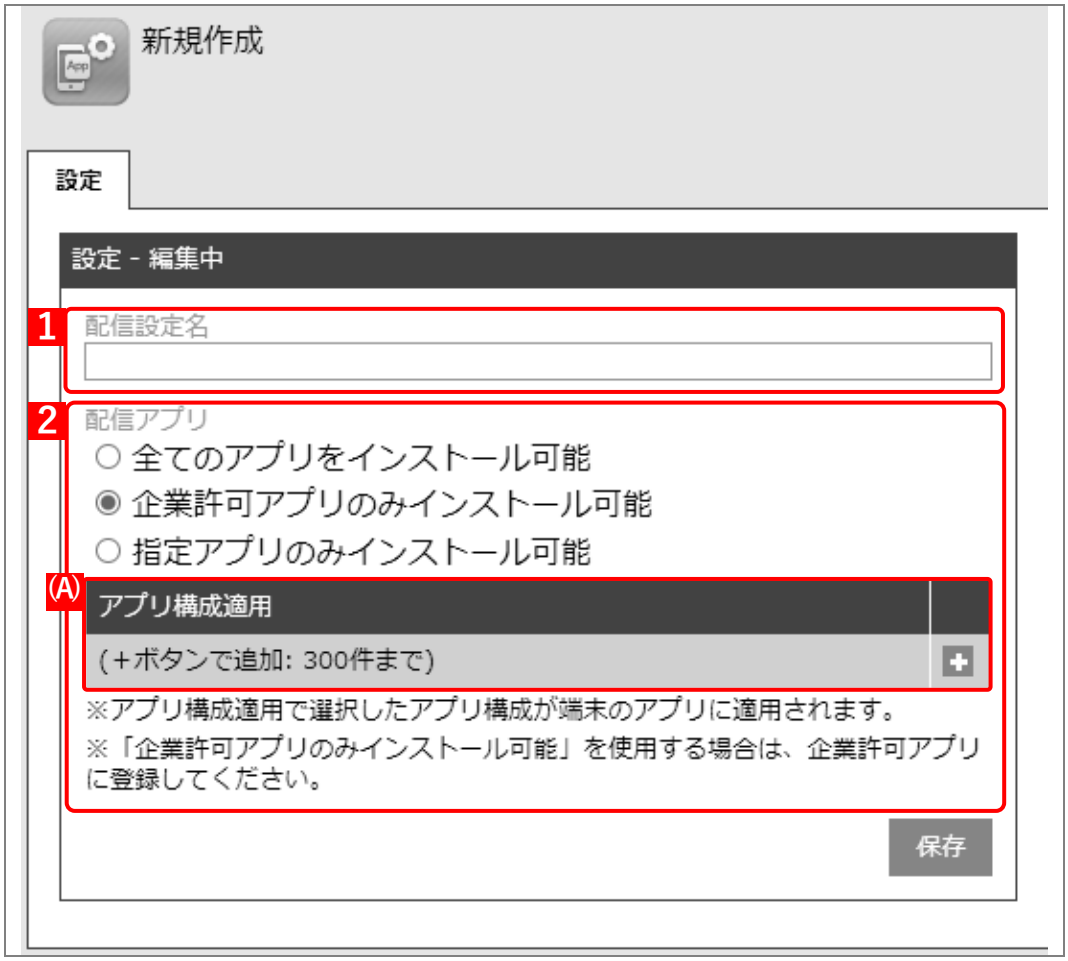
表示操作　［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［アプリケーション配信］→ ✚ →［全てのアプリをインストール可能］



項番	項目	説明
1	配信設定名	配信設定の名称を 1 文字から 30 文字で入力します。
2	配信アプリ	［全てのアプリをインストール可能］を選択した場合は、managed Google Play ストアに公開されているすべてのアプリを配信します。 詳細については、以下のマニュアルを参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」ー「すべてのアプリのインストールを許可する」ー「アプリケーション配信設定を作成する」 配信するアプリには、「アプリ構成」の設定値を付加することもできます。その場合は、「アプリ構成」を適用したアプリ個別設定を作成し、(A)「アプリ構成適用」に追加してください。1 設定に 300 件まで登録できます。また、同じ「アプリ構成」を重複して設定することはできません。 「アプリ構成」の詳細およびアプリ個別設定を作成方法については、以下を参照してください。 「Android Enterprise／個別アプリケーション」333 ページ

◆画面（新規作成：［企業許可アプリのみインストール可能］を選択した場合）

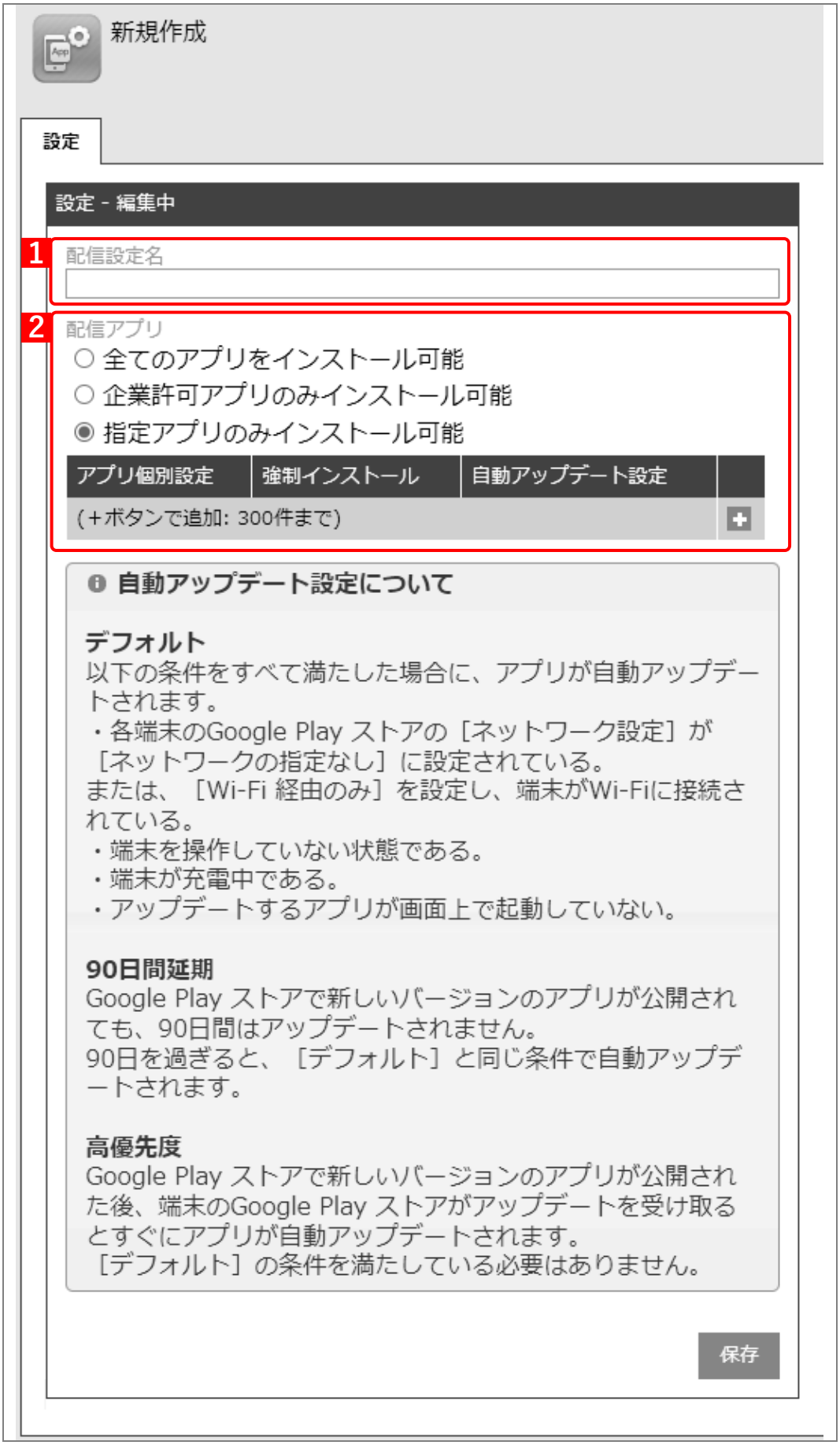
表示操作　［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［アプリケーション配信］→ ✚ →［企業許可アプリのみインストール可能］



項番	項目	説明
1	配信設定名	配信設定の名称を 1 文字から 30 文字で入力します。
2	配信アプリ	［企業許可アプリのみインストール可能］を選択した場合は、managed Google Play ストアに公開されているすべてのアプリのうち、「企業許可アプリ」に登録されているアプリのみ配信します。 詳細については、以下のマニュアルを参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」ー「管理者が登録したアプリのみインストールを許可する」ー「アプリケーション配信設定を作成する」 あらかじめ配信するアプリを「企業許可アプリ」に追加してください。 「Android Enterprise／企業許可アプリ」338 ページ 配信するアプリには、「アプリ構成」の設定値を付加することもできます。その場合は、「アプリ構成」を適用したアプリ個別設定を作成し、(A)「アプリ構成適用」に追加してください。1 設定に 300 件まで登録できます。また、同じ「アプリ構成」を重複して設定することはできません。 「アプリ構成」の詳細およびアプリ個別設定を作成方法については、以下を参照してください。 「Android Enterprise／個別アプリケーション」333 ページ

◆画面（新規作成：［指定アプリのみインストール可能］を選択した場合）

表示操作　［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［アプリケーション配信］→ ✚ →［指定アプリのみインストール可能］



項番	項目	説明
1	配信設定名	配信設定の名称を 1 文字から 30 文字で入力します。
2	配信アプリ	［指定アプリのみインストール可能］を選択した場合は、managed Google Play ストアに公開されているすべてのアプリのうち、「企業許可アプリ」に登録されている、かつ「アプリ個別設定」が設定されているアプリのみ配信します。強制インストールは、この場合のみ設定できます。 以下の項目を設定します。1 設定に 300 件まで登録できます。また、同じ「アプリ構成」を重複して設定することはできません。 ●アプリ個別設定 配信するアプリの「アプリ個別設定」をリストボックスから選択します。 ●強制インストール 「する」にチェックを入れると、強制インストールします。 ●自動アップデート設定 アプリのアップデート方法を以下から選択します。 ・デフォルト 以下の条件をすべて満たした場合に、アプリが自動アップデートされます。 ・各端末の Google Play ストアの［ネットワーク設定］が［ネットワークの指定なし］に設定されている。または、［Wi-Fi 経由のみ］を設定し、端末が Wi-Fi に接続されている。 ・端末を操作していない状態である。 ・端末が充電中である。 ・アップデートするアプリが画面上で起動していない。 ・90 日間延期 Google Play ストアで新しいバージョンのアプリが公開されても、90 日間はアップデートされません。90 日を過ぎると、［デフォルト］と同じ条件で自動アップデートされます。 ・高優先度 Google Play ストアで新しいバージョンのアプリが公開されたあと、端末の Google Play ストアがアップデートを受け取ると、すぐにアプリが自動アップデートされます。［デフォルト］の条件を満たしている必要はありません。 端末で使用中のアプリがアップデートされる場合、アプリが終了し、ユーザーに影響を与える場合があります。 詳細については、以下のマニュアルを参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリを強制インストールする」、「オリジナルアプリをインストールする」、「ウェブアプリ（ショートカット）をインストールする」、「アプリ構成を利用してアプリをインストールする」－「アプリケーション配信設定を作成する」 あらかじめ配信するアプリを「企業許可アプリ」に追加し、「アプリ個別設定」を設定してください。 「Android Enterprise／企業許可アプリ」338 ページ 「Android Enterprise／個別アプリケーション」333 ページ 端末にインストール済みの本設定で指定したアプリ（バージョンアップ含む）をアンインストールしたい場合は、該当のアプリを本設定から外して端末に割り当ててください。該当のアプリはアンインストールされます。ただし、エージェントアプリはアンインストールされません。

◆画面（一括配信）

表示操作　［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［アプリケーション配信］→一覧から対象を選択

Android Enterprise のアプリケーション配信設定がないとき、またはアプリケーション配信設定を新規作成および編集しているときは、アプリを一括で配信することはできません。

項番	項目	説明
1	［配信］	クリックすると、Android Enterprise アプリ配信設定が割り当てられているユーザーの端末に、アプリを一括で配信します。 詳細については、以下を参照してください。 『Android Enterprise アプリケーション配信 手順書』の「その他」－「インストール／アップデートできないときは」－「参考」 Android Enterprise アプリ配信設定については、以下を参照してください。 「［その他▼］タブ／設定」270 ページ

7.4.5 Android Enterprise／個別アプリケーション

アプリごとにランタイムパーミッションやアプリ構成などを設定した設定セットを作成します。

画面（新規作成）

画面（編集画面）

画面（編集画面（旧アプリ構成））

「アプリケーション配信」の［指定したアプリのみインストール可能］を選択し、作成した設定セットを「アプリ個別設定」で指定すると、managed Google Play ストアから、設定したアプリを配信することができます。

「Android Enterprise／アプリケーション配信」327 ページ

1 つのアプリ個別設定に登録できるのは、1 つのアプリのみです。アプリごとに、1 つの設定セットが必要です。設定セットの件数に上限はありません。

アプリ個別設定で選択したいアプリは、「企業許可アプリ」に登録されている必要があります。未登録の場合は、「企業許可アプリ」に選択したいアプリを登録してください。

「Android Enterprise／企業許可アプリ」338 ページ

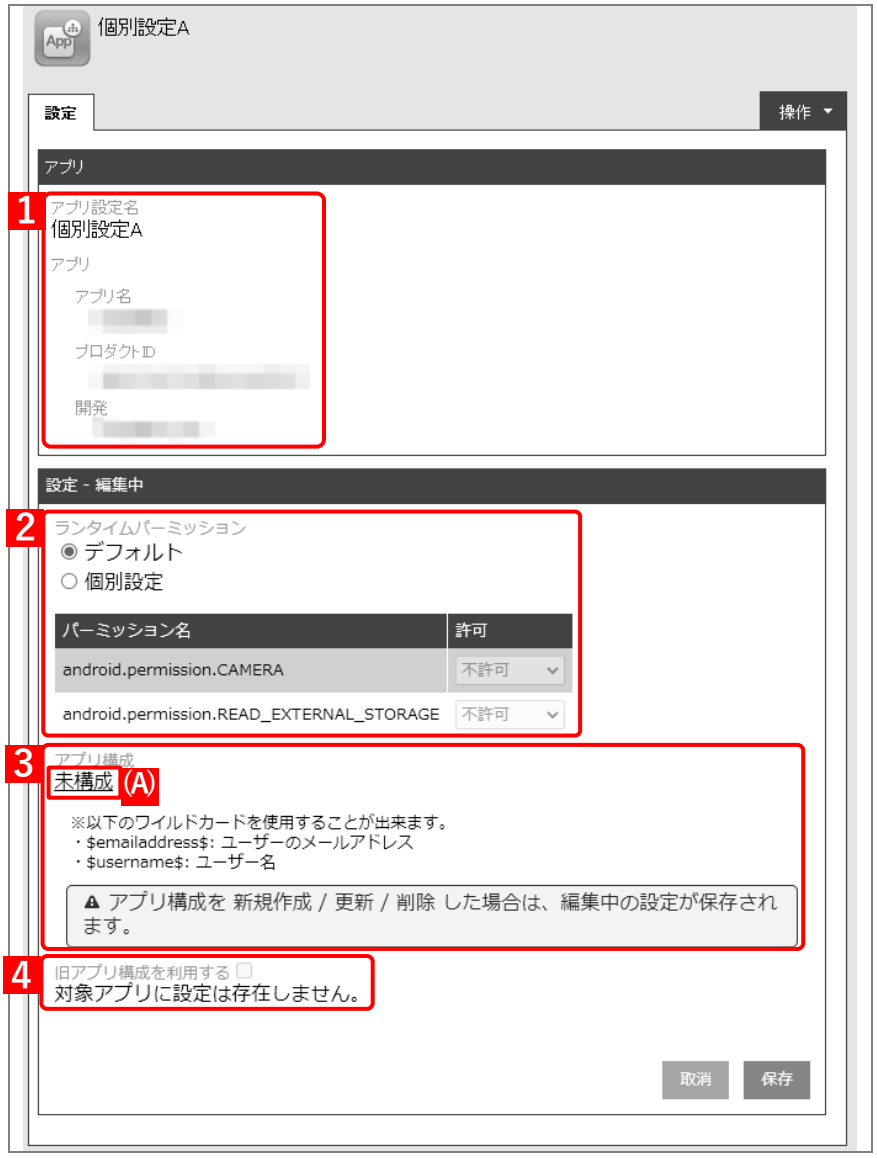
◆画面（新規作成）

表示操作　［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［個別アプリケーション］→ ✚

項番	項目	説明
1	アプリ設定名	アプリ設定の名称を 1 文字から 30 文字で入力します。 登録されているアプリ設定名は変更できません。変更が必要な場合は、不要な設定を削除してから、新しいアプリ設定名で再度、登録してください。
2	アプリ選択	［アプリを選択する］をクリックし、Google Play ストアからインストールするアプリを選択します。詳細については、以下のマニュアルを参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリを強制インストールする」、「オリジナルアプリをインストールする」、「ウェブアプリ（ショートカット）をインストールする」、「アプリ構成を利用してアプリをインストールする」－「アプリ個別設定を作成する」

◆画面（編集画面）

表示操作　**［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［個別アプリケーション］→一覧から対象を選択→［編集］**



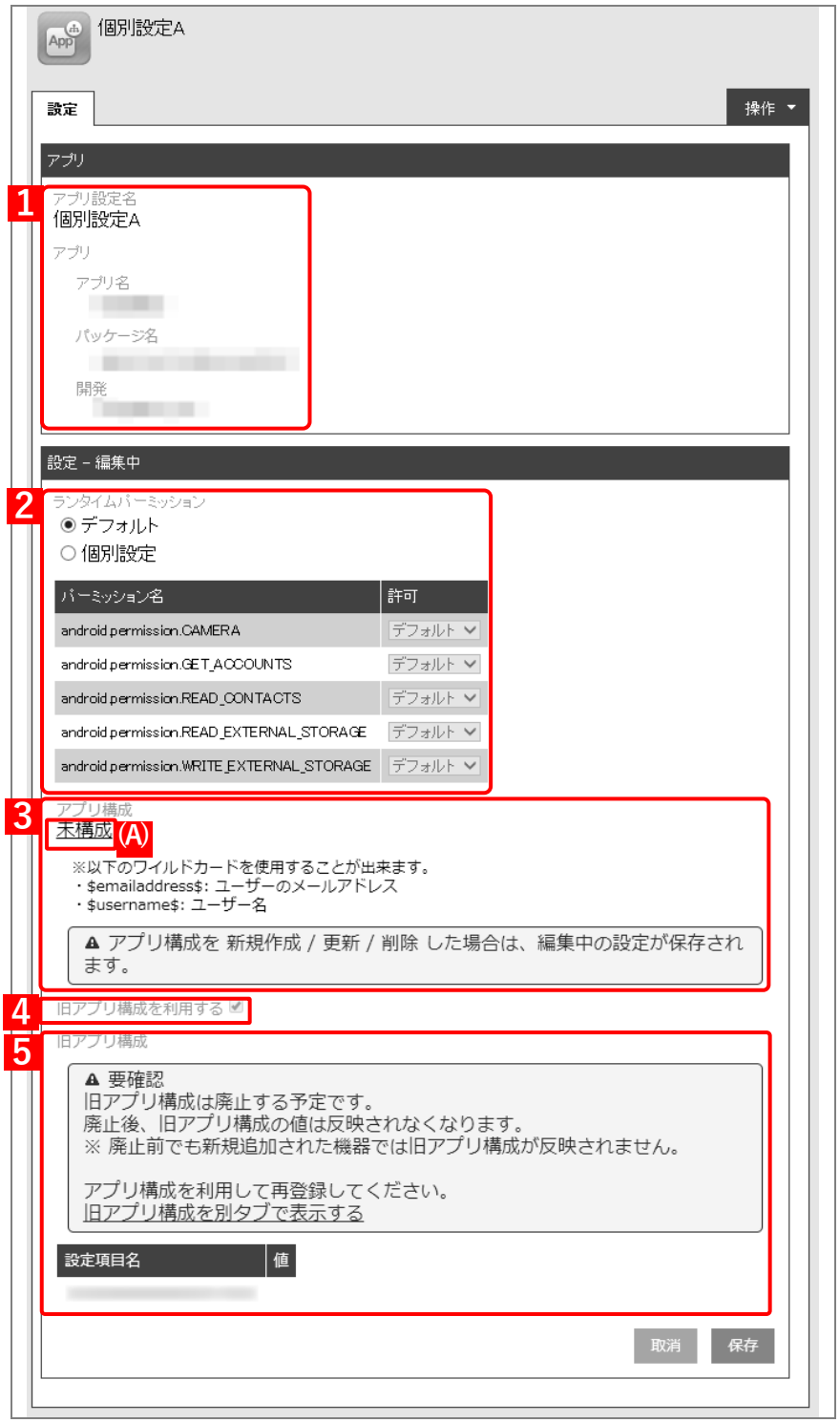
項番	項目	説明
1	アプリ設定名 アプリ	アプリ設定の名称とアプリ名、パッケージ名、開発元の情報が表示されます。
2	ランタイムパーミッション	アプリの機能の利用許可について以下から選択します。 ●デフォルト 端末でアプリを利用したときの動作は、「アプリ権限ポリシー」で設定したデフォルトのアプリ権限に従います。 「Android Enterprise／アプリ権限ポリシー」340 ページ ●個別設定 パーミッションごとに、以下の項目を設定できます。 ・デフォルト 端末でアプリを利用したときの動作は、「アプリ権限ポリシー」で設定したデフォルトのアプリ権限に従います。 ・許可 ユーザー操作なし（権限確認なし）で利用できます。 ・不許可 ユーザー操作なし（権限確認なし）で利用を禁止します。
3	アプリ構成	Managed configurations iframe で、アプリ構成を設定します。 （A）［未構成］をクリックすると、アプリ個別設定画面が表示されます。設定方法は以下を参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」ー「アプリ構成を利用してアプリをインストールする」ー「アプリ個別設定を作成する」
4	旧アプリ構成を利用する	旧アプリ構成を設定している場合は、チェックが入っています。

◆画面（編集画面（旧アプリ構成））

旧アプリ構成で設定された値は、無効になります。切り替えタイミングは未定ですが、旧アプリ構成で設定されている場合は、Google が提供する Managed configurations iframe を利用して、再登録を行ってください。再登録については、以下を参照してください。

『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリ構成を利用してアプリをインストールする」－「アプリ個別設定を作成する」

表示操作 ［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［個別アプリケーション］→一覧から対象を選択→［編集］



項番	項目	説明
1	アプリ設定名 アプリ	アプリ設定の名称とアプリ名、パッケージ名、開発元の情報が表示されます。
2	ランタイムパーミッション	アプリの機能の利用許可について以下から選択します。 ●デフォルト 端末でアプリを利用したときの動作は、「アプリ権限ポリシー」で設定したデフォルトのアプリ権限に従います。 「Android Enterprise／アプリ権限ポリシー」340 ページ ●個別設定 パーミッションごとに、以下の項目を設定できます。 ・デフォルト 端末でアプリを利用したときの動作は、「アプリ権限ポリシー」で設定したデフォルトのアプリ権限に従います。 ・許可 ユーザー操作なし（権限確認なし）で利用できます。 ・不許可 ユーザー操作なし（権限確認なし）で利用を禁止します。
3	アプリ構成	Managed configurations iframe で、アプリ構成を設定します。 （A）［未構成］をクリックすると、アプリ個別設定画面が表示されます。設定方法は以下を参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」ー「アプリ構成を利用してアプリをインストールする」ー「アプリ個別設定を作成する」
4	旧アプリ構成を利用する	旧アプリ構成で設定していると、チェックが入っています。
5	旧アプリ構成	旧アプリ構成が表示されています。 旧アプリ構成は、廃止されますので、アプリ構成の（A）［未構成］をクリックして再登録を行ってください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」ー「アプリ構成を利用してアプリをインストールする」ー「アプリ個別設定を作成する」

7.4.6 Android Enterprise／企業許可アプリ

managed Google Play ストアに公開されているアプリのうち、企業で使用を許可するアプリを追加します。追加したアプリは「企業許可アプリ」として管理サイトに登録されます。

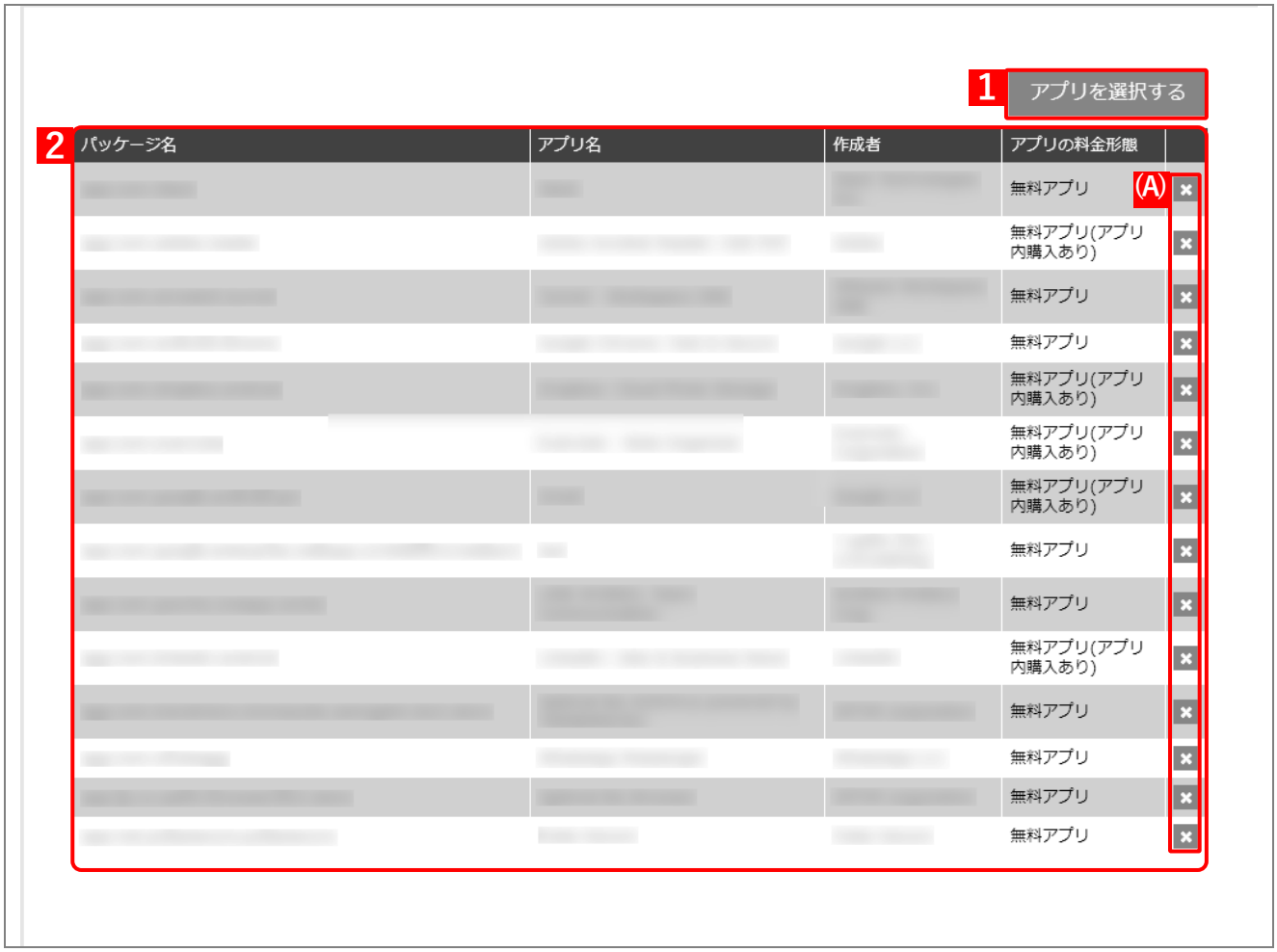
詳細については、以下のマニュアルを参照してください。

『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリを強制インストールする」、「オリジナルアプリをインストールする」、「アプリ構成を利用してアプリをインストールする」－「企業許可アプリを追加する」

企業許可アプリは、1,000 件まで登録できます。

◆画面

表示操作 ［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［企業許可アプリ］→ ✚



項番	項目	説明
1	［アプリを選択する］	クリックすると、managed Google Play ストアが表示されます。企業で許可するアプリを選択します。詳細については、以下のマニュアルを参照してください。 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリを強制インストールする」、「オリジナルアプリをインストールする」、「アプリ構成を利用してアプリをインストールする」－「企業許可アプリを追加する」
2	企業許可アプリ一覧	選択したアプリの以下の情報が表示されます。 ●パッケージ名 ●アプリ名 ●作成者 ●アプリの料金形態 企業許可アプリから削除する場合は、（A）をクリックします。

7.4.7 Android Enterprise／アプリ権限ポリシー

Android 端末で実行中のアプリが、カメラやアドレス帳などのアプリを使用するためにアクセス権限要求した場合、使用を許可、禁止、またはユーザー確認後に許可／禁止を判断するかを設定します。

本機能は、［個別アプリケーション］の「ランタイムパーミッション」で、［デフォルト］ラジオボタンを選択した場合、または［個別設定］をラジオボタン選択し、各パーミッションの「許可」項目で、リストボックスから［デフォルト］を選択した場合の、デフォルトの設定値として使用されます。

「Android Enterprise／個別アプリケーション」333 ページ

Android 端末としてのポリシーを設定することになります。Android Enterprise 連携を行い、Android 端末をキッティングした時点で、本機能は有効になります。

『Android キッティングマニュアル』

本機能で設定している場合でも、アプリが権限を要求する前に Android 端末の［設定］→［アプリ］で権限を付与することもできます。

本機能で設定したポリシーが、個別アプリケーションの「ランタイムパーミッション」でデフォルトになります。デフォルトを変更したい場合は、アプリごとにポリシーの変更を設定できます。個別アプリケーションで作成したアプリを Android Enterprise で配信すると、アプリごとに変更したポリシーが有効になります。

「Android Enterprise／個別アプリケーション」333 ページ

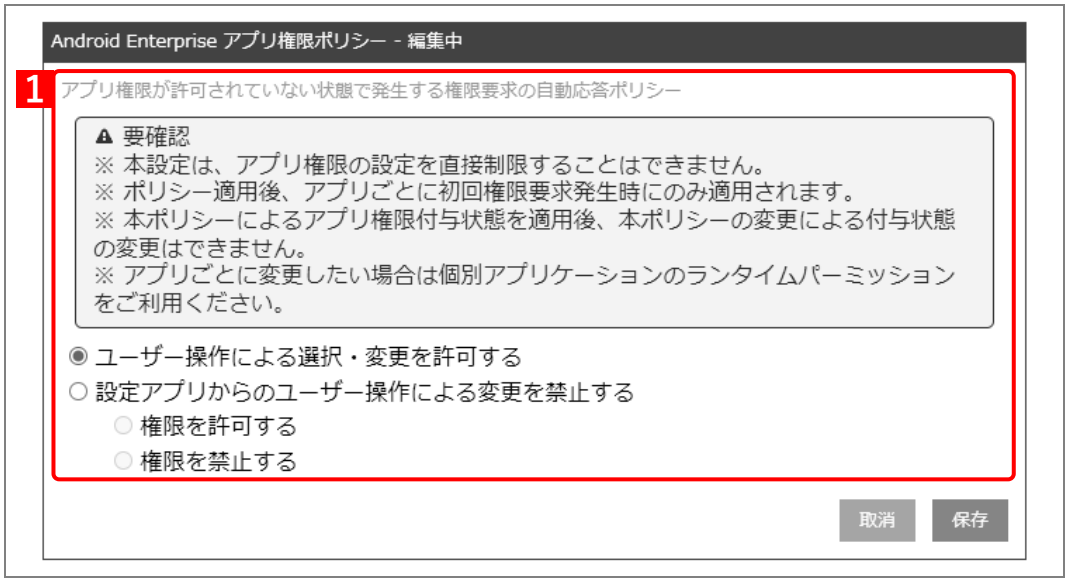
「Android Enterprise／アプリケーション配信」327 ページ

本機能の設定および個別アプリケーションの「ランタイムパーミッション」の設定したときの Android 端末の動作については、以下を参照してください。

「「アプリ権限ポリシー」の設定による Android 端末の動作」341 ページ

◆画面

表示操作　**［設定］→［Android］→［アプリケーション］→［Android Enterprise］→［アプリ権限ポリシー］→［編集］**



項番	項目	説明
1	アプリ権限が許可されていない状態で発生する権限要求の自動応答ポリシー	端末のアプリの利用について、デフォルトの設定を以下から選択します。 ●ユーザー操作による選択・変更を許可する アプリを実行するたびに権限が要求されます。ユーザー操作で権限を許可するかを選択するようにします。 ●設定アプリからのユーザー操作による変更を禁止する ・権限を許可する 権限の確認をすることなく、アプリを利用できます。アプリが権限を要求する契機で、ユーザー操作なし（権限確認なし）で許可されます。 ・権限を禁止する 権限の確認をすることなく、アプリを利用できます。アプリが権限を要求する契機で、ユーザー操作なし（権限確認なし）で禁止されます。 アプリ権限の設定を直接制限することはできません。 適用後は、アプリごとに初回権限要求発生時にのみ適用されます。 本設定による アプリ権限付与状態を適用後は、本設定の変更による付与状態の変更はできません。 アプリごとに変更する場合は、個別アプリケーションのランタイムパーミッションをご利用ください。

◆「アプリ権限ポリシー」の設定による Android 端末の動作

本機能の設定、および個別アプリケーションの「ランタイムパーミッション」を設定し、Android 端末でアプリを実行して、アクセス権限を要求されたときの、Android 端末の動作は以下のとおりです。

個別アプリケーションの「ランタイムパーミッション」の設定が優先になります。

個別アプリケーションのランタイムパーミッション	アプリ権限ポリシーの設定	Android 端末の動作
デフォルト	権限を許可する	権限を要求するダイアログは表示されません。 自動的に権限は「許可」されています。 ユーザーが権限を変更することはできません。
	権限を禁止する	権限を要求するダイアログは表示されません。 自動的に権限は「禁止」されています。 ユーザーが権限を変更することはできません。 アプリの利用は、アプリの仕様に依存します。
	ユーザー操作による選択・変更を許可する	権限を要求するダイアログが表示されます。 ユーザーが「許可」または「禁止」を選択できます。 通常利用時と同様です。
許可	—	権限を要求するダイアログは表示されません。 自動的に権限は「許可」されています。 ユーザーが権限を変更することはできません。
不許可	—	権限を要求するダイアログは表示されません。 自動的に権限は「禁止」されています。 ユーザーが権限を変更することはできません。 アプリの利用は、アプリの仕様に依存します。

7.5 インターネット

インターネットに関連する設定を行います。

Wi-Fi フィルタリングを設定することができます。

7.5.1 Wi-Fi フィルタリング

特定の無線 LAN アクセスポイントのみに端末の接続を許可する設定セットを作成します。他の SSID への Wi-Fi 接続はできなくなります。

誤った設定を行うと、Wi-Fi モデルは一切ネットワークに接続できなくなります。注意してください。

本製品の利用を解約しても、端末に行った設定はそのまま保持されます。解約の前に各種設定セットを［設定なし］に設定し、端末に反映してください。

Android 8.x の場合、本機能は Device Owner Mode でのみ動作します。Device Owner Mode でご利用いただかないと、本機能は動作しません。Device Owner Mode キッティング手順については、以下のマニュアルを参照してください。

『Android キッティングマニュアル』

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

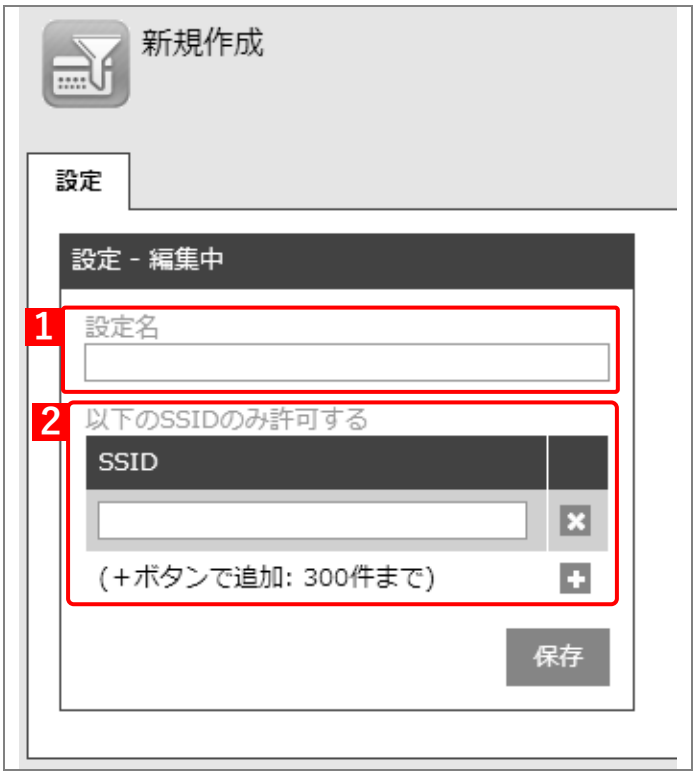
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［インターネット］→［Wi-Fi フィルタリング］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	以下の SSID のみ許可する	端末で接続を許可する Wi-Fi の SSID の名称を 32 文字以内の半角英数字、「-」、「_」、「@」で入力します。300 件まで登録できます。 をクリックすると、新規に追加できます。 SSID を 31 個以上登録した場合、ご使用の端末によっては Wi-Fi フィルタリングに時間がかかる場合があります。

7.6 便利機能

連絡先の登録などを行うことができます。

7.6.1 連絡先

端末の電話帳に連絡先を追加する設定セットを作成します。

画面（新規作成）

画面（編集）

端末に反映された連絡先の変更や削除はできません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成）

表示操作　［設定］→［Android］→［便利機能］→［連絡先］→ ＋

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。

◆画面（編集）

表示操作［設定］→［Android］→［便利機能］→［連絡先］→作成した設定を選択

項番	項目	説明
1	インポート・エクスポート	CSV ファイルから連絡先の登録をまとめて行います。また、現在登録されている連絡先を CSV ファイルに保存できます。 操作手順については、以下を参照してください。 『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」 ●連絡先一覧を CSV ファイルからインポート CSV ファイルに発信先をインポートする画面が表示されます。 ●連絡先一覧を CSV ファイルでエクスポート 選択している設定内容の発信先を CSV ファイルでダウンロードします。 エクスポートを実施すると「再度ダウンロードする場合は画面を更新してください。」と表示されます。 CSV ファイルを Excel で編集したとき、電話番号の頭文字の「0」が消えてしまいますので、セルの表示形式を「文字列」に指定してください。または、「TEL:0**********」と「TEL:」を付けて入力すると、頭文字の「0」は消えません。

項番	項目	説明
2	連絡先一覧	連絡先の情報を登録します。 をクリックし、以下の項目を入力して連絡先を登録します。最大 1,000 件登録できます。 登録するには、「姓」、「名」、「姓（フリガナ）」、「名（フリガナ）」のいずれかの入力が必要です。 ●姓 姓を 15 文字以内で入力します。 ●名 名を 15 文字以内で入力します。 ●姓（フリガナ） 姓のフリガナを 15 文字以内の全角カタカナ、半角カタカナ、半角空白で入力します。 ●名（フリガナ） 名のフリガナを 15 文字以内の全角カタカナ、半角カタカナ、半角空白で入力します。 ●電話番号 連絡先の電話番号を 20 文字以内の半角数字、「-」、「+」、「*」、「#」、「,」で入力します。 端末で電話番号を編集したときに、アプリの仕様で自動的にハイフン「-」が挿入されることがあります。ハイフン「-」の有無で、管理サイトから配信した連絡先のデータと重複する場合があります。 ハイフン「-」やスペースがあると、電話番号が同一と判断されず、連絡先のデータが重複する場合があります。 ●メールアドレス 連絡先メールアドレスを 255 文字以内の半角英数字、記号で入力します。「@」の前後にそれぞれ 1 文字以上入力してください。

7.6.2 SIM ステータス変更検知

SIM ステータス変更検知の設定セットを作成します。SIM ステータス変更検知は、SIM が抜かれた場合や SIM が挿入された場合に、ログを出力する機能です。

この設定は、Android と iOS で共有することができます。

端末を認証するとき、本設定が端末に割り当てられている場合、初回の同期でログが出力されます。

ネットワークが未接続の状態や同期ができない状態のときは、SIM を変更してもログは出力されません。

SIM のスロットが複数ある端末の場合、1 つめのスロットから SIM を抜いて、2 つめのスロットに SIM の挿入や入れ替えしてもログは出力されません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

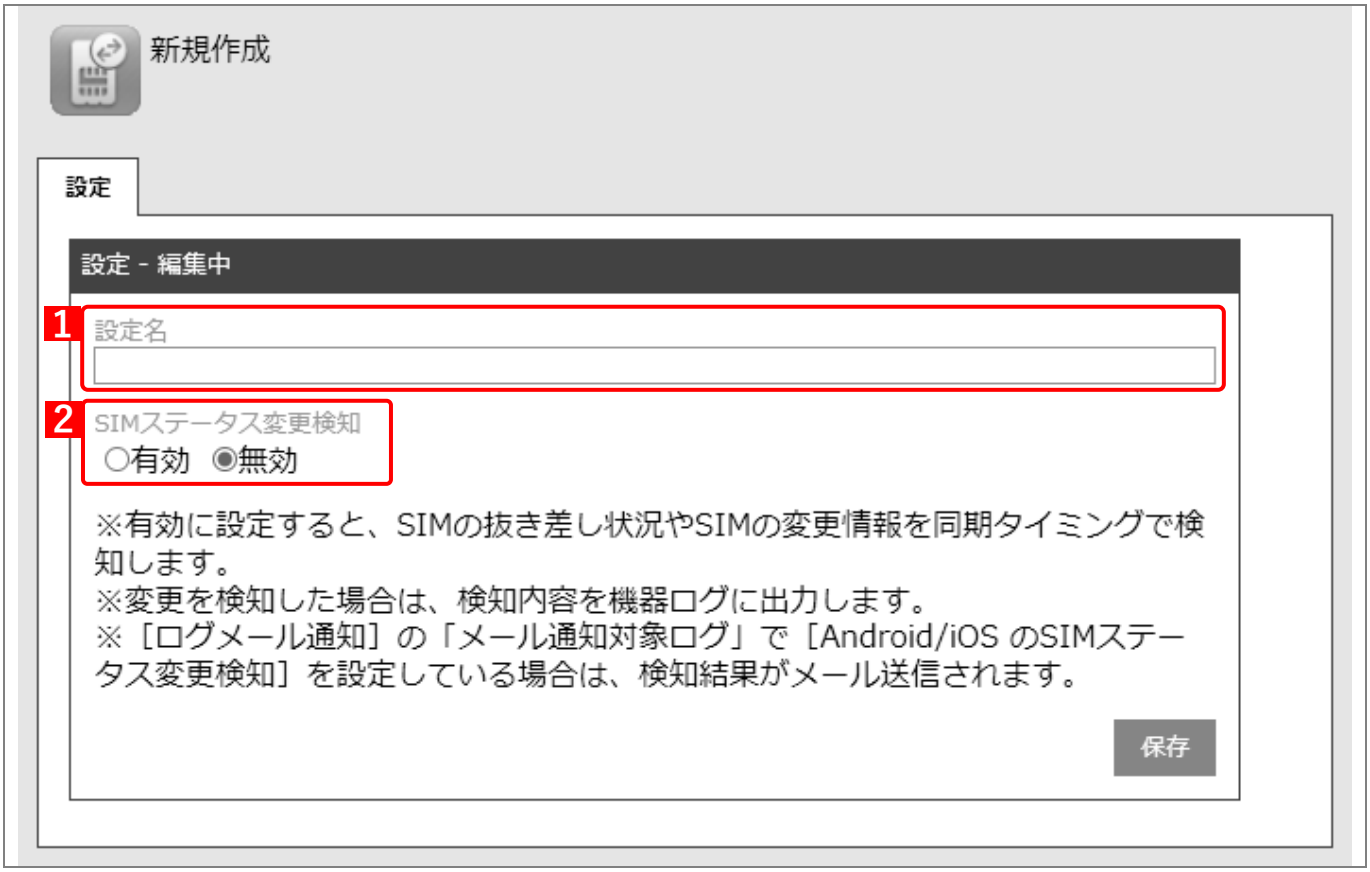
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［便利機能］→［SIM ステータス変更検知］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	SIM ステータス変更検知	有効に設定すると、SIM の抜き差し状況や SIM の変更情報を同期タイミングで検知します。

7.7 証明書管理

クライアント証明書の管理や一括アップロード、一括削除のほか、CA 証明書の管理を行います。

7.7.1 クライアント証明書管理

クライアント証明書を管理サイトに 1 ファイルずつアップロードして保存し、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

画面（新規作成）

画面（管理）

画面（編集）

事前にクライアント証明書を取得してください。

本製品はクライアント証明書の配信までを行います。端末内に保存されるクライアント証明書の場所やインストール方法については、端末メーカーへ問い合わせてください。

アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。

「画面（編集）」351 ページ

クライアント証明書をまとめてアップロードする場合は、以下を参照してください。

「クライアント証明書一括アップロード」352 ページ

管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。

「（設定－Android）クライアント証明書」79 ページ

「（設定－iOS）クライアント証明書」86 ページ

「（設定－iOS）Exchange（ActiveSync）設定」89 ページ

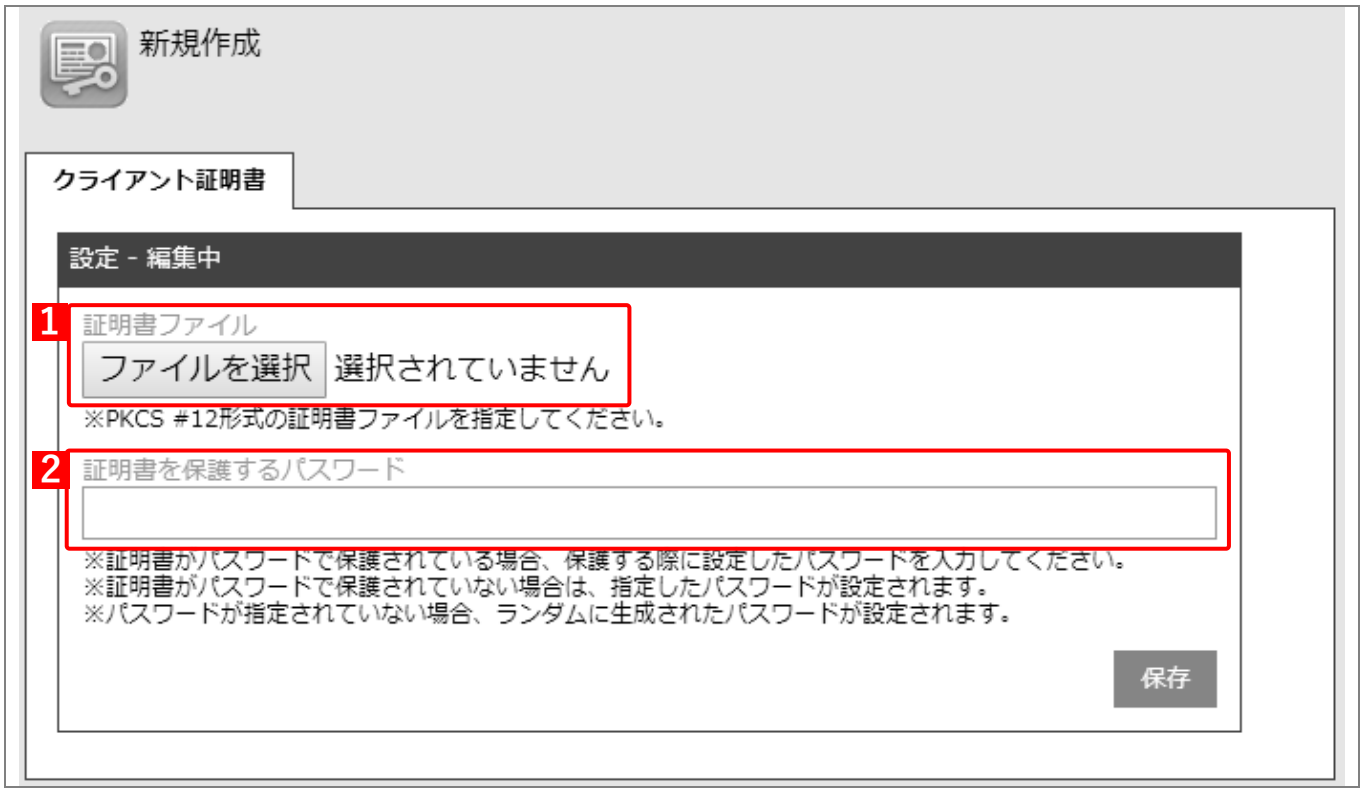
「（設定－iOS）VPN 設定」94 ページ

「（設定－Windows）クライアント証明書」106 ページ

設定セットは、最大で 500,000 件まで作成できます。

◆画面（新規作成）

表示操作［設定］→［Android］→［証明書管理］→［クライアント証明書管理］→ ✚



項番	項目	説明
1	証明書ファイル	アップロードするクライアント証明書を指定します。［ファイルを選択］をクリックし、クライアント証明書ファイルを選択します。 PKCS #12 形式のクライアント証明書を指定してください。 ファイル名は 30 文字以内で設定してください。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを 255 文字以内の半角英数字で入力します。 パスワード未設定の場合は入力不要です。

◆画面（管理）

表示操作　［設定］→［Android］→［証明書管理］→［クライアント証明書管理］

項番	項目	説明
1	検索/並び替え	（A）に検索対象項目、（B）に並び替えの対象項目が表示されます。 検索する場合は、検索するキーワードを（C）に入力し、［検索］をクリックします。検索したあとに、すべてのクライアント証明書を再表示するにはブラウザーを再読み込み、または（C）を空欄にし、再度［検索］ をクリックします。
2	✚	クリックするとクライアント証明書情報欄に入力欄が表示されます。 「画面（新規作成）」349 ページ
3	▼	クリックすると以下のメニューが表示されます。 ●全てにチェックを入れる 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスにチェックが入ります。 ●全てのチェックをはずす 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスのチェックが外れます。 ●検索対象 検索対象をファイル名、発行先（証明書情報）のいずれかに変更できます。 ●並べ替え 昇順 ユーザー一覧をファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで昇順に並び替えます。 ●並べ替え 降順 ファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで降順に並び替えます。 ●一括削除 クライアント証明書一覧でチェックの入っている証明書を削除します。
4	クライアント証明書一覧	登録されているクライアント証明書一覧が表示されます。 ●（D） クライアント証明書のファイル名です。 ●（E） 発行先（クライアント証明書情報）です。 ●（F） 有効期間です。
5	クライアント証明書情報	クライアント証明書一覧から選択したクライアント証明書の情報が表示されます。

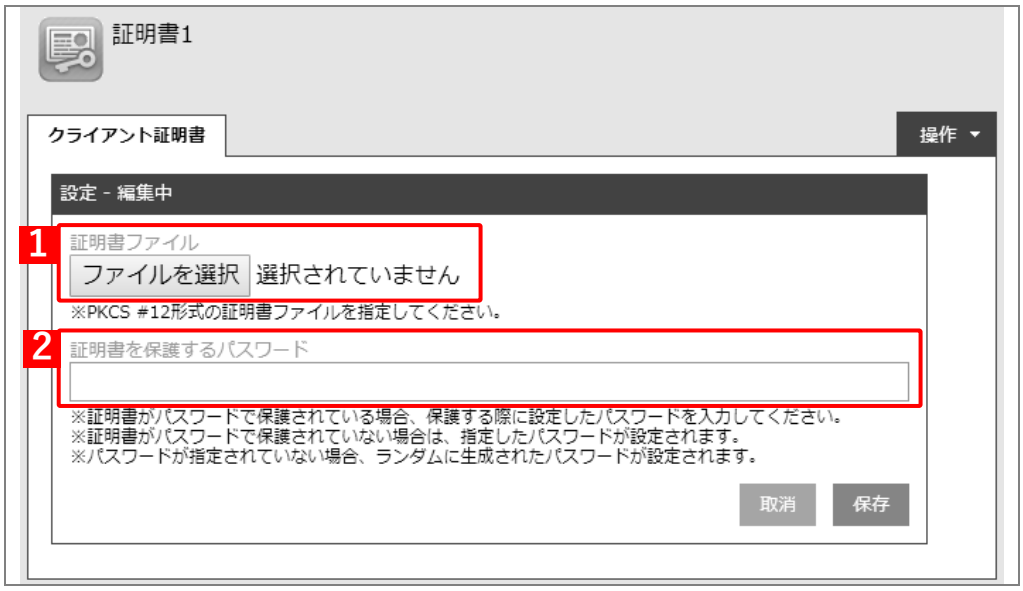
項番	項目	説明
6	［操作］	クリックすると以下のメニューが表示されます。 ●削除 クライアント証明書を削除します。
7	［編集］	クリックすると、登録されているクライアント証明書情報を編集できます。

◆画面（編集）

アップロード済みのクライアント証明書の差し替えやパスワードを変更する場合に内容を修正します。

設定項目は新規作成と同様です。

表示操作　**［設定］→［Android］→［証明書管理］→［クライアント証明書管理］→一覧から対象を選択→［編集］**



項番	項目	説明
1	証明書ファイル	クライアント証明書一覧から再アップロードする証明書を指定します。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを入力します。パスワード未設定の場合は入力不要です。

7.7.2 クライアント証明書一括アップロード

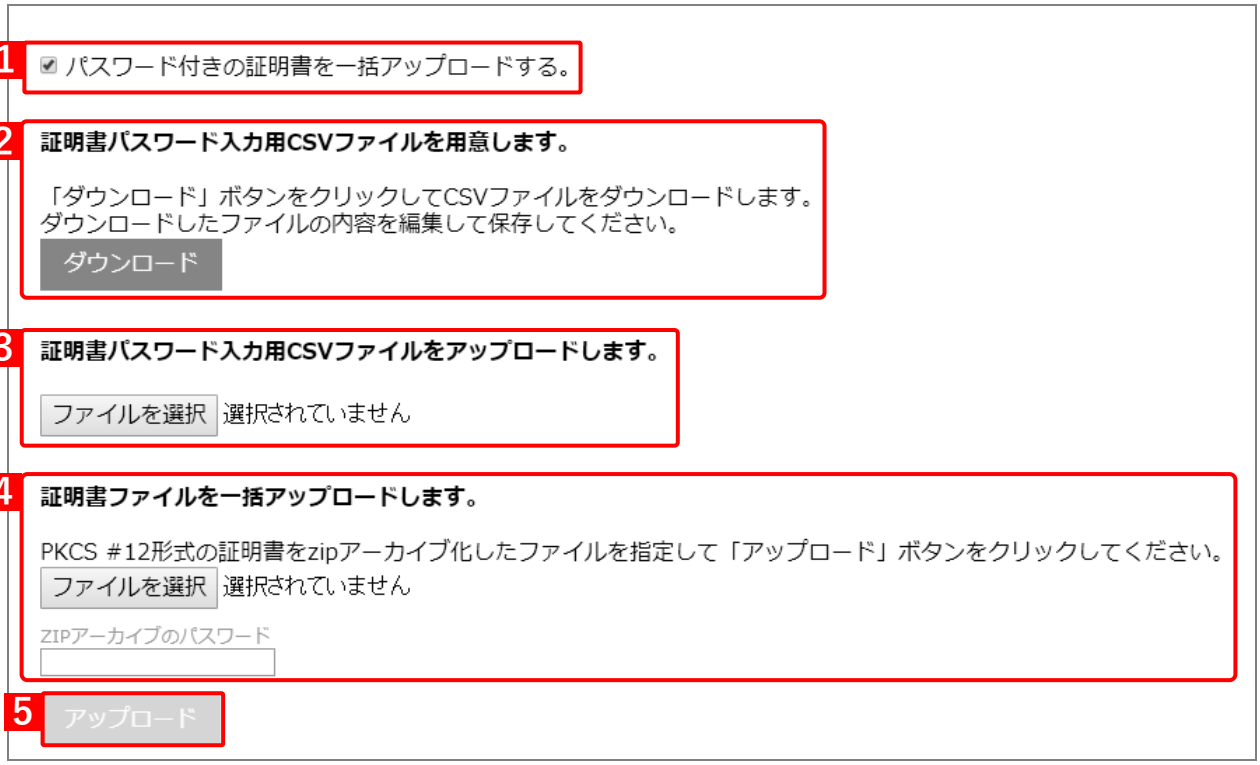
複数のクライアント証明書を ZIP ファイルにまとめて管理サイトにアップロードし、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

- 事前にクライアント証明書を取得してください。
- アップロードする複数のクライアント証明書は、まとめて zip ファイル形式で保存してください。
- アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。
  ☞「画面（編集）」351 ページ
- 管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。
  ☞「（設定－Android）クライアント証明書」79 ページ
  ☞「（設定－iOS）クライアント証明書」86 ページ
  ☞「（設定－iOS）Exchange（ActiveSync）設定」89 ページ
  ☞「（設定－iOS）VPN 設定」94 ページ
  ☞「（設定－Windows）クライアント証明書」106 ページ

◆画面

表示操作 ［設定］→［Android］→［証明書管理］→［クライアント証明書一括アップロード］→［パスワード付きの証明書を一括アップロードする］



項番	項目	説明
1	パスワード付きの証明書を一括アップロードする。	チェックを入れると、証明書パスワード入力用 CSV ファイルをアップロードできます。 パスワード付きのクライアント証明書でない場合は、チェックを入れません。

項番	項目	説明
2	証明書パスワード入力用 CSV ファイルを用意します。	証明書パスワード入力用 CSV ファイルをアップロードする場合、［ダウンロード］をクリックし、任意の場所に証明書パスワード入力用 CSV ファイルを保存します。保存したファイルを Excel やメモ帳で開き、クライアント証明書に設定されているパスワードを入力して保存します。 CSV ファイルの「[S]ファイル名」には、拡張子を除いたクライアント証明書のファイル名を入力してください。
3	証明書パスワード入力用 CSV ファイルをアップロードします。	［ファイルを選択］をクリックし、証明書パスワード入力用 CSV ファイルを選択します。
4	証明書ファイルを一括アップロードします。	［ファイルを選択］をクリックし、アップロードする ZIP ファイルを選択します。パスワードで保護された ZIP ファイルを選択した場合は、「ZIP アーカイブのパスワード」に設定されているパスワードを 255 文字以内の半角英数字で入力します。 一括でアップロードする PKCS #12 形式のクライアント証明書のファイルは、あらかじめ ZIP ファイルにまとめておく必要があります。 ファイル名は 30 文字以内で設定してください。
5	［アップロード］	クリックすると、ZIP ファイルに含まれるクライアント証明書の一覧が表示されます。表示内容に問題がないことを確認し、［アップロードを実行］をクリックします。 アップロード済みの同名のクライアント証明書を上書きする場合は「同じファイル名の証明書がすでに存在した場合は上書き保存する」にチェックを入れます。

7.7.3 クライアント証明書一括削除

管理サイトにアップロードされているクライアント証明書を、CSV ファイルを利用して一括で削除します。

操作手順については、以下を参照してください。

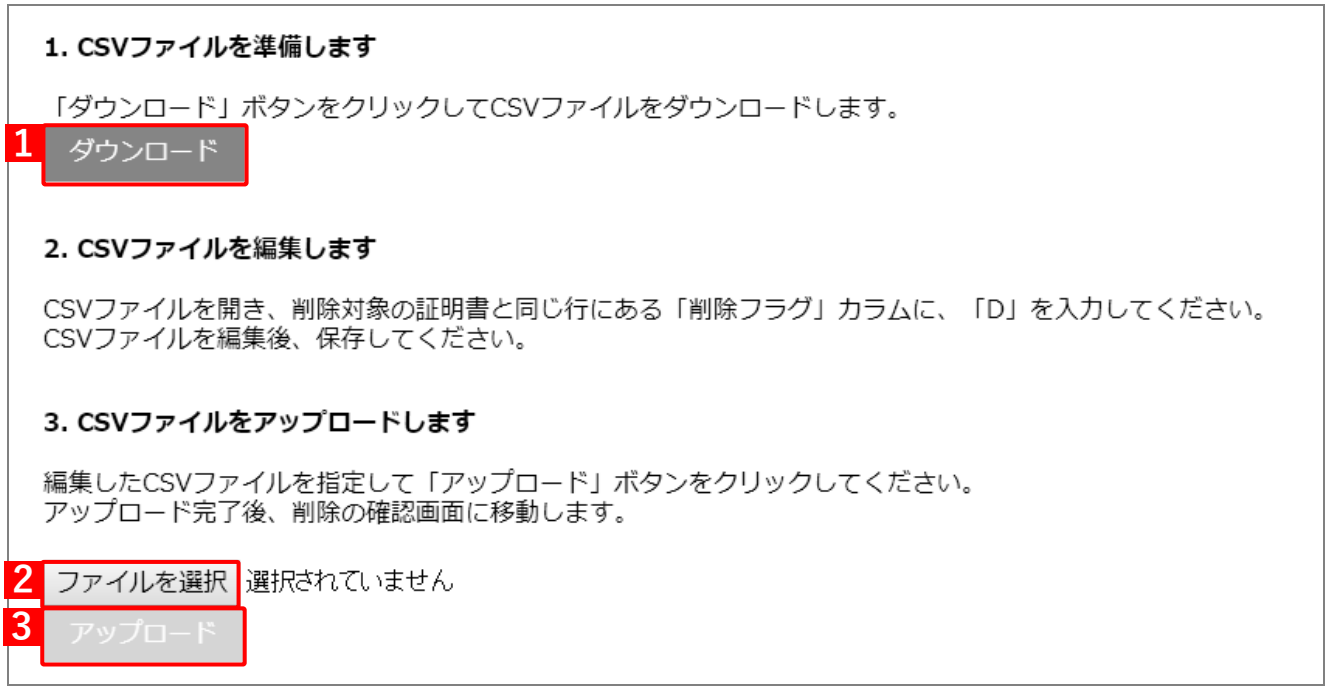
『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

端末に紐づけられているクライアント証明書を削除した場合は、端末に割り当てられている設定が動作しなくなることがあります。

削除対象のクライアント証明書は、管理サイトおよび iOS 端末からも削除されます。

◆画面

表示操作　［設定］→［Android］→［証明書管理］→［クライアント証明書一括削除］



項番	項目	説明
1	［ダウンロード］	任意の場所にクライアント証明書を削除するための CSV ファイルを保存します。保存した CSV ファイルを Excel やメモ帳で開き、削除したいクライアント証明書名の右側にある「[S]削除フラグ」列に「D」と入力して保存します。
2	［ファイルを選択］	項番 1 で保存した CSV ファイルを選択します。
3	［アップロード］	CSV ファイルのアップロードが開始されます。アップロードが完了すると、インポート画面が表示されます。

7.7.4 CA 証明書管理

Android 端末にインストールする CA 証明書をアップロードし、端末に適用する設定セットを作成します。

本機能でアップロードした CA 証明書は、Android、Windows で共有することができます。

画面（新規作成）

画面（CA 証明書の情報）

CA 証明書をサイレントインストールすると、Android 端末の仕様により通知バー上に AndroidSystem からの通知が表示される場合があります。詳細については、以下を参照してください。

『Android クライアント リファレンスマニュアル』の「管理サイトからの指示による動作」－「CA 証明書がサイレントインストールされた場合」

iOS 端末の CA 証明書は、本メニューを利用できません。構成プロファイルとして配信してください。

「［その他▼］タブ／証明書設定」425 ページ

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

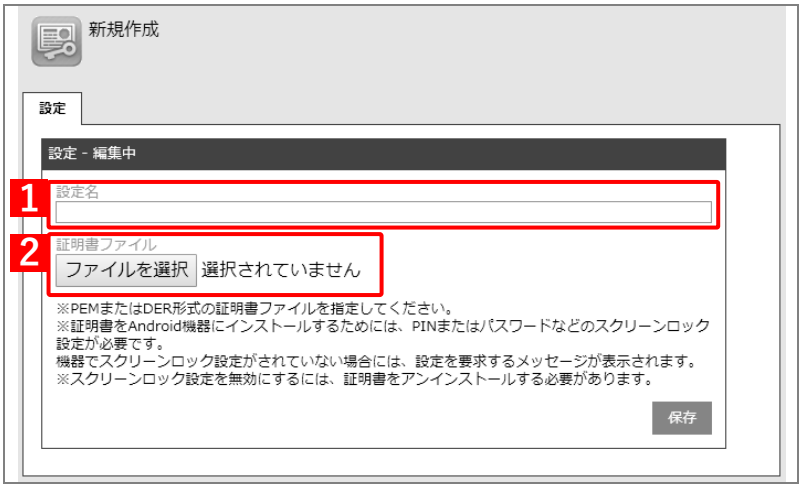
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成）

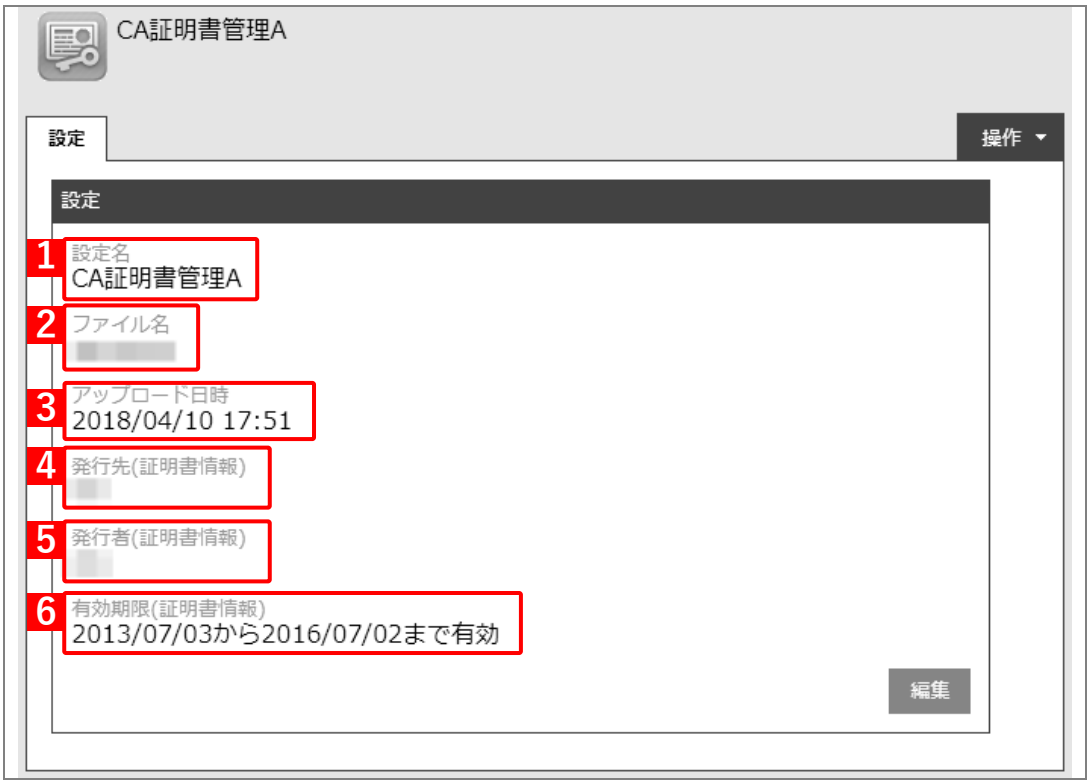
表示操作　［設定］→［Android］→［証明書管理］→［CA 証明書管理］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	証明書ファイル	［ファイルを選択］をクリックし、アップロードする CA 証明書を選択します。 PEM または DER 形式の CA 証明書ファイルを指定してください。 CA 証明書を Android 端末にインストールするには、PIN またはパスワードなどのスクリーンロック設定が必要です。

◆画面（CA 証明書の情報）

表示操作　［設定］→［Android］→［証明書管理］→［CA 証明書管理］→一覧から対象を選択



項番	項目	説明
1	設定名	設定した CA 証明書の名称が表示されます。
2	ファイル名	CA 証明書のファイル名が表示されます。
3	アップロード日時	CA 証明書ファイルのアップロード日時が表示されます。
4	発行先(証明書情報)	CA 証明書の発行先が表示されます。
5	発行者(証明書情報)	CA 証明書の発行者が表示されます。
6	有効期限(証明書情報)	CA 証明書の有効期限が表示されます。

7.8 Zone Management

特定のネットワーク・位置・時間帯を設定したゾーン設定と、Android 端末と Windows 端末に適用する各機能の設定セットを選択したポリシー設定を組み合わせ、ゾーンポリシー構成の設定セットを作成します。

学校や職場など、特定の条件下で使用する端末を設定する場合に有効な機能です。

本機能を Android 端末に割り当てると、エージェントのメニュー画面に「現在のゾーン」が表示されます。

『Android クライアント リファレンスマニュアル』の「エージェントの基本操作」ー「メニュー画面の表示内容」

7.8.1 ゾーン

接続先のネットワーク・位置情報・時間帯を組み合わせ、ゾーン設定として保存します。

保存したゾーン設定をポリシー設定と組み合わせ、ゾーンポリシー構成の設定セットを作成します。

「ポリシー」360 ページ

「ゾーンポリシー構成」362 ページ

この設定は、Android と Windows で共有することができます。

単一のゾーンに複数の SSID を設定した場合は、いずれかの SSID が検知された場合に「ゾーン内」となります。また複数の位置情報とスケジュール設定も、いずれかの設定が満たされた場合に「ゾーン内」となります。SSID と位置情報、SSID とスケジュールなど異なる設定を複数組み合わせる場合は、すべての設定を満たした場合に「ゾーン内」となります。

【複数の条件を組み合わせた場合】

- 場所：SSID1、SSID2、SSID3
- 時間：月曜 17:00～18:00、土曜 16:00～17:30

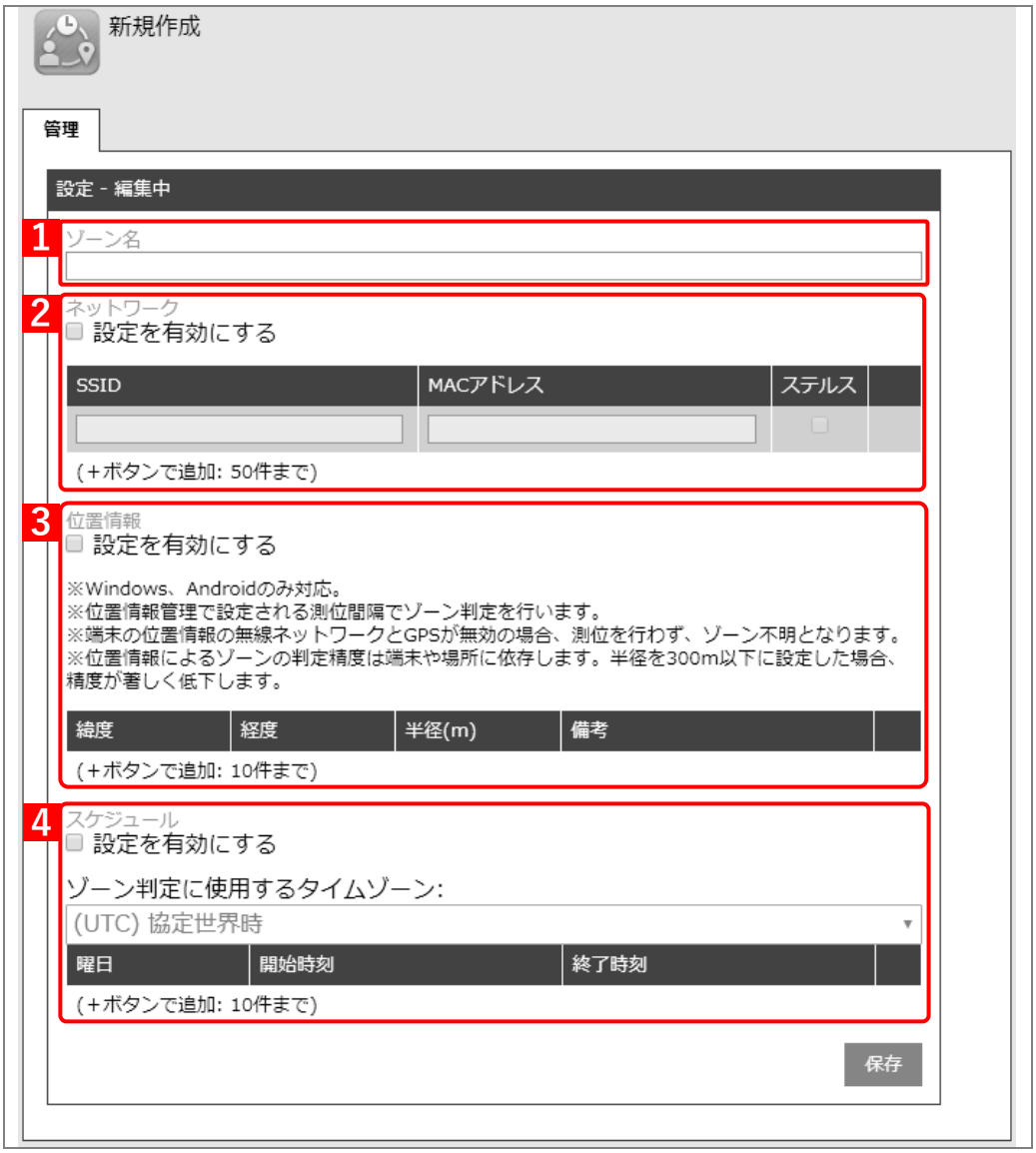
上記のゾーン設定では SSID が「SSID1」「SSID2」「SSID3」のいずれかに一致し、さらに日時が「月曜 17:00～18:00」「土曜 16:00～17:30」のいずれかに一致した場合に「ゾーン内」となります。

Android 8.0 以上の場合は、Wi-Fi の SSID 情報および位置情報の取得が 1 時間に 1 回程度へ制限されます。ゾーンの切り替えを即時検知できず、約 1 時間程度のタイムラグが発生します。

ゾーン設定は、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［Zone Management］→［ゾーン］→ ＋



項番	項目	説明
1	ゾーン名	ゾーンの名称を 1 文字から 30 文字で入力します。 先頭が「S」で始まる名称は設定できません。
2	ネットワーク	ゾーンに設定するネットワークの SSID、MAC アドレスの設定を行います。ネットワークは、50 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で、以降で設定するネットワークが有効になります。＋ をクリックし、必要なネットワークを追加します。 ●SSID ネットワークの SSID を 32 文字以内の半角英数字、「-」、「_」、「@」で入力します。 ●MAC アドレス アクセスポイントの MAC アドレスを入力します。「XX:XX:XX:XX:XX:XX」（X は大文字の 16 進数）という形式で入力してください。 ●ステルス SSID ステルスを有効としたネットワークの場合は、チェックを入れます。 SSID と MAC アドレスは重複しないものを入力してください。

項番	項目	説明
3	位置情報	ゾーンに設定する位置の緯度と経度、エリアの範囲を指定します。位置情報は 10 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で、以降で設定する位置情報が有効になります。 をクリックし、必要な位置情報を追加します。 ●緯度 -90 から 90 の範囲の値を入力します。 ●経度 -180 から 180 の範囲の値を入力します。 ●半径（m） 1 から 20037500 の範囲の値を入力します。 ●備考 備考が必要な場合は、30 文字以内で入力します。 端末の位置情報の無線ネットワークと GPS が無効な場合、または管理サイトの時刻と端末時刻の間に大幅な差がある場合は、測位を行わず「ゾーン不明」となります。「ゾーン不明」と判定された端末に特定のポリシーを適用できます。 ☞「ゾーンポリシー構成」362 ページ Android 端末の位置情報取得が「許可しない」の場合、位置情報を取得しません。 位置情報の測位間隔の詳細については、以下を参照してください。 ☞「位置情報管理」309 ページ Android 12 以上は、正確な位置情報を取得するために、端末の設定で「正確な位置情報を使用」を有効にしてください。
4	スケジュール	ゾーンに設定するスケジュールを登録します。スケジュールは 10 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で以降で設定するスケジュールが有効になります。 をクリックし、必要なスケジュールを追加します。 ●ゾーン判定に使用するタイムゾーン タイムゾーンをリストボックスから選択します。 ●曜日 スケジュール設定を有効にする曜日にチェックを入れます。 ●開始時刻 開始時刻をリストボックスから選択して指定します。00:00 から 23:59 の間で指定します。 ●終了時刻 終了時刻をリストボックスから選択して指定します。00:00 から 35:59 の間で指定します。 土曜日に日またがりで Zone Management を設定する場合は、xx:xx から 24:00 までの設定と、日曜日 0:00 から 35:59 までの設定の 2 つを実施すると、日またがり後の制御ができます。

7.8.2 ポリシー

Android 端末と Windows 端末に適用する各機能の設定セットを選択し、ポリシー設定として保存します。

保存したポリシー設定をゾーン設定と組み合わせ、ゾーンポリシー構成の設定セットを作成します。

「ゾーン」357 ページ

「ゾーンポリシー構成」362 ページ

この設定は、Android と Windows で共有することができます。

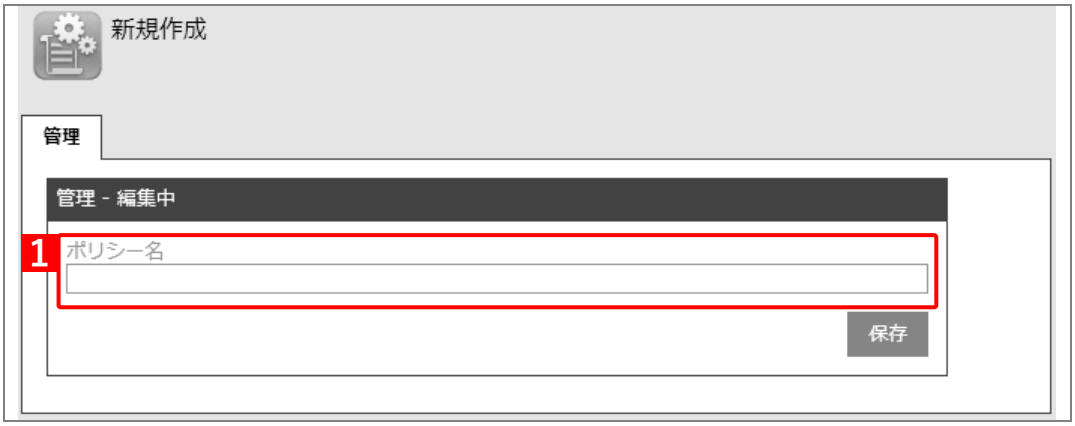
［Android 設定］タブで設定する「リモートロック」は、Android 端末のみ対応しています。

ポリシー設定は、最大 50 件まで作成できます。

7.8.2.1 ［管理］タブ

◆画面（新規作成）

表示操作　［設定］→［Android］→［Zone Management］→［ポリシー］→ ✚



項番	項目	説明
1	ポリシー名	設定の名称を 1 文字から 30 文字で入力します。

7.8.2.2 ［Android 設定］タブ

◆画面

表示操作 ［設定］→［Android］→［Zone Management］→［ポリシー］→一覧から対象を選択→［Android 設定］タブ→［編集］

項番	項目	説明
1	設定	ポリシーにおける Android の設定セットの使用設定を行います。各機能に設定する内容を以下から選択します。 ●各機能の設定名 選択した設定セットを適用します。 ●(機器の設定に従う) ゾーンポリシー以外で設定されている設定が継承されます。 ●(所属組織に従う) 所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(設定なし) 設定を変更しません。

7.8.3 ゾーンポリシー構成

ゾーン設定とポリシー設定を組み合わせて、ゾーンポリシー構成の設定セットを作成します。ゾーンポリシー構成を端末に適用すると、さまざまな場所や時間、ネットワークでの端末の動作を管理できます。

この設定は、Android と Windows で共有することができます。

事前にゾーンとポリシーを作成してください。

「ゾーン」357 ページ
「ポリシー」360 ページ

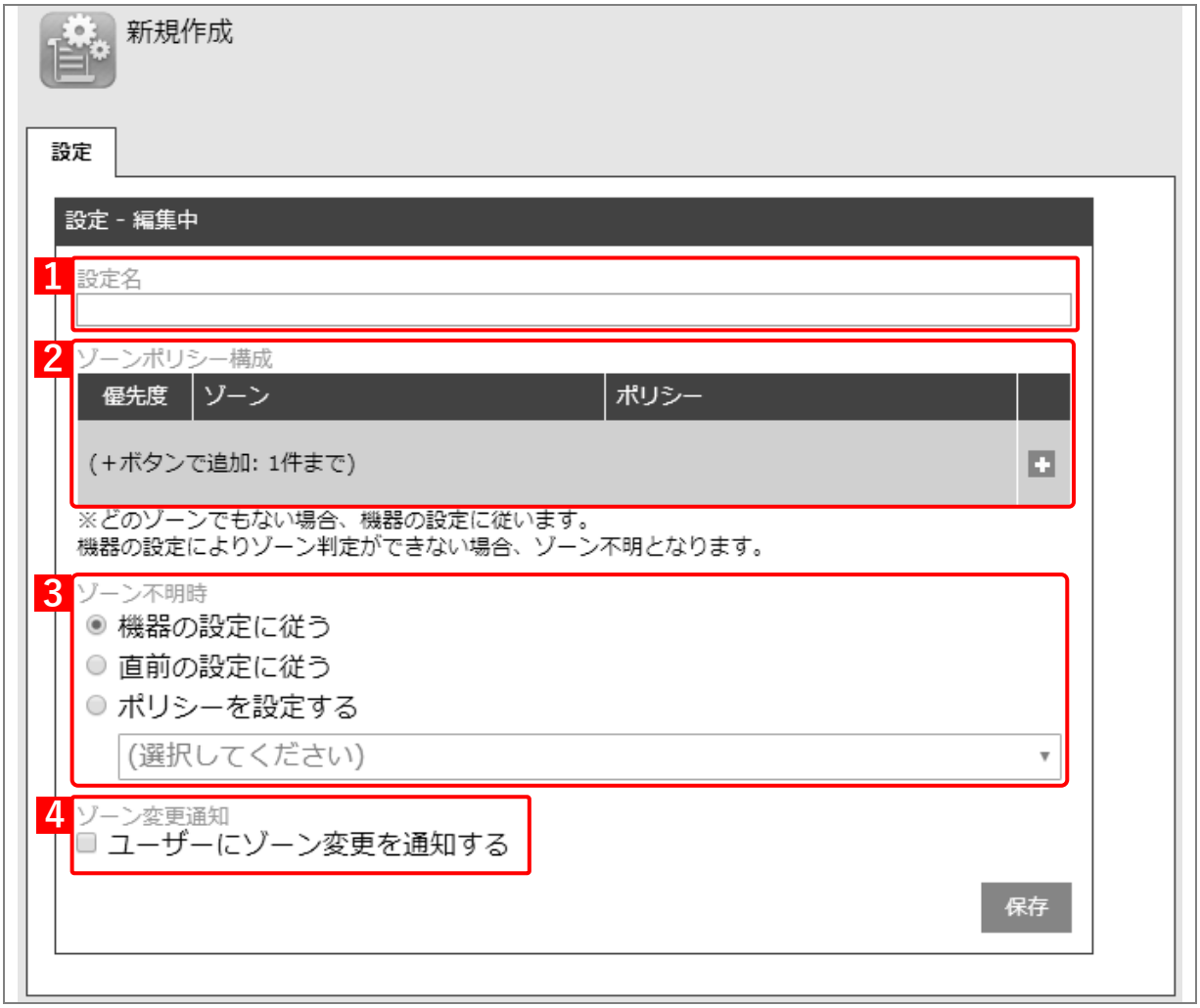
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「(設定－Android) 設定の割り当て」75 ページ
「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［Zone Management］→［ゾーンポリシー構成］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	ゾーンポリシー構成	ゾーンに設定するゾーン優先度、ゾーン、ゾーンポリシーを登録します。 ●ゾーン優先度 ゾーン優先度を入力します。 ●ゾーン ゾーンを選択します。 ☞「ゾーン」357 ページ ●ポリシー ゾーンのポリシーを選択します。 ☞「ポリシー」360 ページ
3	ゾーン不明時	ゾーン不明と判定された場合に適用される設定を以下から選択します。 ●機器の設定に従う ●直前の設定に従う ●ポリシーを設定する この設定を選択した場合は、適用するポリシーをリストボックスから選択します。 ゾーンで設定した項目ごとに以下の条件が当てはまる場合は、端末は「ゾーン判定不可」を検知して、管理サイトに「ゾーン不明」のステータスを送信します。 ・スケジュール 同期時にサーバーと端末の時刻が著しく異なる。 ・ネットワーク 機器設定により Wi-Fi が OFF に設定されている。 ・位置情報 「位置情報 OFF」に設定されている、または位置情報設定が「バッテリー節約」かつ「ネットワーク接続無し」に設定されている。 ゾーンの設定については、以下を参照してください。 ☞「ゾーン」357 ページ
4	ゾーン変更通知	端末のゾーンが変更されたときに、端末上に通知を表示します。 Android 端末では、通知領域、Windows 端末ではステータスバー上のバルーンに通知が表示されます。 スケジュールと位置情報によるゾーン設定によっては、大量の通知が発生する可能性があります。過度な情報通知により、ユーザーの利便性を下げてしまう可能性があるので慎重に設定してください。

7.9 Device Owner Mode

Device Owner Mode 化されたエージェントに各種の設定や操作を行うための設定セットを作成します。

Device Owner Mode は、デバイス管理アプリに Device Owner Mode という特別な権限を持たせることで、より高度な設定を行える状態のことを指します。

本章の機能は、Device Owner Mode 化されたエージェントをインストールしている、以下の端末で利用することができます。

- Optimal Biz 9.5 以上でキッティングを行った端末（従来版エージェントをインストールした端末は除く）
- Optimal Biz 9.4 以下でキッティングを行い、すでに Device Owner Mode 化されている端末

端末の導入の詳細については、以下を参照してください。

『Android キッティングマニュアル』

Android 6.0 以上の端末が対象です。対応機種については、以下を参照してください。

『Android エージェント対応端末表』

7.9.1 セキュリティ設定（DOM）

Device Owner Mode化されたエージェントに、各種項目の許可／禁止、制限を行うための設定セットを作成します。

各種項目の制限に関する制約事項は、以下を参照してください。

『Android エージェント対応端末表』

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Android］→［Device Owner Mode］→［セキュリティ設定］→ ✚

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	Android Enterprise	
	提供元不明アプリのインストール	公式の Google Play ストアなどで提供していない「提供元不明アプリ」のインストールを「許可」または「禁止」に設定します。 Google のポリシーに従い、デフォルトで「禁止」が設定されています。
	開発者向けオプション	専門的な機能などが設定できる「開発者モード」への切り替えを「許可」または「禁止」に設定します。 Google のポリシーに従い、デフォルトで「禁止」が設定されています。

項番	項目	説明
	アプリ確認の強制	端末にインストールされているアプリの検証を「強制する」または「強制しない」に設定します。 Google のポリシーに従い、デフォルトで「強制する」が設定されています。
3	無線とネットワーク	
	Wi-Fi 設定の変更	Wi-Fi（無線 LAN）の設定の変更を「許可」または「禁止」に設定します。 「禁止」を設定すると、端末で Wi-Fi の設定が変更できないため、ネットワークに接続できなくなることがあります。その場合は、SIM を挿入して、モバイルネットワークで接続してください。
	Bluetooth	Bluetooth（近距離無線通信）の使用を「許可」または「禁止」に設定します。 Android 8.0 以上の端末で、設定できます。 「禁止」を設定すると、端末で Bluetooth の機能が使用できなくなります。
	機内モード	通信機能をオフにする「機内モード」への切り替えを「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	プライベート DNS 設定の変更	モバイルネットワークで、任意の DNS（ホスト名やドメイン名などと IP アドレスの紐づけ）設定の変更を「許可」または「禁止」に設定します。 Android 10 以上の端末で、設定できます。
	データ出力 NFC 利用	端末をかざすだけで通信ができる Android Beam を使用して、データの出力を「許可」または「禁止」に設定します。 Android 10 以上の端末は、Android Beam に対応していないため、本設定は無効になります。
	テザリング設定の変更	他の機器などにインターネット接続を共有できるテザリング設定の変更を「許可」または「禁止」に設定します。 「禁止」を設定すると、テザリング設定を禁止できます。端末のテザリング設定がオンになっていた場合でも、自動的にオフになります。 Bluetooth テザリング設定をオンの状態で、本機能で「禁止」したあとで解除しても、端末によっては「禁止」になる場合がありますので、注意してください。
	VPN 設定の変更	VPN（仮想専用通信網）設定の変更を「許可」または「禁止」に設定します。
	モバイルネットワーク設定の変更	モバイルネットワーク（通信事業者と契約するデータ通信）設定の変更を「許可」または「禁止」に設定します。
	緊急警報設定の変更	災害などの緊急時に受信する緊急警報設定の変更を「許可」または「禁止」に設定します。
	ローミング	データローミングの使用を「許可」または「禁止」に設定します。 Android 7.0 以上の端末で、設定できます。
4	端末	
	明るさの設定の変更	画面の明るさの変更を「許可」または「禁止」に設定します。 Android 9.0 以上の端末で、設定できます。
	壁紙の変更	壁紙（ホーム画面やロック画面の背景）の変更を「許可」または「禁止」に設定します。 Android 7.0 以上の端末で、設定できます。

項番	項目	説明
	画面消灯設定の変更	画面を消灯するときの設定の変更を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	アンビエント表示	スリープ画面に時計などの表示を行うアンビエント表示を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	音量設定の変更	音量の設定の変更を「許可」または「禁止」に設定します。
	アプリの制御	インストール済みのアプリの制御を「許可」または「禁止」に設定します。 「禁止」を設定すると、端末の［設定］→［アプリ情報］で以下の項目が制御されます。端末により、項目名や階層が異なります。 ・無効 ・アンインストール ・強制終了 ・ストレージを消去 ・キャッシュを削除 ・デフォルトで開く
	物理外部メディアへのマウント	端末への物理外部メディア（SD カードや USB メモリなど）のマウントを制限します。 「禁止」にすると、端末上でマウント操作が行えなくなりますが、すでにマウントされている場合は、アンマウントされるまではマウントされたままになります。（手動でアンマウント操作、端末再起動など） 制限されるのは端末のマウント機能が対象になります。
	ユーザーアイコンの変更	マルチユーザー機能でユーザーが使用しているアイコンの変更を「許可」または「禁止」に設定します。 Android 7.0 以上の端末で、設定できます。 Device Owner Mode が有効の場合、マルチユーザー機能は無効になるため、所有者ユーザーのアイコンが対象になります。
5	ユーザー設定	
	位置情報設定の変更	位置情報設定の変更を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	認証情報設定の変更	証明書などの「認証情報」に関する設定の変更を「許可」または「禁止」に設定します。 設定にかかわらず、証明書管理で証明書を配信することはできます。詳細については、以下を参照してください。 「証明書管理」348 ページ
	アカウントの追加と削除	Google アカウントや Exchange などのアカウントの追加および削除を「許可」または「禁止」に設定します。 利用するアプリの動作に必要なアカウント情報を端末に登録してから、「禁止」に設定してください。
	言語設定の変更	言語設定の変更を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	Google のバックアップサービスの利用	端末で管理しているコンテンツや設定など、Google アカウントにバックアップするかを「許可」または「禁止」に設定します。 初期値は OS 仕様のため、「禁止」が選択されています。 Android 8.0 以上の端末で、設定できます。

項番	項目	説明
	ネットワーク設定のリセット	ネットワーク設定のリセットを「許可」または「禁止」に設定します。
	ファクトリーリセット	端末の初期化を「許可」または「禁止」に設定します。 本設定を「禁止」にしていても、以下の機能で初期化することができます。 ・リモートワイプ 「（操作－Android）リモートワイプ」114 ページ ・画面ロック 「ロック解除失敗時の設定」－「○回失敗でワイプ」 「画面ロック」304 ページ ・ハードウェアリセット
6	システム	
	日付、時刻、タイムゾーンの設定の変更	日付、時刻、タイムゾーンの設定の変更を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	印刷	端末からの印刷を「許可」または「禁止」に設定します。 Android 9 以上の端末で、設定できます。
	イースターエッグ	Android の隠し機能である「イースターエッグ」の表示を「許可」または「禁止」に設定します。
7	その他	
	ステータスバーの操作と通知表示	ステータスバーの利用を「許可」または「禁止」に設定します。 「禁止」にすると、ステータスバーで Wi-Fi や Bluetooth などの設定変更や通知領域の操作を防げます。 Android 7.0 以上の場合は、「禁止」に設定しても端末によっては、スクリーンロック画面に通知が表示されたときに通知領域の操作ができます。この現象は端末の仕様に依存するため、あらかじめご了承ください。 「禁止」に設定すると、通知領域の通知も表示されなくなります。これにより、通知受信時の着信音やバイブレーションも動作しません。
	USB ファイル転送	端末を PC に接続したときに、「MTP」モードおよび「PTP」モードの利用を制限します。 「禁止」に設定すると、USB を接続したときの通知などに表示される接続種別から、「MTP」モードおよび「PTP」モードが表示されません。 Android 7.1 以上の端末では、「禁止」に設定すると、USB フラッシュメモリのマウントも禁止されます。
	スクリーンショットの撮影	スクリーンショット（スマートフォンの画面の画像）の撮影を「許可」または「禁止」に設定します。
	セーフモードの起動	不具合などが発生したときに、解析や復旧などで利用する「セーフモード」での起動を「許可」または「禁止」に設定します。

7.9.2 アプリケーション非表示

Device Owner Mode 化されたエージェントに設定されたアプリが、Android 端末で非表示となる設定セットを作成します。

画面（新規作成）

画面（編集）

本機能は、バージョンが 9.5.111.0 以上の Android エージェントで利用できます。

本設定セットを割り当てると、すでに Android 端末へ対象のアプリがインストールされていても、非表示（アンインストールされるわけではない）になります。

設定するアプリにより OS の動作に支障をきたす（エージェント停止、OS 強制再起動を繰り返す、Android Recovery 画面になるなど）場合があります。システムアプリをアプリケーション非表示にするときは、慎重に設定してください。システムアプリを禁止した場合、どのような挙動になるかについては、ご利用の端末や OS に依存するため、弊社ではご案内はできかねます。

Android Enterprise のアプリケーション配信で、管理者が強制（サイレント）インストールに設定したアプリを非表示アプリとして設定すると、インストールが繰り返し発生しインストールするたびに通信料がかかります。ご了承ください。
Android Enterprise のアプリケーション配信および強制（サイレント）インストールの詳細については、以下を参照してください。

「Android Enterprise」327 ページ

『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」－「アプリを強制インストールする」、「オリジナルアプリをインストールする」、「ウェブアプリ（ショートカット）をインストールする」、「アプリ構成を利用してアプリをインストールする」－「アプリケーション配信設定を作成する」

Optimal Biz 9.8 以上では、本機能で Google Chrome を制限することはできません。Google Chrome を制限する場合は、アプリケーション禁止をご利用ください。

「アプリケーション禁止」320 ページ

Optimal Biz 9.7 以下で Google Chrome を設定していた場合は、引き続き使用できますが、編集を行うと使用できなくなります。OS の動作に支障をきたすため、新規の端末に本機能を割り当てないでください。

本機能を設定した場合、端末の挙動は以下のとおりです。

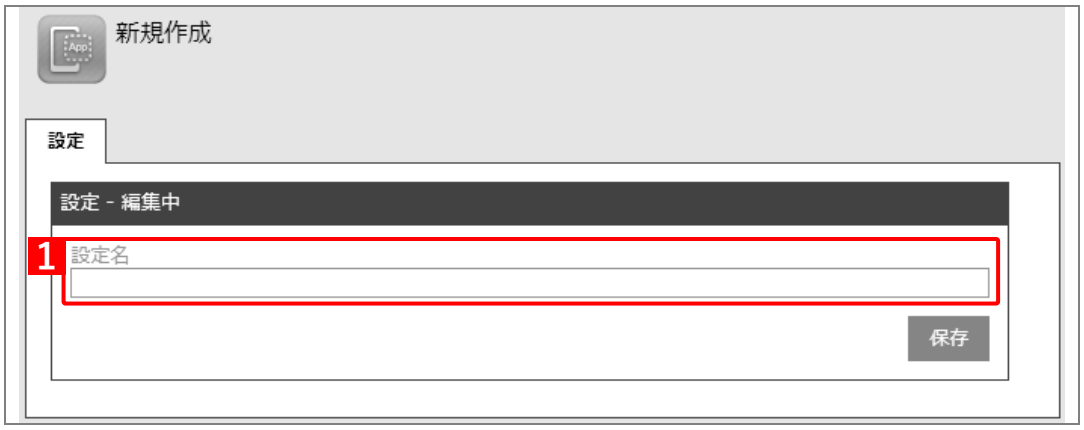
- ホームとアプリ一覧での表示：表示されない
  端末の［設定］→［アプリ］では、アプリ一覧が表示されます。
- アプリ画面の表示：停止
- バックグラウンドの挙動：停止
  アプリケーション禁止を設定した場合は、以下を参照してください。

「アプリケーション禁止」320 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成）

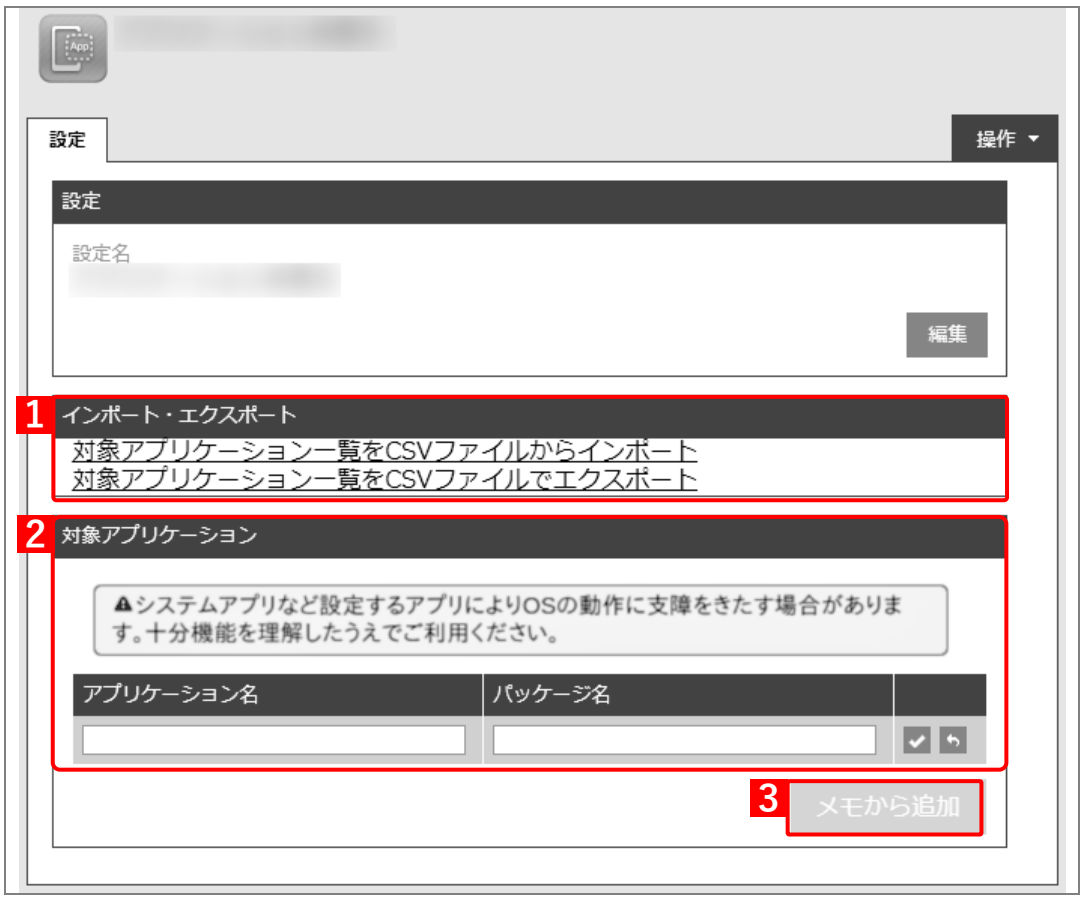
表示操作［設定］→［Android］→［Device Owner Mode］→［アプリケーション非表示］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。

◆画面（編集）

表示操作［設定］→［Android］→［Device Owner Mode］→［アプリケーション非表示］→一覧から対象を選択



項番	項目	説明
1	インポート・エクスポート	CSV ファイルから非表示対象のアプリの登録をまとめて行います。また、現在対象になっているアプリの一覧を CSV ファイルに保存できます。 操作手順については、以下を参照してください。 『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」 このメニューは、設定セットを作成したあとに表示されます。 ●対象アプリケーション一覧を CSV ファイルからインポート クリックすると、CSV ファイルの準備とアップロードをする画面が表示されます。 ●対象アプリケーション一覧を CSV ファイルでエクスポート クリックすると現在の対象アプリケーションの一覧を update_values.csv に保存します。ファイルの保存はメッセージにしたがって操作してください。
2	対象アプリケーション	アプリ名とパッケージ名を指定して、対象アプリを登録します。 （追加）、（削除）、（編集）、（保存）、（取り消し）を使って操作します。 この項目は、設定を作成したあとに表示されます。 ●アプリケーション名 アプリ名を入力します。機器が登録されている場合は、入力された文字を機器に登録されているすべてのアプリの中から関連するアプリを表示します。 ●パッケージ名 アプリのパッケージ名を入力します。 パッケージ名は機器のアプリ詳細画面で確認できます。 「（情報－Android）アプリケーション」141 ページ
3	［メモから追加］	クリックすると、機器の一覧のアプリ一覧の「メモ」に が表示されているアプリが「アプリ一覧」に表示されます。 機器の一覧のアプリ一覧の「メモ」欄の詳細については、以下を参照してください。 「（情報－Android）アプリケーション」141 ページ

7.9.3 OS アップデート（DOM）

Device Owner Mode 化されたエージェントの端末で、OS をアップデートする契機やアップデートを促すメッセージを表示するための設定セットを作成します。

端末のエージェントは、事前に Device Owner Mode 化してください。

端末がネットワークに接続されていないと OS をアップデートできません。また、以下の端末では、OS をアップデートできない場合があります。

- ディスク容量が不足している。
- バッテリー残量が少ない。

本設定で、OS のアップデートを停止することはできません。

端末のエージェントバージョンが古い場合は、［強制的にアップデート］、または［指定した時間内にアップデート］を選択しても、OS のアップデートが行われない場合があります。本設定を使用する前に端末のエージェントを最新の状態にしてください。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

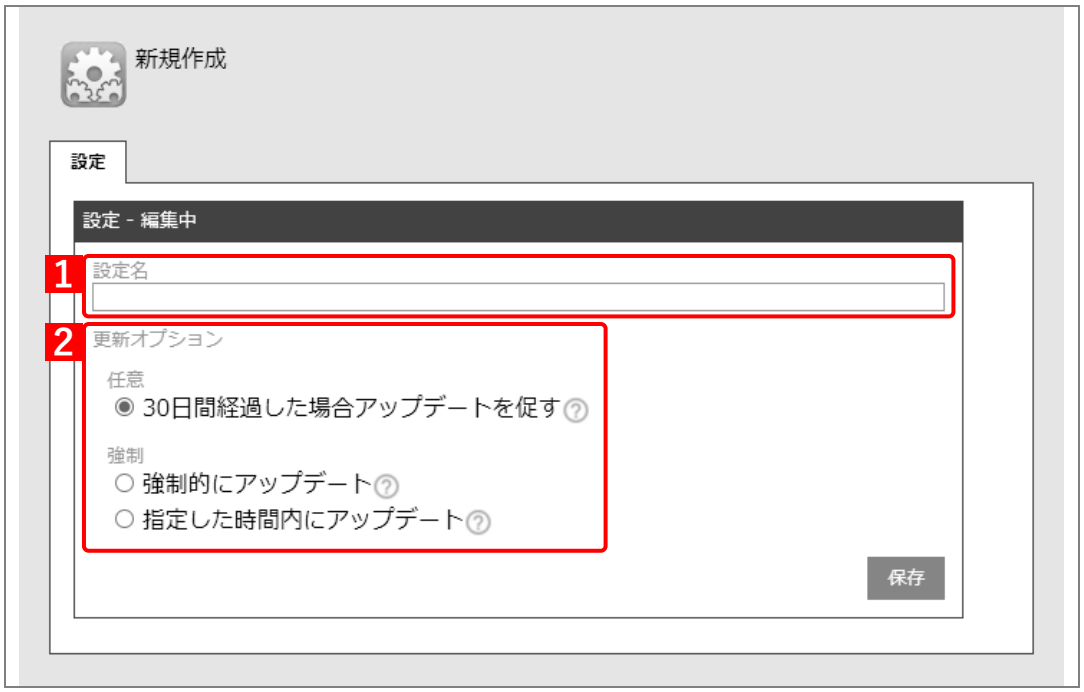
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Android］→［Device Owner Mode］→［OS アップデート］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	更新オプション	OS アップデートの契機を以下から選択します。 ●30 日間経過した場合アップデートを促す OS のアップデートが可能になってから 30 日後、端末にインストールを促すメッセージを表示します。メッセージに従い、OS をインストールします。 OS のインストールを拒否することができますが、翌日に再度メッセージが表示されます。 ●強制的にアップデート アップデートが可能になった OS を強制的にインストールします。 端末の操作中でもインストールが開始され、停止することはできません。 手動で OS をアップデートすることができません。 ●指定した時間内にアップデート 選択すると、開始時間と終了時間が入力できます。 指定した時間に、アップデートが可能になっている OS を強制的にインストールします。 指定した時間に端末の電源が入っていない場合は、インストールされません。 手動で OS をアップデートすることができません。

7.9.4 ファクトリーリセット保護（DOM）

ファクトリーリセット保護に関する設定セットを作成します。

ファクトリーリセット保護とは、Android 端末を初期化したとき、Google アカウントの認証が必要になることで、キッティングが完了できないようにする機能です。Android 端末の盗難防止になります。

画面（新規作成：［無効］を選択した場合）

画面（新規作成：［有効（端末に登録済みの Google アカウントを使用する）］を選択した場合）

画面（新規作成：［有効（Google アカウントを指定する）］を選択した場合）

Android 端末の設定、またはエージェントアプリの［端末初期化］から手動で初期化を実行した場合、本機能は使用できません。キッティング時に Google アカウントの認証が不要になります。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

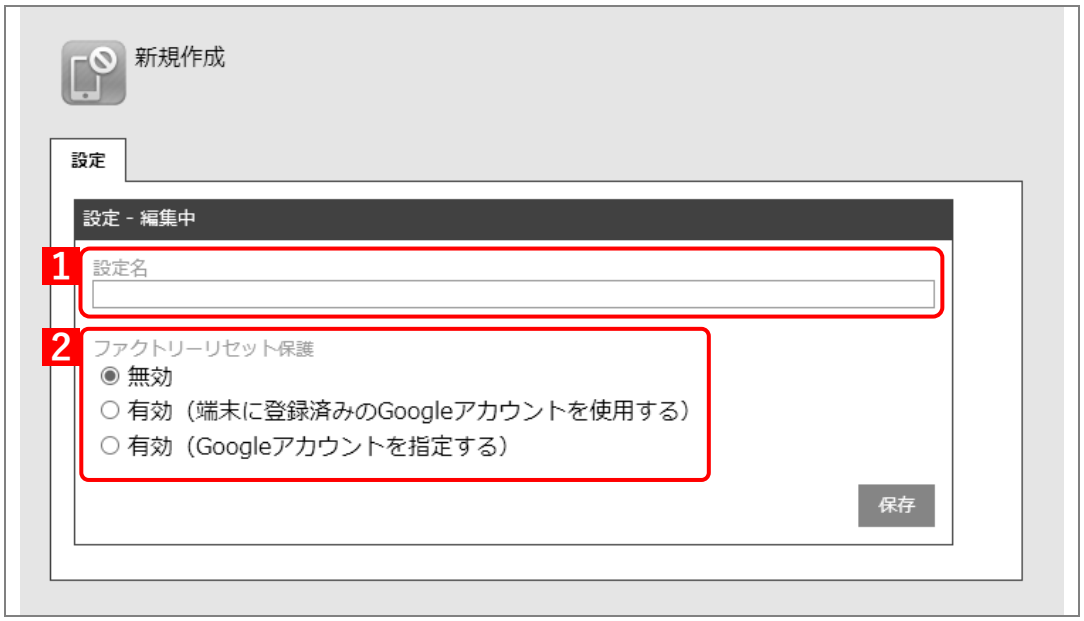
「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成：［無効］を選択した場合）

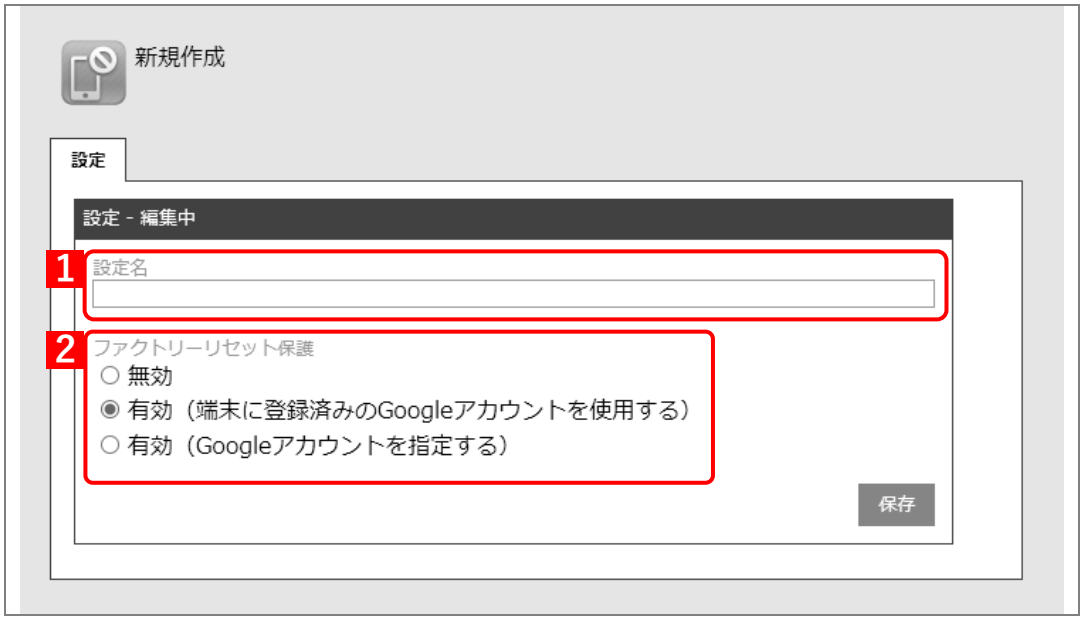
表示操作　［設定］→［Android］→［Device Owner Mode］→［ファクトリーリセット保護］→＋→［無効］



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	ファクトリーリセット保護	［無効］を選択した場合は、Android 端末を初期化したとき、Google アカウントを認証する必要がなく、キッティングが完了できます。

◆画面（新規作成：［有効（端末に登録済みの Google アカウントを使用する）］を選択した場合）

表示操作　**［設定］→［Android］→［Device Owner Mode］→［ファクトリーリセット保護］→ ✚ →［有効（端末に登録済みの Google アカウントを使用する）］**



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	ファクトリーリセット保護	［有効（端末に登録済みの Google アカウントを使用する）］を選択した場合は、Android 端末を初期化したとき、端末に登録済みの Google アカウントを認証することで、キッティングが完了できます。 新規に登録した Google アカウントは、72 時間本機能を使用できません。

◆画面（新規作成：［有効（Google アカウントを指定する）］を選択した場合）

表示操作　［設定］→［Android］→［Device Owner Mode］→［ファクトリーリセット保護］→ ＋ →［有効（Google アカウントを指定する）］

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	ファクトリーリセット保護	［有効（Google アカウントを指定する）］を選択した場合は、Android 端末を初期化したとき、指定した Google アカウントを認証しないと、キッティングが完了できません。 （A）＋をクリックすると、Google アカウントの選択画面またはログイン画面が表示されます。画面の指示に従い、Google アカウントを選択またはログインすると、「Google アカウントのメールアドレス」と「Google アカウント ID」が自動で表示されます。Google アカウントは、10 件まで登録できます。 Android 端末の設定アプリを使用して手動で初期化を実行した場合、本機能は使用できず、セットアップ時にスキップされます。 新規に登録した Google アカウントは、72 時間本機能を使用できません。

7.10 ゼロタッチ登録

ゼロタッチ登録に必要な、管理サイトとゼロタッチサーバー紐づけるための設定や、Google API 認証後の端末の一覧を表示します。

ゼロタッチ登録は、Android エージェントのキッティング手法の 1 つです。キッティング手順が省略化されるため、大規模な端末の導入を効率的に行うことができます。また、ゼロタッチ登録端末には、エージェントが自動的に Device Owner Mode としてインストールされるため、より安全な端末管理が可能です。

管理サイトでは、ゼロタッチサーバーとの連携設定を行います。

- モバイルネットワークが利用できるゼロタッチ登録に対応した端末を、事前に用意してください。Wi-Fi 専用端末は、本製品に対応していません。
- 端末の導入の詳細については、以下を参照してください。

  『Android キッティングマニュアル』
- ゼロタッチ登録の詳細については、以下を参照してください。

  https://www.android.com/intl/ja_jp/enterprise/management/zero-touch/

7.10.1 利用登録

管理サイトとゼロタッチサーバーを紐づけるために必要な情報を登録します。

画面

画面（登録後）

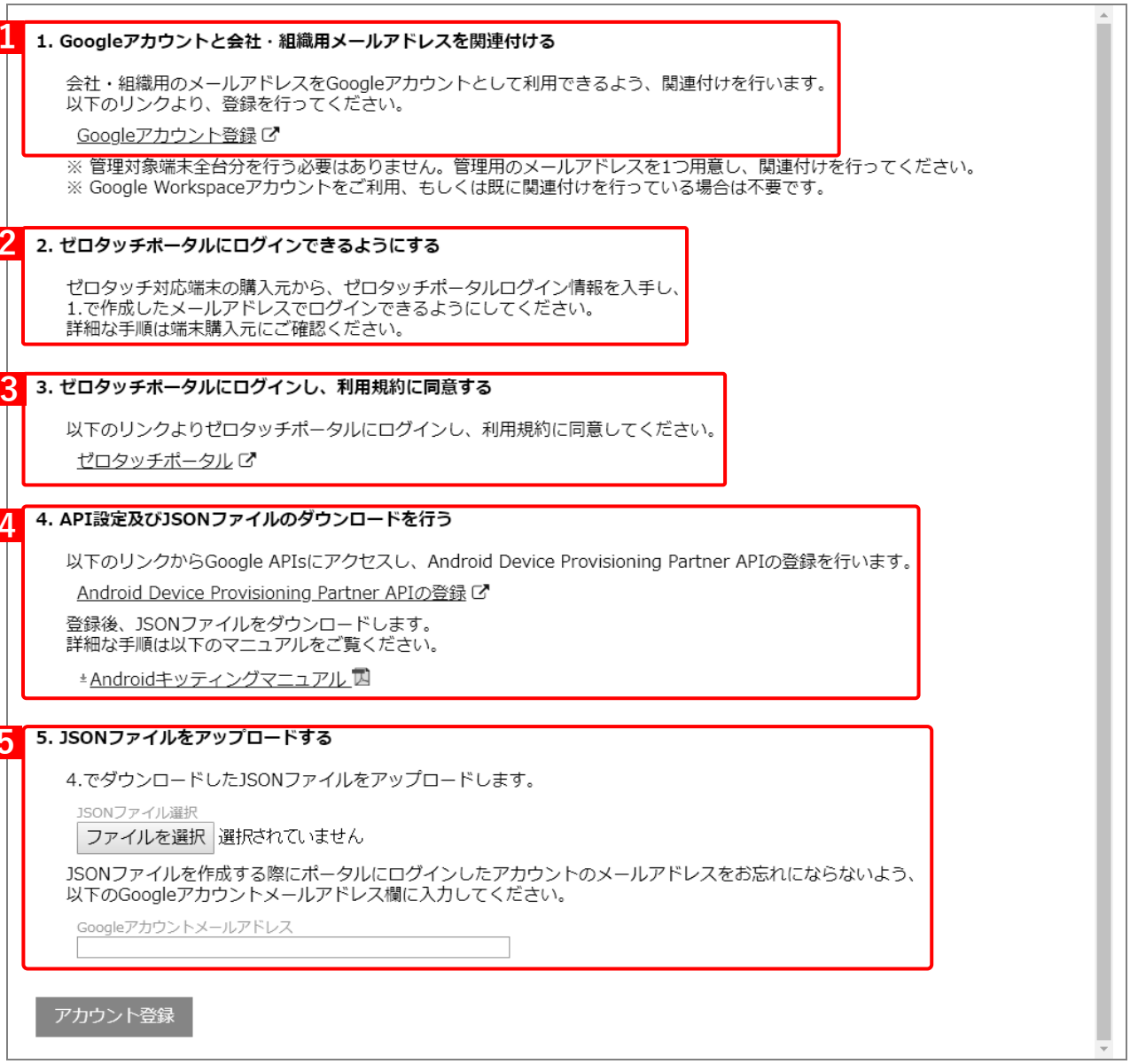
詳細については、以下を参照してください。

『Android キッティングマニュアル』の「Google アカウントでゼロタッチ登録を利用して Android Enterprise 連携を行う」

『Android キッティングマニュアル』の「Google Workspace アカウントでゼロタッチ登録を利用して Android Enterprise 連携を行う」

◆画面

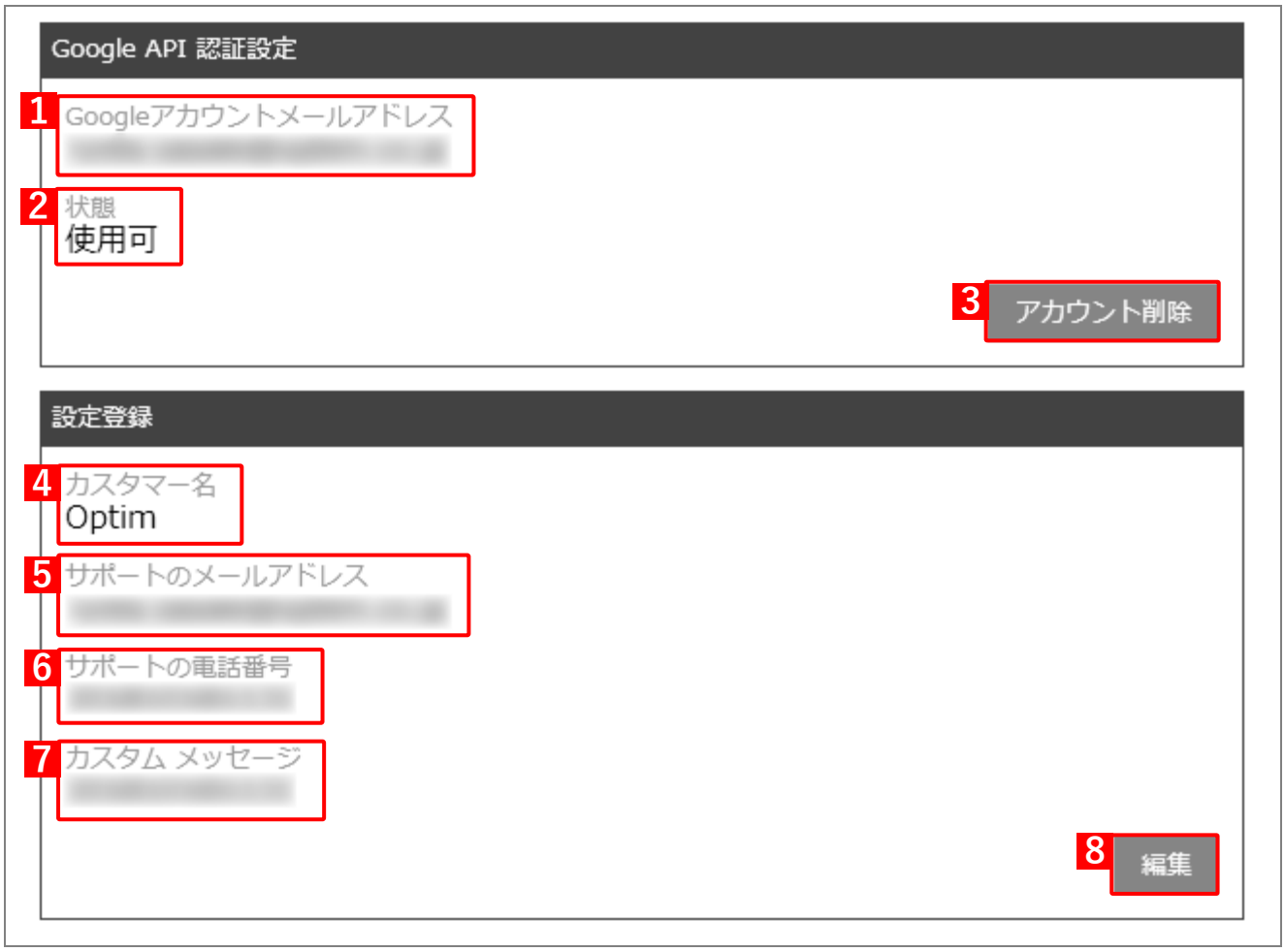
表示操作　［設定］→［Android］→［ゼロタッチ登録］→［利用登録］



項番	項目	説明
1	Google アカウントと会社・組織用メールアドレスを関連付ける	会社または組織用のメールアドレスを Google アカウントとして利用できるようにします。
2	ゼロタッチポータルにログインできるようにする	ゼロタッチ対応端末の購入元から、ゼロタッチポータルへログインするための情報を入手し、登録したメールアドレスでログインできるようにします。 詳細については、端末の購入元に問い合わせてください。
3	ゼロタッチポータルにログインし、利用規約に同意する	ゼロタッチポータルの利用規約に同意します。
4	API 設定及び JSON ファイルのダウンロードを行う	Android Device Provisioning Partner API の登録、および JSON ファイルのダウンロードを行います。
5	JSON ファイルをアップロードする	Google APIs でダウンロードした JSON ファイルを管理サイトにアップロードします。

◆画面（登録後）

表示操作　［設定］→［Android］→［ゼロタッチ登録］→［利用登録］



項番	項目	説明
1	Google アカウントメールアドレス	Google アカウントとして登録したメールアドレスが表示されます。
2	状態	ゼロタッチ端末の使用状態が表示されます。
3	［アカウント削除］	クリックすると、Google アカウントメールアドレスを削除します。
4	カスタマー名	ゼロタッチポータルで設定されているカスタマー名が表示されます。 カスタマー名は変更できません。
5	サポートのメールアドレス	ゼロタッチポータルで設定されているサポートのメールアドレスが表示されます。
6	サポートの電話番号	ゼロタッチポータルで設定されているサポートの電話番号が表示されます。
7	カスタムメッセージ	ゼロタッチポータルで設定されているカスタムメッセージが表示されます。
8	［編集］	クリックすると、サポートのメールアドレス、サポートの電話番号、カスタムメッセージを変更できます。

7.10.2 機器一覧

Google API 認証が完了したゼロタッチ端末を一覧表示します。

◆画面

表示操作　［設定］→［Android］→［ゼロタッチ登録］→［機器一覧］

項番	項目	説明
1	［ゼロタッチ登録サーバ同期］	ゼロタッチサーバーと同期します。これにより、ゼロタッチポータルに登録されている最新の端末情報が一覧表示されます。 Wi-Fi 専用端末は、本製品に対応していないため、同期ができない旨のメッセージが表示されます。必ずモバイルネットワークが利用できるゼロタッチ登録に対応した端末を、事前に用意してください。
2	ゼロタッチ端末一覧	ゼロタッチ端末の一覧が表示されます。 ゼロタッチ機器一覧で表示されたゼロタッチ端末は、機器画面の機器一覧で、認証待ち機器として表示されます。 ☞「機器一覧」54 ページ 本画面では端末を削除できません。端末は、機器画面の端末一覧で削除してください。 ☞「機器の個別削除」73 ページ (A)「IMEI/シリアル番号」をクリックすると、機器画面の機器一覧が表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠Google API 認証設定がありません。ゼロタッチ利用登録で設定する必要があります。	［設定］→［Android］→［ゼロタッチ登録］→［利用登録］にて設定がない状態で、［設定］→［Android］→［ゼロタッチ登録］→［機器一覧］に遷移している。	［設定］→［Android］>［ゼロタッチ登録］→［利用登録］で設定を作成してください。
⚠現在 Google API との連携が取れません。ゼロタッチ利用登録で状態を確認してください。	Google Cloud Platform 上で API エラーなど何らかの問題が発生している状態でゼロタッチの機器一覧を表示している。	［設定］→［Android］→［ゼロタッチ登録］→［利用登録］にて Google Cloud Platform のエラー内容から該当の設定を見直してください。
⚠他のユーザーによって同期処理を実行中です。しばらくお待ちください。	管理サイトに複数ユーザーでログインまたは同一ユーザーで複数タブを開き、複数画面で同時に［ゼロタッチ登録サーバ同期］をクリックしている。	複数画面で同時に［ゼロタッチ登録サーバ同期］をクリックしないでください。

8 設定－iOS

この章では、サブヘッダーメニューの［iOS］画面に表示される、各種の設定について説明します。

注意

●事前に Apple Push 証明書を登録してください。

『Apple Push 証明書年次更新マニュアル』

8.1 管理アプリの通信と動作

管理サイトに登録されているすべての iOS 端末に、共通する操作（エージェント共通管理、MDM 構成プロファイル共通管理、VPN 共通管理、端末名称変更）を適用します。

各項目の詳細については、以下の画面を参照してください。

- 画面（エージェント共通管理）
- 画面（MDM 構成プロファイル共通管理）
- 画面（VPN 共通管理）
- 画面（端末名称変更）

設定を保存した時点ですべての iOS 端末に適用されます。ただし、設定が端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。

サーバーとの通信間隔や端末の通信状態などにより、バッテリー消費に影響があります。

◆画面（エージェント共通管理）

「Jailbreak 状態検知」の設定を行います。

Jailbreak 状態検知は、Jailbreak された iOS 端末を検知する機能です。検知した場合はログに出力されます。

また、状態の確認は詳細画面の「情報」に表示される［デバイス］で行うことができます。

表示操作　**［設定］→［iOS］→［管理アプリの通信と動作］→「エージェント共通管理」の［編集］**

項番	項目	説明
1	Jailbreak 状態検知	Jailbreak 状態検知を行うかを指定します。 ●「検知する」、「検知しない」

◆画面（MDM 構成プロファイル共通管理）

アクティベーションロックの設定を編集します。アクティベーションロックは、Apple が提供している iPhone の盗難予防機能です。アクティベーションロックを有効にするには、Apple ID とパスワードが必要です。有効化にしたあと、端末が紛失、盗難にあった場合でも、第三者は設定時の Apple ID とパスワードがわからなければ端末の再アクティベーションはできません。この機能で端末紛失時・盗難時の悪用、情報漏洩を防げます。また、セキュリティが確保されることで端末を取り戻せる可能性が高くなります。

アクティベーションロックは、iOS 端末の［iPhone を探す］の設定と合わせて行ってください。

●アクティベーションロックを無効から有効にする場合

・iOS 端末で［iPhone を探す］をオンにします。
・本機能で［許可する］に設定した設定セットを iOS 端末に反映します。

●アクティベーションロックを有効から無効にする場合

・iOS 端末で［iPhone を探す］をオフにします。

本機能で［許可しない］に設定した設定セットを iOS 端末に反映しても、アクティベーションロックは有効から無効になりません。

アクティベーションロックを有効にするには、Apple ID とパスワードが必要です。

有効化にしたあと、端末が紛失、盗難にあった場合でも、第三者は設定時の Apple ID とパスワードがわからなければ、端末の再アクティベーションはできません。

監視対象ではない端末で「iPhone を探す」の設定を ON にすると、アクティベーションロックは自動的に有効化されます。その場合、管理サイトからの解除はできません。
アクティベーションロックの解除は、以下を参照してください。

☞「[その他▼］タブ／iOS リモート操作」210 ページ

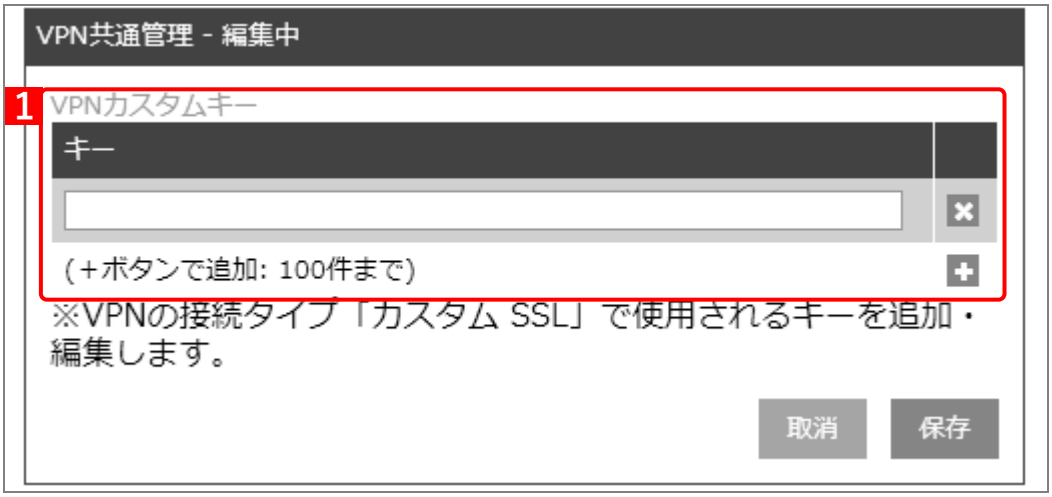
表示操作　［設定］→［iOS］→［管理アプリの通信と動作］→「MDM 構成プロファイル共通管理」の［編集］

項番	項目	説明
1	アクティベーションロック	アクティベーションロックの有効化を許可するかを指定します。 ●許可する アクティベーションロックの有効化を許可します。 ●許可しない アクティベーションロックの有効化を許可しません。

◆画面（VPN 共通管理）

VPN 接続の「カスタム SSL」で使用されるキーを追加、編集します。

表示操作　［設定］→［iOS］→［管理アプリの通信と動作］→「VPN 共通管理」の［編集］



項番	項目	説明
1	VPN カスタムキー	VPN のカスタムキーを記入してください。 ＋ をクリックすると、入力欄が追加されます。 × をクリックすると、入力欄が削除されます。 100 件まで登録できます。

◆画面（端末名称変更）

端末名と［機器］→［一覧］の「機器名」に表示される名称が異なる場合に、端末名を「機器名」に表示される名称に合わせて変更します。

管理画面と端末の名称が同じになるため、管理がしやすくなります。

端末名は、iOS 端末の「設定」アプリ→［一般］→［情報］→「名前」で確認してください。

特定の端末のみ名称を変更することはできません。

変更した端末名は元に戻せないため、管理上元の端末名が必要な場合は、事前に元の端末名を控えておいてください。CSV をダウンロードして保存することをお勧めします。

「CSV をダウンロード」237 ページ

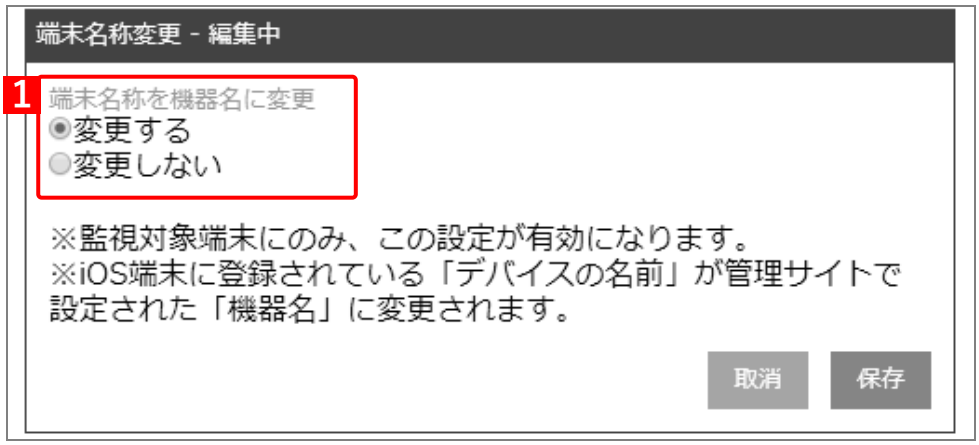
テンプレートとして登録したい各機能の設定セットを、あらかじめ作成してください。

機器画面での機器名の編集、端末名の詳細については、以下を参照してください。

「機器の管理情報」67 ページ

「（情報－iOS）デバイス」151 ページ

表示操作　［設定］→［iOS］→［管理アプリの通信と動作］→「端末名称変更」の［編集］



項番	項目	説明
1	端末名称を機器名に変更	端末名称を機器名に変更するかを指定します。 ●変更する 端末名称を機器名に変更します。 ●変更しない 端末名称を機器名に変更しません。 監視対象端末のみ有効です。

8.2 設定テンプレート

各機能で設定した設定セットの内容を、設定テンプレートとして保存します。

複数の iOS 端末に同じ設定内容を繰り返し設定したい場合や、用途に応じて設定内容を切り替えたいときにテンプレートを使用すると、簡単に設定内容を適用することができます。

本機能では、設定テンプレートの作成や作成したテンプレートをデフォルトに設定するなどの操作を行うことができます。

画面

画面（設定テンプレートの作成）

設定テンプレートを一括で複数の iOS 端末に適用することはできません。

テンプレートとして登録したい各機能の設定セットを、あらかじめ作成してください。

作成した設定テンプレートは、iOS 端末ごと、または組織ごとに適用できます。

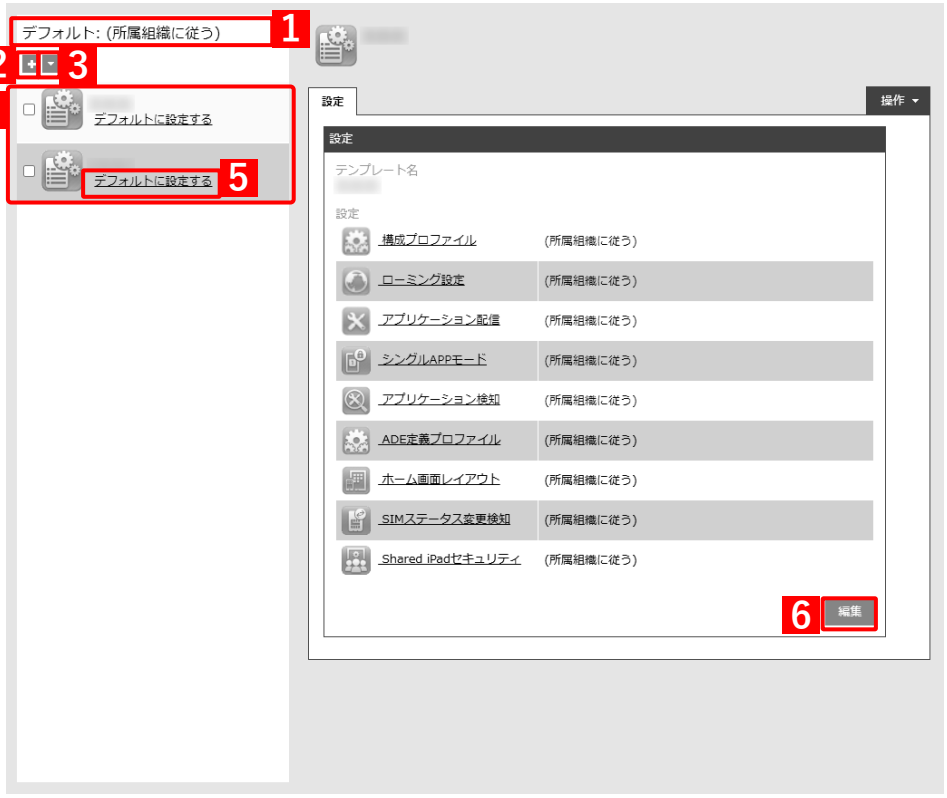
「（設定－iOS）設定テンプレートの割り当て」85 ページ

「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」286 ページ

設定テンプレートは、最大 51 件まで作成できます。

◆画面

表示操作　［設定］→［iOS］→［設定テンプレート］



項番	項目	説明
1	デフォルトテンプレート表示	デフォルトに設定したテンプレートの名称が表示されます。 デフォルトに設定したときは、「(所属組織に従う)」が表示されます。 「(所属組織に従う)」は設定テンプレートの初期設定値です。
2	＋	設定テンプレートを新規に作成します。 「画面（設定テンプレートの作成)」389 ページ

項番	項目	説明
3		設定テンプレートのチェックや、チェックした設定テンプレートの一括削除のほか、デフォルトに設定した設定テンプレートを初期設定値の「(所属組織に従う)」に戻します。 ☞「(所属組織に従う)をデフォルトに設定する」391 ページ
4	設定テンプレート	で作成した設定テンプレートが表示されます。
5	［デフォルトに設定する］	作成した設定テンプレートをデフォルトにします。 ☞「設定テンプレートをデフォルトに設定する」390 ページ
6	［編集］	設定テンプレートを編集します。 ☞「画面（設定テンプレートの作成)」389 ページ

◆画面（設定テンプレートの作成）

表示操作［設定］→［iOS］→［設定テンプレート］→ ＋（一覧から対象を選択→［編集］）

項番	項目	説明
1	テンプレート名	設定テンプレートの名称を 1 文字から 30 文字以内で指定します。
2	設定	各機能に設定する内容を以下から選択します。 ●各機能の設定名 各機能で作成した設定の名称を指定します。指定した設定名に対する編集および削除が行われた場合、設定テンプレートにも反映されます。 ●(所属組織に従う) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(変更しない) 機器ごとに適用している設定に変更を行いません。 ●(設定なし) 各機能の設定を外します。

設定テンプレートをデフォルトに設定する

作成した設定テンプレートをデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が設定テンプレートの内容に設定されます。

管理サイトに登録する端末を同じ設定にしたい場合に便利です。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［iOS］→［設定テンプレート］→デフォルトにするテンプレートの「デフォルトに設定する」

項番	項目	説明
1	デフォルト	デフォルトに設定しているテンプレート名が表示されます。また、デフォルトになっているテンプレート名の下に「デフォルト」と表示されます。(A)の箇所に記載されます。
2	［デフォルトに設定する］	クリックすると、そのテンプレート名の設定をデフォルトにできます。
3	メッセージボックス	選択したテンプレートをデフォルトにすることを確認する画面です。 ●OK 選択したテンプレートをデフォルトに設定します。 ●キャンセル 選択したテンプレートをデフォルトに設定することを中断します。

(所属組織に従う)をデフォルトに設定する

「(所属組織に従う)」をデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が「(所属組織に従う)」に設定されます。

初期設定では、デフォルトに「(所属組織に従う)」が設定されています。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［iOS］→［設定テンプレート］→ ▼ →［(所属組織に従う)をデフォルトにする］

項番	項目	説明
1	(所属組織に従う)をデフォルトにする	各種設定内容が「(所属組織に従う)」になるテンプレートをデフォルトにします。
2	メッセージボックス	デフォルトに設定することを確認する画面です。 ●OK 「(所属組織に従う)」をデフォルト設定します。 ●キャンセル 設定を行いません。

8.3 構成プロファイル

構成プロファイルは、Apple が提供している Apple Configurator 2 上で作成できるプロファイルで iOS 端末に対する制御や設定ができます。

本設定では、管理サイト上で作成した構成プロファイルを保存し、保存した構成プロファイルを使用して、構成プロファイルの設定セットを作成することができます。

また、Apple Configurator 2 で作成した構成プロファイルを管理サイトにアップロードし、新しいプロファイル名を付けて保存することで、Apple Configurator 2 で作成した構成プロファイルを利用することもできます。

- Apple Configurator 2 の詳細については、Apple に問い合わせてください。
- 監視対象の端末にのみ利用できる「コンテンツフィルタ設定」、または「グローバル HTTP プロキシ設定」を含む構成プロファイルは、監視対象ではない端末には反映できません。［iOS 制限設定］タブの各画面に表示される「(監視対象のみ)」の設定を含む構成プロファイルを、監視対象ではない端末に適用した場合は、構成プロファイルは適用されますが、「(監視対象のみ)」の設定は反映されません。
- ［構成プロファイル］の「削除防止」項目を設定した場合、端末に構成プロファイルを再適用するには、端末のポータルから構成プロファイルをインストールしてください。
- すでに構成プロファイルが適用されている端末に、構成プロファイルの再適用を行うと、あとから配布された構成プロファイルに上書きされますので、注意してください。ただし、後述の削除防止が設定された構成プロファイルは上書きされません（削除するにはワイプまたは Apple Configurator 2 での作業が必要です）。この場合は、各構成プロファイルの内容が結合されて適用されます。同一の項目に複数の設定が存在する場合、どの設定を優先するかなど、結合方法の詳細については Apple の仕様に依存するため、本製品では制御を行っていません。
- 構成プロファイル配信時、競合する（相反する）設定内容を適用すると OS の判断で、より安全なものが反映されます（設定内容によってはインストールエラーが発生する場合があります）。
- 構成プロファイルのアップロードについては、以下を参照してください。

「構成プロファイルアップロード」393 ページ

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「(設定－iOS) 設定の割り当て」83 ページ
「全機器一括設定」200 ページ

8.3.1 構成プロファイルアップロード

構成プロファイルの設定セットを作成するときに使用する構成プロファイルを作成します。本設定では、各のタブで iOS 端末のパスコードや、各種制限に関する設定（「FaceTime を許可(監視対象のみ)」、「共有アルバムを許可」など）を簡単に行うことができます。

［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→［その他▼］→［コンテンツフィルタ設定］で「アダルトコンテンツを制限」もしくは「指定した Web サイトのみ」が指定されている場合、MDM ライセンス認証時に「※インストール画面が表示されない場合はこちらを押してください。」のリンクが機能せず、MDM 構成プロファイルをインストールできません。

iOS 9.0～9.1 の場合、端末に反映された構成プロファイルの「コンテンツフィルタ設定」機能→「許可された Web サイト」オプションに、「アダルトコンテンツを制限」、または「指定した Web サイトのみ」が指定されている場合、ポータルからこの端末に削除防止を設定された構成プロファイルはインストールできません（この場合、構成プロファイルが適用されても、Safari 上での構成プロファイルのインストール画面に移行しません）。
削除防止を設定された構成プロファイルについては、以下を参照してください。

☞「構成プロファイル」500 ページ

1 企業がアップロードできる構成プロファイルは 300 ファイルです。

8.3.1.1 ［管理］タブ

構成プロファイルの名称と設定内容を新規に作成するか、Apple Configurator 2 で作成したファイルの内容を利用するかを設定します。

構成プロファイルを新規作成し、［管理］タブの内容を設定して保存すると、［管理］タブを含む［一般］／［パスコード設定］／［iOS 制限設定］／［Wi-Fi 設定］／［その他］の各タブで、編集を行うことができます。

また、作成した構成プロファイルを一覧から選択し、ファイルとして PC にダウンロードすることもできます。

［管理］タブでは、構成プロファイルの新規作成、編集およびダウンロードを行うことができます。

画面（新規作成）

画面（編集）

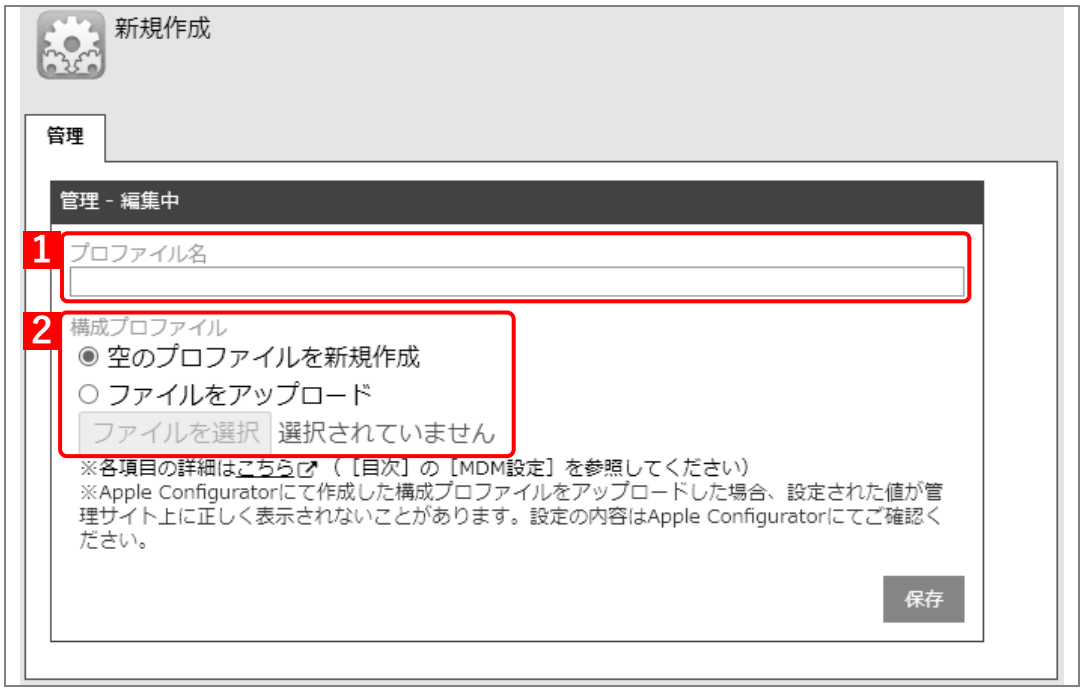
画面（ダウンロード）

［構成プロファイルアップロード］で設定できる項目は、Apple Configurator 2 で設定できる項目よりも少ないため、Apple Configurator 2 で作成した構成プロファイルを編集する場合は、本機能を使用せず、Apple Configurator 2 で行ってください。
Apple Configurator 2 で作成した構成プロファイルを本機能で編集した場合の動作は保証しておりません。

設定セットは、最大 300 件まで作成できます。

◆画面（新規作成）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→ ✚

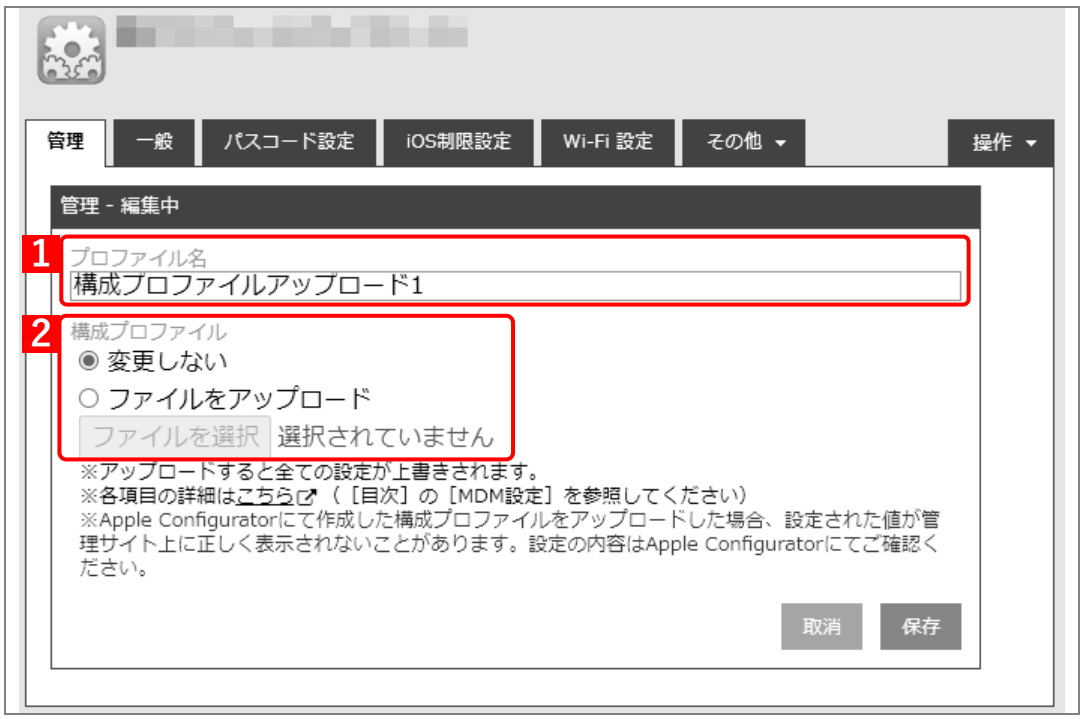


項番	項目	説明
1	プロファイル名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	構成プロファイル	アップロードする構成プロファイルを指定します。 ●空のプロファイルを新規作成 空のプロファイルをアップロードします。詳細については、以下を参照してください。 ☞「構成プロファイルアップロード」393 ページ ●ファイルをアップロード 構成プロファイルをアップロードします。［ファイルを選択］をクリックして、アップロードするファイルを指定します。 インストール時にユーザー名やパスワードを求められる構成プロファイルはインストールできません。ユーザー名やパスワードの設定のない構成プロファイルを指定してください。 Apple Configurator 2（※1）で構成プロファイルを作成する場合、VPN ペイロードの接続タイプ（VPNType）は、以下を設定してください。 ・L2TP ・PPTP ・PSec ・IKEv2 ・AlwaysOn（VPN 常時接続が ON の場合） ・VPN（Aruba VIA、Check Point Mobile VPN、Cisco AnyConnect、Cisco Legacy AnyConnect、F5 SSL、Juniper SSL、Pulse Secure）

※1：Apple Configurator 2 の詳細については、Apple に問い合わせてください。

◆画面（編集）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［管理］タブ→［編集］**



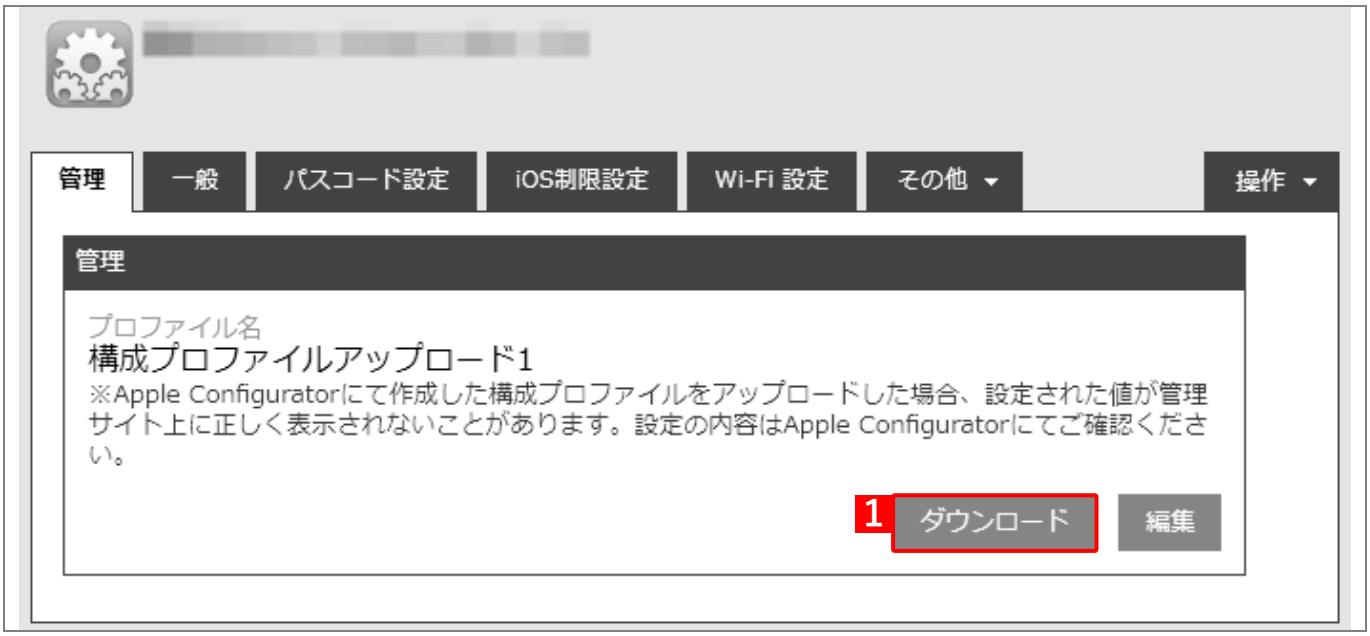
項番	項目	説明
1	プロファイル名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	構成プロファイル	アップロードする構成プロファイルを指定します。 ●変更しない 構成プロファイルを変更しません。（編集を取り消すことと同じです） ●ファイルをアップロード 構成プロファイルを上書きします。［ファイルを選択］をクリックして、アップロードするファイルを指定してください。

◆画面（ダウンロード）

管理サイトで作成して保存されている構成プロファイルを、一覧から選択してダウンロードします。

設定内容を流用し、少しだけ異なる構成プロファイルを作成したい場合などに便利です。

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択**



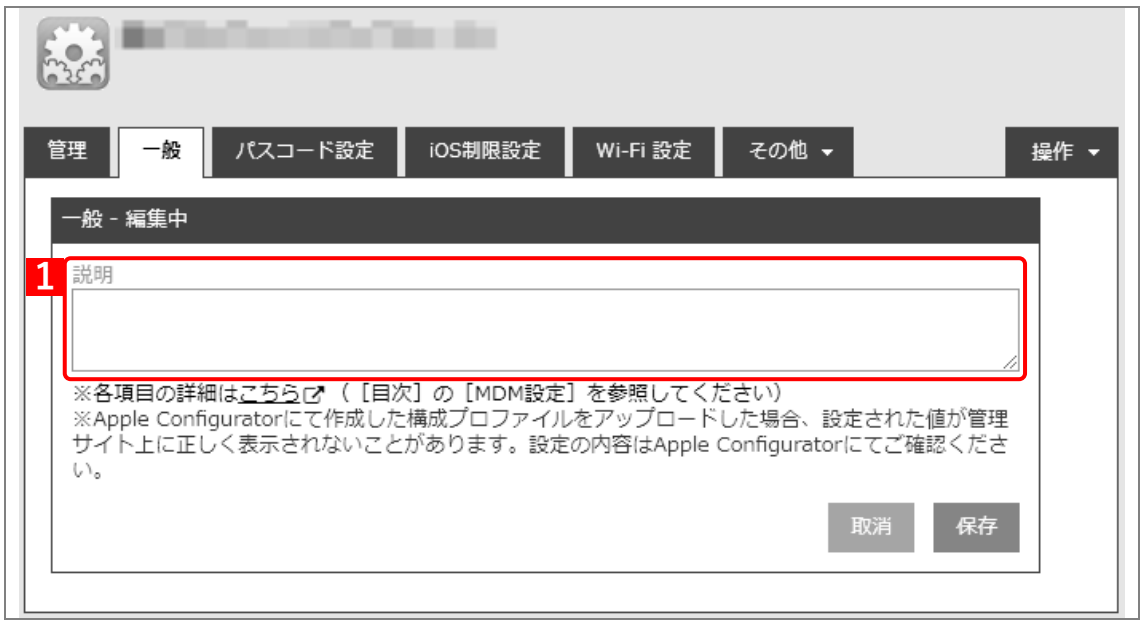
項番	項目	説明
1	［ダウンロード］	クリックして、任意の場所に構成プロファイルを保存してください。

8.3.1.2 ［一般］タブ

作成した構成プロファイルの説明を入力します。

◆画面

表示操作 **［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［一般］タブ→［編集］**



項番	項目	説明
1	説明	構成プロファイルの説明を入力してください。1 文字から 1,000 文字で入力してください。

8.3.1.3 ［パスコード設定］タブ

パスコード（画面ロックを解除するときに入力する文字列）に関する各種の設定を行います。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［パスコード設定］タブ→［新規作成］または［編集］

項番	項目	説明
1	単純値を許可	●する 「する」にチェックを入れると、パスコードに連続する文字や反復する文字を使用することをユーザーに許可します。例えば、「3333」や「DEFG」のようなパスコードが許可されます。
2	英数字の値が必要	●はい 「はい」をチェックすると、パスコードに少なくとも 1 つの英数字を含めることを強制します。
3	最小のパスコード長	パスコードの最小文字数を指定します。以下から選択します。 ●「(なし)」、「1」、「2」、「3」、「4」、「5」、「6」、「7」、「8」、「9」、「10」、「11」、「12」、「13」、「14」、「15」、「16」
4	複合文字の最小数	パスコードに必要な英数字以外の文字（$、&、!、@など）の最小数を指定します。以下から選択します。 ●「(なし)」、「1」、「2」、「3」、「4」
5	パスコードの有効期限（1～730日、またはなし）	指定した間隔（日数）でユーザーにパスコードの変更を要求します。1 以上 730 以下を半角数字で入力してください。 指定しない場合は、空欄にしてください。
6	自動ロックまでの最長時間（分）	自動ロックまでの最大時間を指定します。以下から選択します。 「10」、「15」は iPad の場合のみ使用できます。 ●「(なし)」、「1」、「2」、「3」、「4」、「5」、「10」、「15」

項番	項目	説明
7	パスコードの履歴（1～50 個のパスコード、またはなし）	新しいパスコードが以前に使用したパスコードと一致した場合、そのパスコードは受け入れられません。この設定では、受け入れ禁止として記憶するパスコードの数を指定します。1 以上 50 以下を半角数字で入力してください。 指定しない場合は、空欄にしてください。
8	デバイスロックの最大猶予期間	パスコードの入力を行わずに、ロックを解除できるまでの最大時間を指定します。以下から選択します。 ●「(なし)」、「即時」、「1 分」、「5 分」、「15 分」、「1 時間」、「4 時間」
9	入力を失敗できる回数	ロック解除のとき、試行できるパスコード誤入力の回数を決定します。以下から選択します。 ●「(なし)」、「2」、「3」、「4」、「5」、「6」、「7」、「8」、「9」、「10」

8.3.1.4 ［iOS 制限設定］タブ

端末機能の制限、アプリの制限、メディアコンテンツの制限について設定します。

画面（機能の制限）

画面（App の制限）

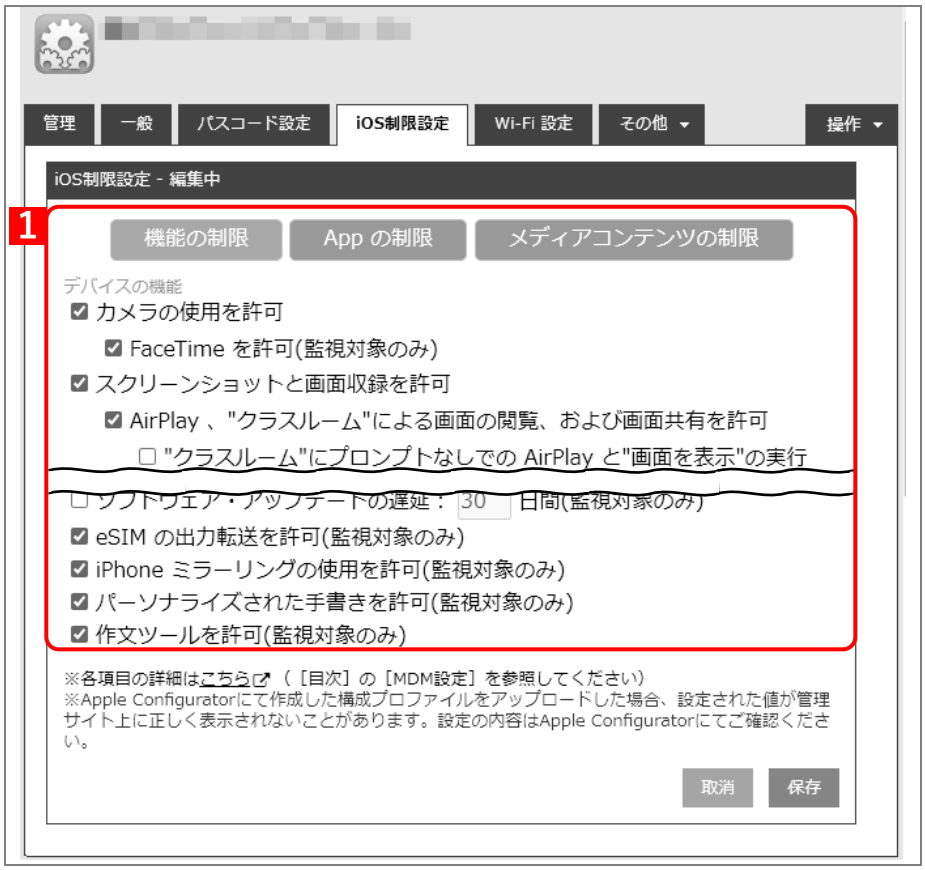
画面（メディアコンテンツの制限）

iOS 端末のバージョンによって、挙動が異なります。対応バージョンについては、以下を参照してください。また、参照先の記載内容と実際の画面の表記が異なる場合があります。

https://support.apple.com/ja-jp/guide/mdm/mdm0f7dd3d8/web

◆画面（機能の制限）

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［iOS 制限設定］タブ→［新規作成］または［機能の制限］→［編集］



項番	項目	説明
1	デバイスの機能	● カメラの使用を許可 チェックボックスのチェックを外すと、カメラは完全に無効になり、カメラアイコンがホーム画面から削除されます。ユーザーは写真やビデオを撮ったり、「FaceTime」を使うことはできません。 iOS 13.5 以上は監視対象のみ有効です。 ・FaceTime を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは FaceTime ビデオコールの配置または受信ができません。 ●スクリーンショットと画面収録を許可 チェックボックスのチェックを外すと、ユーザーはディスプレイのスクリーンショットと画面収録を保存できません。 ・AirPlay、"クラスルーム"による画面の閲覧、および画面共有を許可 チェックボックスのチェックを外すと、「クラスルーム」を使っている教師は、生徒の

項番	項目	説明
		iPad 画面で AirPlay を使用したり、生徒の iPad 画面を表示したりできません。 ・"クラスルーム"にプロンプトなしでの AirPlay と"画面を表示"の実行を許可(監視対象のみ) チェックボックスのチェックを入れると、教師が管理対象クラスの生徒の iPad で AirPlay や画面表示を使用するときに、生徒が通知を受けなくなります。 ●AirDrop を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは App で AirDrop を使用できなくなります。 ●iMessage を許可(監視対象のみ) チェックボックスのチェックを外すと、iMessage を使用したメッセージの送受信ができなくなります。iOS 端末が SMS に対応している場合、SMS の送受信はできます。SMS に対応していない場合は、ホーム画面から「メッセージ」アイコンが削除されます。 ●Apple Music を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーはミュージックアプリ内の Apple Music に関連する機能を使用できなくなります。 ●ラジオを許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーはミュージックアプリ内のラジオに関連する機能を使用できなくなります。 ●Siri を許可 チェックボックスのチェックを外すと、ユーザーは Siri、音声コントロール、または読み上げを使用できません。 ・デバイスのロック中も Siri を許可 チェックボックスのチェックを外すと、ユーザーはパスコードを使って機器のロックを解除しないと Siri を使用できなくなります。 ・Siri の不適切な単語フィルタを有効にする(監視対象のみ) チェックボックスのチェックを外すと、不適切な単語がフィルタリングされなくなります。 ・Siri にユーザ生成コンテンツを表示(監視対象のみ) チェックボックスのチェックを外すと、ユーザ生成コンテンツを許可するソース（Wikipedia など）のコンテンツにアクセスできなくなります。 ●Siri の検索候補を許可 チェックボックスのチェックを外すと、検索候補が表示されなくなります。 ●Apple Books を許可(監視対象のみ) チェックボックスのチェックを外すと、Apple Books が無効になり、ユーザーが「iBooks」App から Apple Books にアクセスできなくなります。 ●App のインストールを許可(監視対象のみ) チェックボックスのチェックを外すと、App Store は無効になり、アイコンがホーム画面から削除されます。ユーザーは、App Store や「Apple Configurator 2」を使ってアプリのインストールやアップデートはできません。 iOS 13.0 以上は監視対象のみ有効です。 ・App Store からの App のインストールを許可(監視対象のみ) チェックボックスのチェックを外すと、App Store は無効になり、アイコンがホーム画面から削除されます。ただし、ユーザーが「Apple Configurator 2」または MDM を使って App Store から App をインストールやアンインストールはできます。またインハウスエンタープライズ App は引き続きインストールおよびアップデート可能です。 iOS 9.0 以上で設定できます。 ・App の自動ダウンロードを許可(監視対象のみ) チェックボックスのチェックを外すと、ほかのデバイスで購入されたアプリの自動ダウンロードを防止します。すでにインストールされたアプリとデフォルトアプリの更新は防止されません。 iOS 9.0 以上で設定できます。 ●App の削除を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは App を削除できません。App Store や「iTunes」など、iOS に付属している App をユーザーが削除はできません。 iOS 14.0 以上は、「ホーム画面から取り除く」で削除することができます。 ●システム App の削除を許可(監視対象のみ)

項番	項目	説明
		チェックボックスのチェックを外すと、ユーザーは iOS のネイティブ App を削除できません。 iOS 11.0 以上で設定できます。 ●App Clip を許可(監視対象のみ) チェックボックスのチェックを外すと、App Clip を追加できなくなり、デバイス上の既存の App Clip はすべて削除されます。 iOS 14.0 以上で設定できます。 ●App 内課金を許可 チェックボックスのチェックを外すと、ユーザーは App 内で購入できません。 ●iCloud バックアップを許可 チェックボックスにチェックを入れると、ユーザーは機器から iCloud にバックアップを作成できます。 ●iCloud 書類とデータを許可(監視対象のみ) チェックボックスにチェックを入れると、ユーザーは iCloud に書類を保存できます。 iOS 13.0 以上は監視対象のみ有効です。 ●iCloud キーチェーンを許可 チェックボックスのチェックを外すと、iCloud キーチェーンは使用されなくなります。 ●管理対象 App が iCloud にデータを保存することを許可 チェックボックスのチェックを外すと、App による iCloud へのデータ保存が禁止されます。 ●エンタープライズブックのバックアップを許可 チェックボックスのチェックを外すと、ユーザーは組織から配布されたブックのバックアップを iCloud または iTunes に作成できません。 ●エンタープライズブックのメモとハイライトの同期を許可 チェックボックスのチェックを外すと iCloud 経由でほかのデバイスとメモやハイライトを同期できません。 ●共有アルバムを許可 チェックボックスにチェックを入れると、ユーザーはほかの人に自分の写真を見るように勧めたり、ほかの人が共有しているフォトストリームを表示したりできます。 ●iCloud 写真を許可 チェックボックスのチェックを外すと、iCloud のフォトライブラリを無効にします。iCloud のフォトライブラリが無効に設定された場合、ローカルストレージから iCloud のフォトライブラリの画像が削除されます。 iOS 9.0 以上で設定できます。 ●ローミング中の自動同期を許可 チェックボックスのチェックを外すと、ユーザーがアカウントにアクセスしているときに限りローミング中の機器が同期されます。 ●"ファイル"App で USB ドライブへのアクセスを許可(監視対象のみ) チェックボックスのチェックを外すと、ファイル App で接続されている USB デバイスに接続できなくなります。 iOS 13.1 以上で設定できます。 ●"ファイル"App でネットワークドライブへのアクセスを許可(監視対象のみ) チェックボックスのチェックを外すと、ファイル App でネットワークドライブに接続できなくなります。 iOS 13.1 以上で設定できます。 ●App からのトラッキング要求を禁止 チェックボックスにチェックを入れると、App で広告識別子（非永続的、デバイス識別子）を使用してターゲット広告の表示が禁止されます。 ●Apple によるパーソナライズされた広告の配信を許可 チェックボックスのチェックを外すと、パーソナライズド広告を制限します。 iOS 14.0 以上で設定できます。 ●"すべてのコンテンツと設定を消去"を許可(監視対象のみ) チェックボックスのチェックを外すと、端末のリセット機能「すべてのコンテンツと設定を消去」が使用できなくなります。 ●信頼されていない TLS 証明書の受け入れをユーザに許可

項番	項目	説明
		チェックボックスのチェックを外すと、検証できない TLS 証明書をユーザーが許可しようとする場合に、ユーザーに確認を求めません。この設定は「Safari」および「メール/連絡先/カレンダー」アカウントに適用されます。 ●証明書信頼設定の自動アップデートを許可 チェックボックスのチェックを外すと、iOS デバイスが端末内に保持している信頼できる TLS 証明書の信頼設定変更を自動的に受け入れなくなります。 ●新しいエンタープライズ App 作成者の信頼を許可 チェックボックスのチェックを外すと、新しいエンタープライズ App 作成者を信頼できなくなります。すでに信頼済みの作成者については本設定をオフにしても引き続き利用できます。また、その場合、信頼済みの作成者と同じ作成者を利用しているエンタープライズアプリ（InHouse アプリ、オリジナルアプリ）も利用できます。 iOS 9.0 以上で設定できます。 ●構成プロファイルのインストールを許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは各自のデバイスに追加の構成プロファイルをインストールできなくなります。 ●VPN 構成の追加を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは VPN 構成の作成または追加ができなくなります。 ●日付と時刻を強制的に自動設定(監視対象のみ) チェックボックスにチェックを入れると、日付と時刻の自動設定機能が有効になり、ユーザーが無効にすることはできません。デバイスのタイムゾーンは、位置情報サービスが有効になっているセルラー接続または Wi-Fi を使用して、デバイスが位置を特定できる場合にのみ更新されます。 iOS 12.0 以上で設定できます。 ●"クラスルーム"にプロンプトなしでの App の制限とデバイスのロックを許可(監視対象のみ) チェックボックスにチェックを入れると、教師はプロンプトすることなく、App を開いたままロックしたり、デバイスをロックしたりできるようになります。 ●"クラスルーム"のクラスにプロンプトなしで自動的に参加(監視対象のみ) チェックボックスにチェックを入れると、生徒は教師へのプロンプトなしでクラスに参加できるようになります。 ●"クラスルーム"の管理対象外クラスを退席するときに教師の許可を要求(監視対象のみ) チェックボックスにチェックを入れると、生徒は管理対象外（教師作成）クラスを退席する前に許可を要求する必要があります。 ●Wi-Fi の電源を強制的にオン(監視対象のみ) チェックボックスにチェックを入れると、機内モードをオンにしても、設定またはコントロールセンターで Wi-Fi がオフにならないようにします。使用する Wi-Fi ネットワークの選択を妨げるものではありません。 iOS 13.0 以上で設定できます。 ●アカウント設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは新規アカウントの作成も、ユーザー名、パスワードおよびアカウントに紐づけられているその他の設定の変更もできなくなります。 ●Bluetooth 設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは Bluetooth の設定を変更できなくなります。 Bluetooth の ON/OFF だけではなく、Bluetooth デバイスの追加や削除もできません。 端末で Bluetooth を ON に設定している状態で、本設定を適用した場合、ペアリング済みのデバイスは、OS と Bluetooth デバイスの挙動に依存します。 ●モバイルデータ通信 App 設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、モバイルデータ通信 App 設定を変更できなくなります。 ●モバイルデータ通信プラン設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、モバイルデータ通信プラン設定を変更できなくなります。 ●eSIM 設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、キャリアプラン関連の設定の変更を無効にしま

項番	項目	説明
		す（一部のキャリアでのみ利用可能）。 iOS 11.0 以上で設定できます。 ●デバイス名の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、デバイス名の変更を防げます。 iOS 9.0 以上で設定できます。 ●通知設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは通知設定の変更ができなくなります。 ●パスコードの変更を許可(監視対象のみ) チェックボックスのチェックを外すと、デバイスのパスコードを追加、変更、または削除を防げます。 iOS 9.0 以上で設定できます。 ・Touch ID の指紋/Face ID の顔の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、Touch ID に登録された指紋または Face ID の顔の追加・変更・削除ができなくなります。 ●スクリーンタイムを許可(監視対象のみ) チェックボックスのチェックを外すと、端末の［設定］メニューの［スクリーンタイム］が使用できなくなります。 チェックを外して同期すると、端末のスクリーンタイム設定はクリアされ、強制的にオフになります。再度、スクリーンタイム設定をオンにする場合は、本項目にチェックを入れて同期したあと、端末でスクリーンタイム設定を行ってください。 ●壁紙の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、壁紙の変更を防ぐことができます。 iOS 9.0 以上で設定できます。 ●インターネット共有設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、インターネット共有設定の変更を無効にします。 iOS 12.2 以上で設定できます。 ●"友達を探す"を許可(監視対象のみ) チェックボックスのチェックを外すと、「探す」app で「友達を探す」を無効にします。 iOS 13.0 以上で設定できます。 ●"探す"の"デバイスを探す"を許可(監視対象のみ) チェックボックスのチェックを外すと、「探す」app で「デバイスを探す」を無効にします。 iOS 13.0 以上で設定できます。 ●"友達を探す"設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは「友達を探す」App の設定を変更できなくなります。 ●デバイスのロック中も USB アクセサリを許可(監視対象のみ) チェックボックスのチェックを入れると、デバイスがロックされている間、USB アクセサリに接続できます。 iOS 11.4.1 以上で設定できます。 ●Configurator 以外のホストとのペアリングを許可(監視対象のみ) チェックボックスのチェックを外すと、PC（Mac/Windows）に接続してもコンピュータを信頼する/しないのポップアップが非表示になり、データのやり取りができなくなります。 ●ペアリングが解除されたデバイスのリカバリモードへの移行を許可(監視対象のみ) チェックボックスにチェックを入れると、ペアリングされていないデバイスによってデバイスを起動して回復できるようにします。 iOS 14.5 以上で設定できます。 ●管理対象外出力先で管理対象ソースからの書類を許可 「管理対象ソース」は、［その他▼］タブの［ドメイン設定］の「管理対象の Safari Web ドメイン」で指定された Web サイトのコンテンツです。PDF 形式などのコンテンツを Safari からアクセスするときに、Safari の画面下部に Safari 以外の外部アプリからコンテンツを表示するメニュー画面が表示される場合があります。チェックボックスのチェックを外すと、管理サイトで非管理対象として配信したアプリ、もしくは手動で App Store からインストールしたアプリ（管理対象外出力先）は、Safari の外部アプリの一

項番	項目	説明
		覧に表示されなくなります。つまり、管理対象外出力先のアプリから、「管理対象の Safari Web ドメイン」で指定されたコンテンツにアクセスできなくなります。この設定で、Safari を経由した外部アプリの起動を制限できますが、外部アプリから直接 URL を入力する場合など、Safari を経由しないコンテンツアクセスは制御されません。「管理対象の Safari Web ドメイン」については、以下を参照してください。 ☞「[その他▼] タブ／ドメイン設定」434 ページ ●管理対象出力先で管理対象外ソースからの書類を許可 チェックボックスのチェックを外すと、管理対象外 App で作成した書類を管理対象 App で開けなくなります。 ●AirDrop を管理対象外の出力先とみなす チェックボックスにチェックを入れると、AirDrop は管理対象外となります。さらに厳密にダウンロード対象を管理するには [制限] タブの「管理対象外出力先で管理対象ソースからの書類を許可」と「管理対象出力先で管理対象外ソースからの書類を許可」を設定する必要があります。設定は、以下を参照してください。 ☞「画面（機能の制限）」400 ページ iOS 9.0 以上で設定できます。 ●Handoff を許可 チェックボックスのチェックを外すと、Handoff 機能が使用できなくなります。 ●Apple への診断情報と使用状況データの送信を許可 チェックボックスのチェックを外すと、Apple に iOS の診断情報が送信されません。 ・診断設定の変更を許可(監視対象のみ) チェックボックスのチェックを外すと診断設定の変更ができません。 ●Touch ID/Face ID によるデバイスロック解除を許可 チェックボックスのチェックを外すと、ユーザーはデバイスのロックを解除するためにパスコードを入力する必要があります。 ●パスワードの自動入力を許可(監視対象のみ) チェックボックスのチェックを外すと、iOS の自動入力パスワード機能（キーチェーンおよびサードパーティのパスワードマネージャーを使用）が無効になり、ユーザーは Safari またはアプリで保存されたパスワードを使用するように求められません。この制限によりパスワードの自動入力も無効になり、強度の高いパスワードはユーザーに提案されなくなります。Safari での連絡先情報とクレジットカードの自動入力は妨げられません。 iOS 12.0 以上で設定できます。 ●自動入力の前に Touch ID/Face ID 認証を要求(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは Touch ID/Face ID 認証を使って App データを自動入力できません。 ●Apple Watch によるロック解除を許可 チェックボックスのチェックを外すと、Apple Watch による自動ロック解除を無効にします。 iOS 14.5 以上で設定できます。 ●Apple Watch の手首検出を強制 チェックボックスにチェックを入れると、ペアリングされた Apple Watch は手首の検出を使用するように強制されます。 iOS 8.2 以上で設定できます。 ●Apple Watch とのペアリングを許可(監視対象のみ) チェックボックスのチェックを外すと、Apple Watch とのペアリングを無効にします。既存のペアリングは無効になり、Apple Watch は初期化されます。 iOS 9.0 以上で設定できます。 ●最初の AirPlay ペアリングでパスコードを要求 チェックボックスにチェックを入れると、最初の AirPlay ペアリングで端末のパスコードが要求されます。 ●Wi-Fi ペイロードによってインストールされた Wi-Fi ネットワークのみに接続(監視対象のみ) チェックボックスにチェックを入れると、構成プロファイルで登録済みの Wi-Fi のみにアクセスできるようになります。Wi-Fi のみを利用している端末が Wi-Fi のアクセスポイントを 1 つも登録していない状態で、このオプションをオンにした構成プロファイル

項番	項目	説明
		をインストールした場合は、同期ができなくなります。この場合は、以下の「復旧方法」で再度同期ができるようになります。条件が揃っていない場合は、端末の初期化を行うしか方法がなくなりますのでご注意ください。 ☞「復旧方法」407 ページ iOS 14.5 以上で設定できます。 ●近くのデバイスの新規設定を許可(監視対象のみ) チェックボックスのチェックを外すと、新しい Apple デバイスの初期設定をしたときに、自動的に設定を行ったり、データを移行したりできなくなります。 ●近接通信に基づくパスワード共有要求を許可(監視対象のみ) チェックボックスのチェックを外すと、近くのデバイスからのパスワードの要求を無効にします。 iOS 12.0 以上で設定できます。 ●パスワードの共有を許可(監視対象のみ) チェックボックスのチェックを外すと、AirDrop によるパスワードの共有を無効にします。 iOS 12.0 以上で設定できます。 ●AirPrint を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは AirPrint を使用できません。 ・iBeacon を使った AirPrint プリンタの検出を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは周辺の iBeacon 互換ハードウェアトランスミッタを使って AirPrint プリンターを検出できません。 ・キーチェーンへの AirPrint 資格情報の保存を許可(監視対象のみ) チェックボックスのチェックを外すと、ユーザーは AirPrint 資格情報をキーチェーンに保存できません。 ・証明書が信頼されていない出力先への AirPrint を禁止(監視対象のみ) チェックボックスにチェックを入れると、AirPrint を使って TLS 証明書が信頼されていないプリンターにプリントできなくなります。 ●予測表示キーボードを許可(監視対象のみ) チェックボックスのチェックを外すと、予測入力キーボードが無効になります。 iOS 8.1.3 以上で設定できます。 ●キーボードショートカットを許可(監視対象のみ) チェックボックスのチェックを外すと、キーボード ショートカットを無効にします。 iOS 9.0 以上で設定できます。 ●なぞり入力キーボードを許可(監視対象のみ) チェックボックスのチェックを外すと、なぞり入力 キーボードを無効にします。 iOS 13.0 以上で設定できます。 ●自動修正を許可(監視対象のみ) チェックボックスのチェックを外すと、キーボードの自動修正機能が無効になります。 iOS 8.1.3 以上で設定できます。 ●スペルチェックを許可(監視対象のみ) チェックボックスのチェックを外すと、キーボードのスペルチェックが無効になります。 iOS 8.1.3 以上で設定できます。 ●定義を許可(監視対象のみ) チェックボックスのチェックを外すと、単語の定義の検索機能が無効になります。 iOS 8.1.3 以上で設定できます。 ●音声入力を許可(監視対象のみ) チェックボックスのチェックを外すと、デバイスでの音声入力を使用できません。 ●ロック画面でのウォレット通知を許可 チェックボックスのチェックを外すと、ロックされている間は機器にウォレット通知が表示されなくなります。 ●ロック画面にコントロールセンターを表示 チェックボックスのチェックを外すと、ユーザーは上にスワイプしてコントロールセンターを表示できなくなります。 ●ロック画面に通知センターを表示

項番	項目	説明
		チェックボックスのチェックを外すと、画面がロックされている場合にユーザーは通知を受信できなくなります。 ●ロック画面に今日表示を表示 チェックボックスのチェックを外すと、ユーザーは下にスワイプして今日表示を使用する通知センターをロック画面で表示できなくなります。チェックボックスにチェックを入れると、ロック画面に本日の日付が表示されます。 ●ソフトウェア・アップデートの遅延：xx 日間(監視対象のみ) チェックボックスにチェックを入れると、「xx」で指定した期間、ユーザーがワイヤレス接続（Wi-Fi およびモバイルデータ通信）を使ってデバイスを手動でアップデートすることを禁止できます。 アップデートを禁止する日数は初期値として「30 日間」に設定されていますが、1～90 日の範囲で変更できます。 遅延期限内でも「Apple Configurator 2」または「iTunes」を使ったデバイスのアップデート、および MDM からの OS アップデートは可能です。 ☞「(操作－iOS) OS アップデート」126 ページ 遅延期限のカウントダウンは、端末の OS から見て次回バージョンのアップデート公開日から開始され、設定した遅延期限日になると、iOS 端末にアップデートを求める通知が表示されます。遅延期間内に、次のバージョンへアップデートしたい場合は、チェックボックスのチェックを外して、iOS 端末に同期を行ってください。詳細については、以下の一例を参照してください。 ☞「iOS アップデート公開日と遅延期限の一例」408 ページ ●eSIM の出力転送を許可(監視対象のみ) チェックボックスのチェックを外すと、制限がインストールされているデバイスから別のデバイスへの eSIM の転送を防止します。 iOS 18.0 以上で設定できます。 ●iPhone ミラーリングの使用を許可(監視対象のみ) チェックボックスのチェックを外すと、iPhone ミラーリングの使用を禁止します。 iOS 18.0 以上で設定できます。 Shared iPad（共有 iPad）は利用できません。 ●パーソナライズされた手書きを許可(監視対象のみ) チェックボックスのチェックを外すと、システムがユーザの手書きでテキストを生成しないようにします。 iOS 18.0 以上で設定できます。 Shared iPad（共有 iPad）は利用できません。 ●作文ツールを許可(監視対象のみ) チェックボックスのチェックを外すと、Apple Intelligence 作文ツールが無効になります。 iOS 18.0 以上で設定できます。 Shared iPad（共有 iPad）は利用できません。

◆復旧方法

●パターン 1

- SIM カードが利用できる端末であることを確認します。
- 通信できる SIM カードを入れてください。
- 通信ができるようになりましたら正しい構成プロファイルを再配信してください。

●パターン 2

- 構成プロファイルの「構成プロファイルのインストールを許可」が「はい」になっていることを確認します。
- Mac と USB 接続などをして、Apple Configurator 2 からアクセスポイントの含まれる構成プロファイルを追加してください。
- 通信ができるようになりましたら正しい構成プロファイルを再配信してください。

●パターン 3

・ADE 利用で「MDM 構成プロファイルの削除」を許可している、または ADE 端末以外であることを確認します。

・MDM 構成プロファイルを削除し、再認証してください。

●パターン 4

・ADE 利用で「MDM 構成プロファイルの削除」を許可していないことを確認します。

・端末を初期化してください。

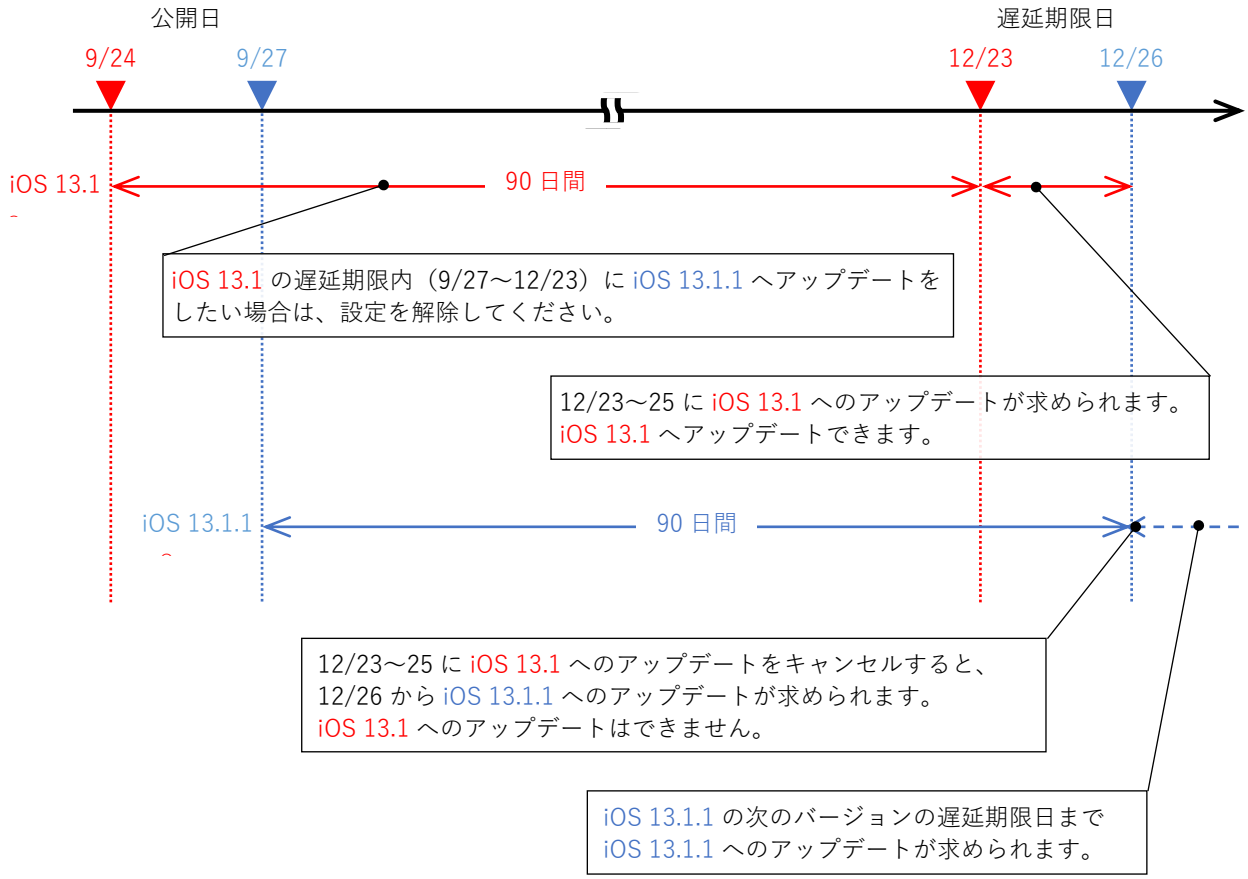
◆iOS アップデート公開日と遅延期限の一例

・利用している iOS 端末のバージョンが iOS 13.0

・ソフトウェア・アップデートの遅延を 90 日間に設定

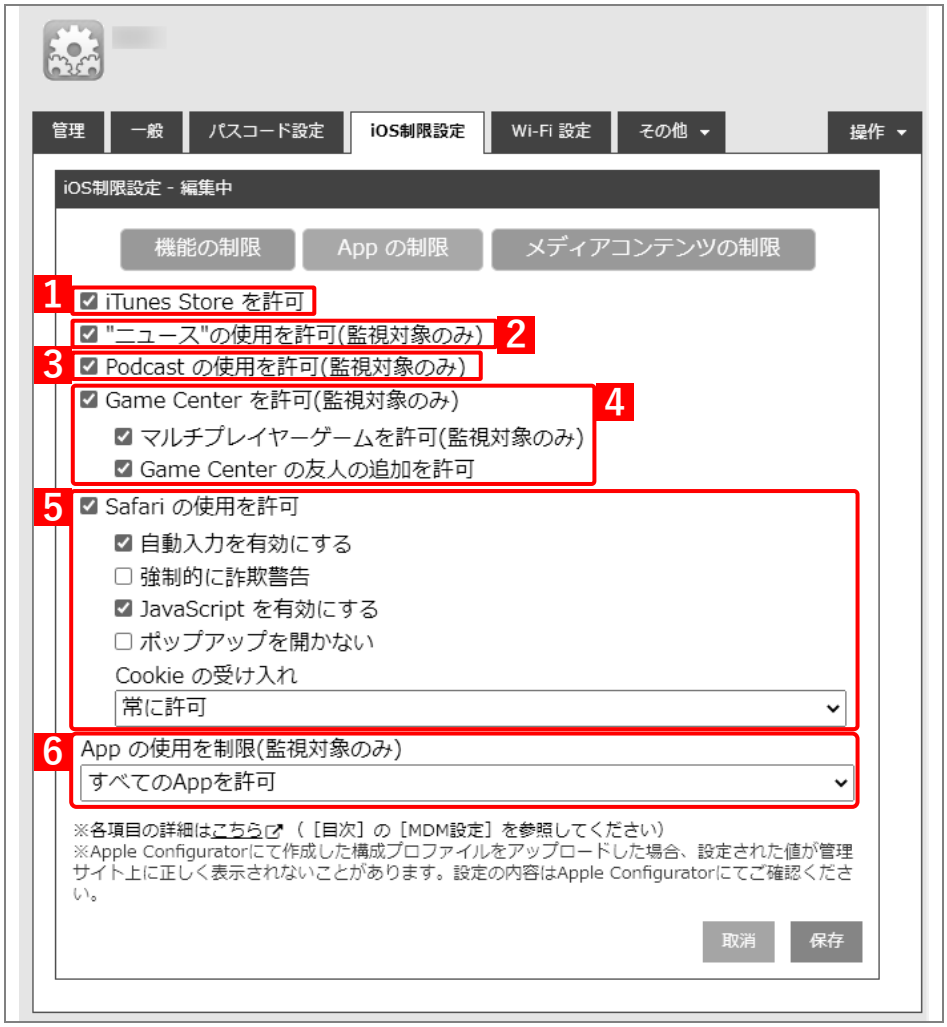
・iOS 13.1 のアップデートが 9/24 に公開
9/24 からカウントダウン開始、90 日後の 12/23 が遅延期限日

・iOS 13.1.1 のアップデートが 9/27 に公開
9/27 からカウントダウン開始、90 日後の 12/26 が遅延期限日



◆画面（App の制限）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［iOS 制限設定］タブ→［新規作成］または［App の制限］→［編集］



項番	項目	説明
1	iTunes Store を許可	チェックボックスのチェックを外すと、iTunes Store は無効になり、アイコンがホーム画面から削除されます。ユーザーはコンテンツをプレビュー、購入、およびダウンロードできません。 iOS 13.0 以上は監視対象のみ有効です。
2	“ニュース”の使用を許可(監視対象のみ)	チェックボックスのチェックを外すと、ニュースが無効になります。
3	Podcast の使用を許可(監視対象のみ)	チェックボックスのチェックを外すと、Podcast が無効になります。
4	Game Center を許可(監視対象のみ)	●マルチプレイヤーゲームを許可 チェックボックスのチェックを外すと、ユーザーは Game Center でマルチプレイヤーゲームをプレイできません。 監視対象端末の場合のみ適用されます。 ●Game Center の友人の追加を許可 チェックボックスのチェックを外すと、ユーザーは Game Center に友達を追加できません。 iOS 13.0 以上は監視対象のみ有効です。

項番	項目	説明
5	Safari の使用を許可	チェックボックスのチェックを外すと、Safari Web ブラウザーApp は無効になり、アイコンがホーム画面から削除されます。ユーザーが Web クリップの表示もできなくなります。 ●自動入力を有効にする チェックボックスのチェックを外すと、「Safari」はユーザーが Web フォームに入力した値を記憶しません。 ●強制的に詐欺警告 チェックボックスのチェックを外すと、「Safari」は不正または欠陥があると判断された Web サイトへのアクセスを禁止しません。 ●JavaScript を有効にする チェックボックスのチェックを外すと、「Safari」は Web サイト上のすべての JavaScript を無視します。 ●ポップアップを開かない チェックボックスのチェックを外すと、「Safari」のポップアップブロック機能が無効になります。 ●Cookie の受け入れ 以下から選択します。 ・「常にブロック」、「アクセス中の Web サイトのみ許可」、「訪問した Web サイトは許可」、「常に許可」
6	App の使用を制限(監視対象のみ)	App の使用を制限します。以下の項目から選択します。 ●「一部の App を許可しない」、「一部の App のみを許可」、「すべての App を許可」 一部の App の許可もしくは禁止を選択すると、対象のアプリを指定する欄が表示されます。指定できるアプリの上限は 1,000 件です。 アプリの指定は、アプリケーション ID（Bundle Identifier）で行います。Store ID ではありませんので、注意してください。 アプリケーション ID の確認については、以下を参照してください。 ☞「(情報－iOS）アプリケーション」157 ページ ☞「アプリケーションレポート」241 ページ 以下の Apple が提供するアプリは禁止できません。 ・「設定」、「電話」

◆画面（メディアコンテンツの制限）

表示操作［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［iOS 制限設定］タブ→［新規作成］または［メディアコンテンツの制限］→［編集］

項番	項目	説明
1	レーティングの地域設定	レーティングの地域を以下から選択します。 ●「アメリカ」、「オーストラリア」、「カナダ」、「ドイツ」、「フランス」、「アイルランド」、「日本」、「ニュージーランド」、「イギリス」
2	許可されるコンテンツレーティング	●ムービー 「レーティングの地域設定」で選択された国のレーティングの一覧から適切なレーティングを以下から選択します。 ・「ムービーを許可しない」、「G」、「PG-12」、「R-15」、「R-18」、「すべてのムービーを許可」 ●テレビ番組 「レーティングの地域」で選択された国のレーティングの一覧から適切なレーティングを以下から選択します。 ・「テレビ番組を許可しない」、「不適切な内容を許可」、「すべてのテレビ番組を許可」 ●App 以下から選択します。 ・「App を許可しない」、「4+」、「9+」、「12+」、「17+」、「すべての App を許可」 ●不適切なミュージック、Podcast、iTunes U の再生を許可 チェックボックスのチェックを外すと、iTunes Store 内の不適切な内容の音楽やビデオコンテンツが隠されます。不適切な内容は、コンテンツプロバイダによってフラグが設定されています。 iOS 13.0 以上は監視対象のみ有効です。

項番	項目	説明
		●Apple Books で不適切な性的描写のあるブックの閲覧を許可 チェックボックスのチェックを外すと、Apple Books のアダルト向けコンテンツが隠されます。不適切な内容は、コンテンツプロバイダによってフラグが設定されています。

8.3.1.5 ［Wi-Fi 設定］タブ

Wi-Fi に関する各種の設定を行います。「プロキシ設定」や「ネットワークのタイプ」などの設定により、タブ内の設定内容が異なります。

画面（プロキシ設定：なし）

画面（プロキシ設定：手動）

画面（プロキシ設定：自動）

画面（ネットワークのタイプ：Passpoint）

画面（エンタープライズ設定（プロトコル））

画面（エンタープライズ設定（信頼））

画面（高速レーンの QoS マーキング：QoS マーキングを制限する）

モバイルネットワークが利用できない端末で本設定を行う場合、設定内容に誤りがあると Wi-Fi に接続できず、通信ができなくなる場合があります。設定内容を確認したうえで使用してください。

［Wi-Fi 設定］タブの設定は、Wi-Fi の設定を端末に反映させる機能です。通信手段を制限する機能ではありません。ただし、端末の［設定］→［Wi-Fi］でプロキシ設定が変更された場合は、同期を行うと、設定した内容に上書きされます。

◆画面（プロキシ設定：なし）

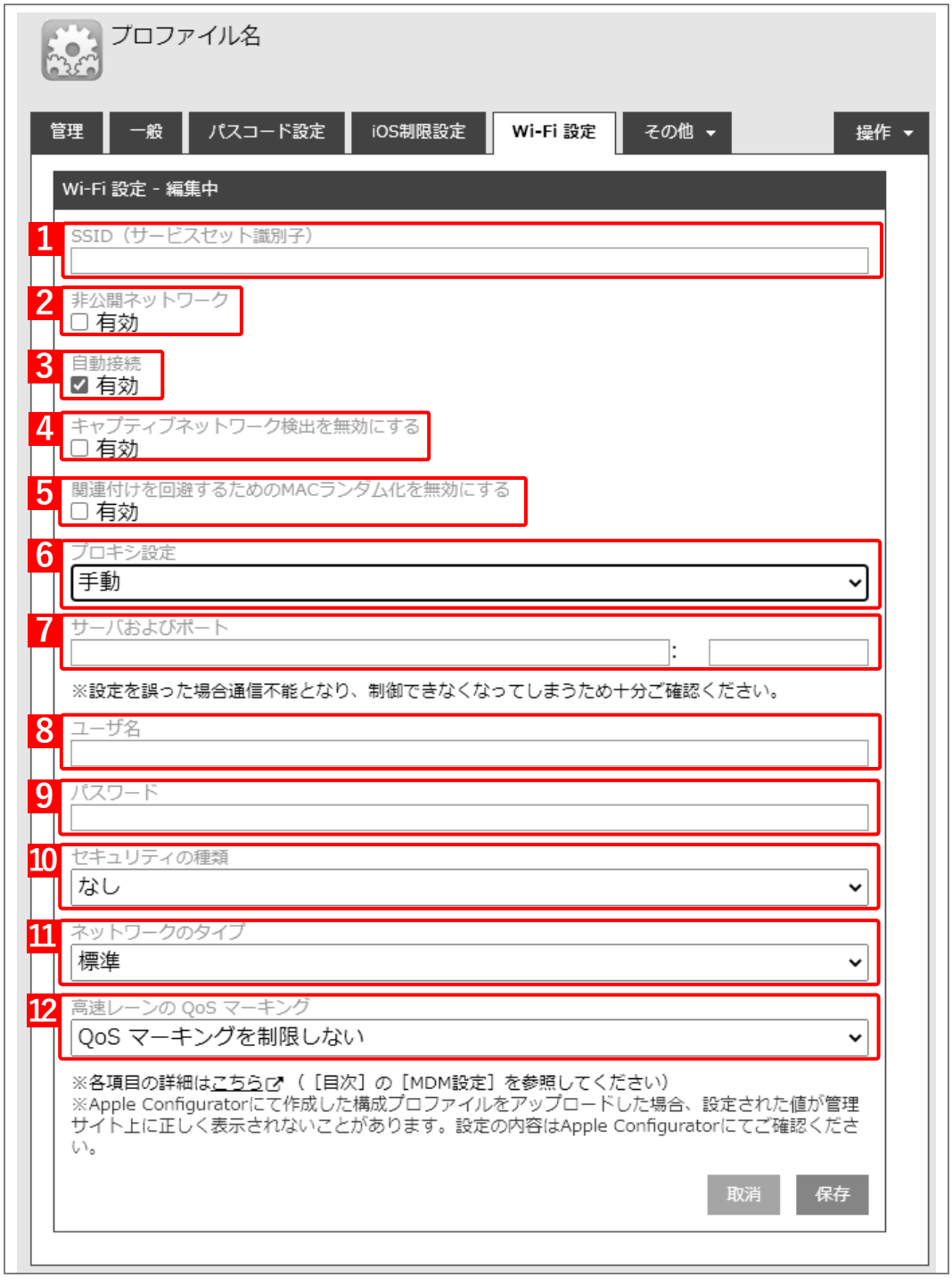
表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］**

項番	項目	説明
1	SSID(サービスセット識別子)	利用する Wi-Fi ネットワークの SSID の名称を入力してください。
2	非公開ネットワーク	●有効 非公開ネットワークを端末に表示する場合は、「有効」にチェックを入れます。
3	自動接続	●有効 自動接続を行う場合は、「有効」にチェックを入れます。 端末の Wi-Fi 設定をオフにしている場合は、自動接続されません。オンにしている場合、項番 1 で設定した SSID に自動接続されます。
4	キャプティブネットワーク検出を無効にする	●有効 キャプティブネットワークの検出を無効にする場合は、「有効」にチェックを入れます。

項番	項目	説明
5	関連付けを回避するためのMAC ランダム化を無効にする	●有効 iOS 14.0 以上の端末で、MAC アドレスのランダム化を無効にする場合は、「有効」にチェックを入れます。 iOS 14.0 以上の端末の［設定］→［Wi-Fi］→［プライベートアドレス］が無効になります。デフォルト値は有効になっています。 iOS 14.0～14.1 の端末の場合は、本設定を無効にしても、端末から手動で有効に変更できます。 iOS 14.0 未満の端末に配信したあとで、iOS 14.0 以上にアップデートしても無効になりません。
6	プロキシ設定	「なし」を選択します。
7	セキュリティの種類	Wi-Fi のセキュリティを設定します。以下の項目から選択します。 ●「なし」、「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」、「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」、「任意（エンタープライズ）」 「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」を選択した場合は、「パスワード」が表示されますので、入力してください。 「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」を選択した場合は、エンタープライズ設定の項目が表示されます。 「画面（エンタープライズ設定（プロトコル））」420 ページ 「画面（エンタープライズ設定（信頼））」422 ページ
8	ネットワークのタイプ	ネットワークのタイプを以下の項目から選択します。 ●標準 標準ネットワークの場合に選択します。 ●レガシーホットスポット レガシーホットスポットの場合に選択します。 ●Passpoint Passpoint の場合に選択します。選択すると設定項目が表示されます。設定項目については、以下を参照してください。 「画面（ネットワークのタイプ：Passpoint）」419 ページ
9	高速レーンの QoS マーキング	QoS マーキングを制限するかどうかを以下の項目から選択します。 ●QoS マーキングを制限しない QoS マーキングを制限しません。 ●QoS マーキングを制限する 選択すると、制限についての設定項目が表示されます。設定項目については、以下を参照してください。 「画面（高速レーンの QoS マーキング：QoS マーキングを制限する）」422 ページ

◆画面（プロキシ設定：手動）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］



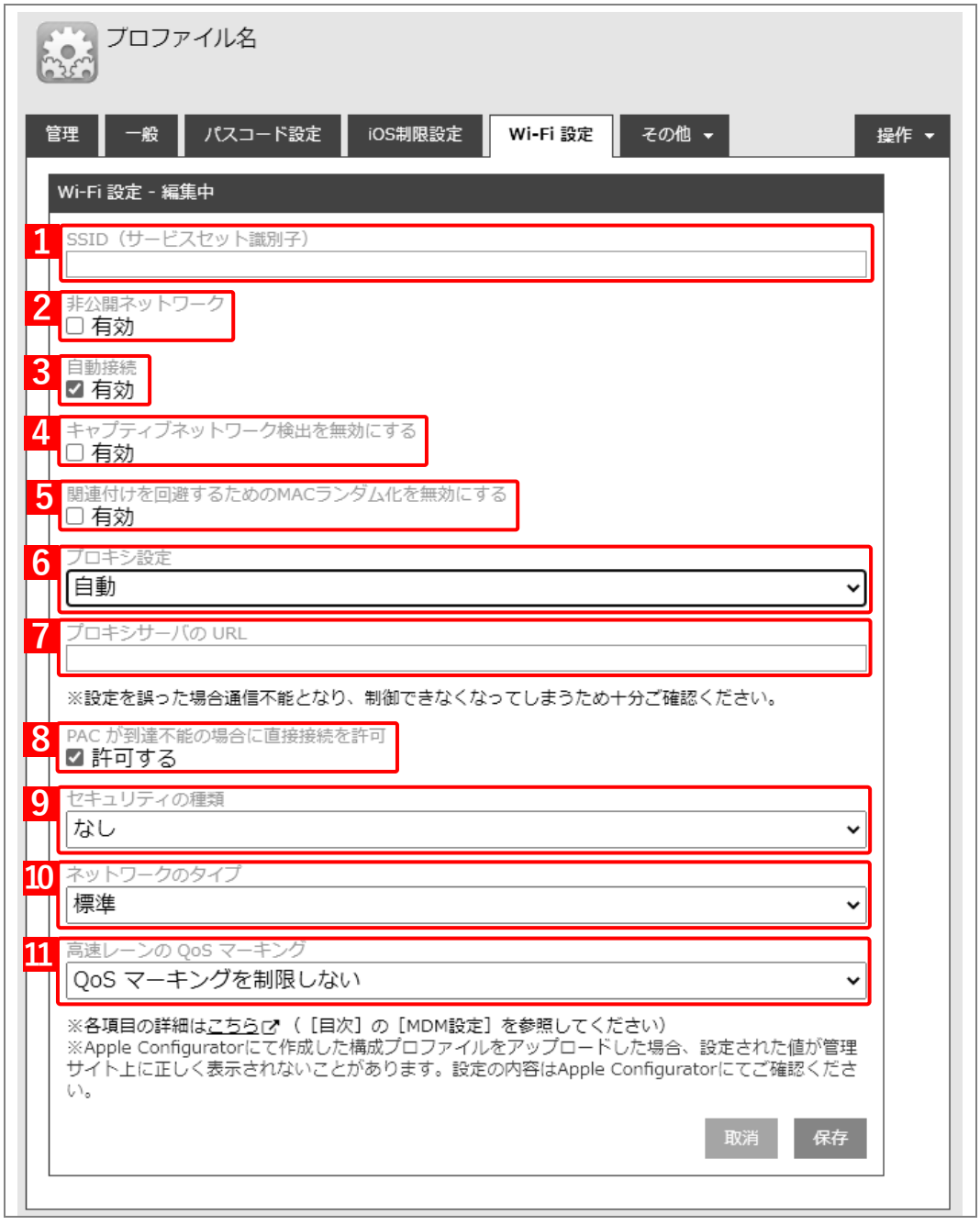
項番	項目	説明
1	SSID(サービスセット識別子)	利用する Wi-Fi ネットワークの SSID の名称を入力してください。
2	非公開ネットワーク	●有効 非公開ネットワークを端末に表示する場合は、「有効」にチェックを入れます。
3	自動接続	●有効 自動接続を行う場合は、「有効」にチェックを入れます。 端末の Wi-Fi 設定をオフにしている場合は、自動接続されません。オンにしている場合、項番 1 で設定した SSID に自動接続されます。

項番	項目	説明
4	キャプティブネットワーク検出を無効にする	●有効 キャプティブネットワークの検出を無効にする場合は、「有効」にチェックを入れます。
5	関連付けを回避するためのMAC ランダム化を無効にする	●有効 iOS 14.0 以上の端末で、MAC アドレスのランダム化を無効にする場合は、「有効」にチェックを入れます。 iOS 14.0 以上の端末の［設定］→［Wi-Fi］→［プライベートアドレス］が無効になります。デフォルト値は有効になっています。 iOS 14.0～14.1 の端末の場合は、本設定を無効にしても、端末から手動で有効に変更できます。 iOS 14.0 未満の端末に配信したあとで、iOS 14.0 以上にアップデートしても無効になりません。
6	プロキシ設定	「手動」を選択します。
7	サーバおよびポート	●サーバ 入力必須です。アドレスを半角英数字で入力します。 ●ポート 入力必須です。使用できる文字は、半角数字です。
8	ユーザ名	プロキシサーバーの認証に用いるユーザー名を入力します。
9	パスワード	プロキシサーバーの認証に用いるパスワードを入力します。 ●変更する パスワードを変更する場合にチェックを入れます。
10	セキュリティの種類	Wi-Fi のセキュリティを設定します。以下の項目から選択します。 ●「なし」、「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」、「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」、「任意（エンタープライズ）」 「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」を選択した場合は、「パスワード」が表示されますので、入力してください。 「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」を選択した場合は、エンタープライズ設定の項目が表示されます。 ☞「画面（エンタープライズ設定（プロトコル））」420 ページ ☞「画面（エンタープライズ設定（信頼））」422 ページ
11	ネットワークのタイプ	ネットワークのタイプを以下の項目から選択します。 ●標準 標準ネットワークの場合に選択します。 ●レガシーホットスポット レガシーホットスポットの場合に選択します。 ●Passpoint Passpoint の場合に選択します。選択すると設定項目が表示されます。設定項目については、以下を参照してください。 ☞「画面（ネットワークのタイプ：Passpoint）」419 ページ

項番	項目	説明
12	高速レーンの QoS マーキング	QoS マーキングを制限するかどうかを以下の項目から選択します。 ●QoS マーキングを制限しない QoS マーキングを制限しません。 ●QoS マーキングを制限する 選択すると、制限についての設定項目が表示されます。設定項目については、以下を参照してください。 ☞「画面（高速レーンの QoS マーキング：QoS マーキングを制限する）」422 ページ

◆画面（プロキシ設定：自動）

表示操作［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］

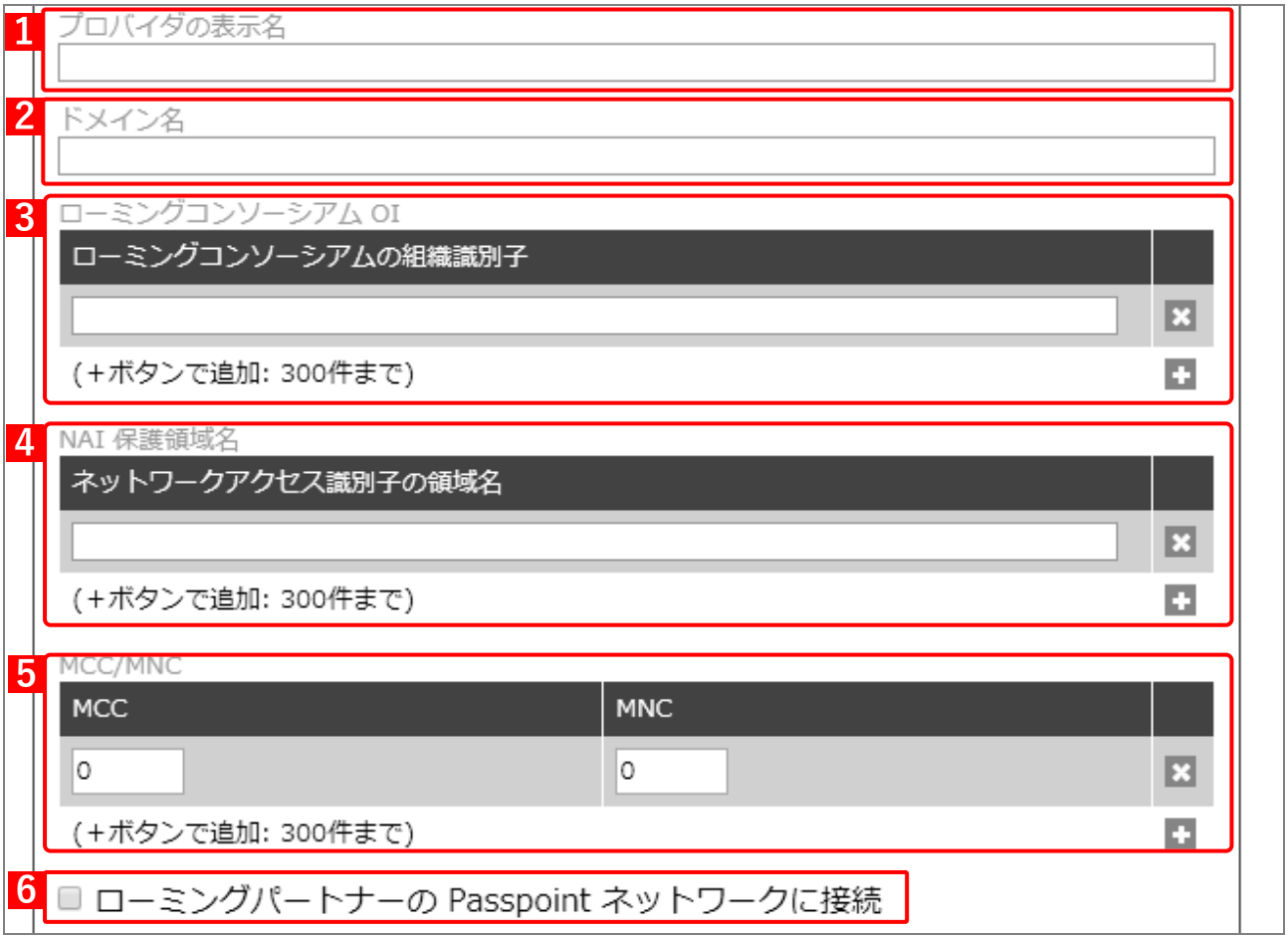


項番	項目	説明
1	SSID(サービスセット識別子)	利用する Wi-Fi ネットワークの SSID の名称を入力してください。
2	非公開ネットワーク	●有効 非公開ネットワークを端末に表示する場合は、「有効」にチェックを入れます。
3	自動接続	●有効 自動接続を行う場合は、「有効」にチェックを入れます。 端末の Wi-Fi 設定をオフにしている場合は、自動接続されません。オンにしている場合、項番 1 で設定した SSID に自動接続されます。
4	キャプティブネットワーク検出を無効にする	●有効 キャプティブネットワークの検出を無効にする場合は、「有効」にチェックを入れます。
5	関連付けを回避するための MAC ランダム化を無効にする	●有効 iOS 14.0 以上の端末で、MAC アドレスのランダム化を無効にする場合は、「有効」にチェックを入れます。 iOS 14.0 以上の端末の［設定］→［Wi-Fi］→［プライベートアドレス］が無効になります。デフォルト値は有効になっています。 iOS14.0～14.1 の端末の場合は、本設定を無効にしても、端末から手動で有効に変更できます。 iOS 14.0 未満の端末に配信したあとで、iOS 14.0 以上にアップデートしても無効になりません。
6	プロキシ設定	「自動」を選択します。
7	プロキシサーバの URL	プロキシ設定が「自動」な場合、入力必須です。プロキシ設定を定義している PAC ファイルの URL です。 設定を誤った場合通信不能となり、制御できなくなりますので十分ご確認ください。
8	PAC が到達不能の場合に直接接続を許可	●許可する チェックボックスのチェックを外すと、PAC ファイルに到達できない場合、デバイスはデスティネーションに直接接続できません。
9	セキュリティの種類	Wi-Fi のセキュリティを設定します。以下の項目から選択します。 ●「なし」、「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」、「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」、「任意（エンタープライズ）」 「WEP」、「WPA／WPA2 パーソナル」、「WPA2 パーソナル（Apple TV を除く iOS 8 以上）」、「WPA3 パーソナル（iOS 13 以上）」、「任意（パーソナル）」を選択した場合は、「パスワード」が表示されますので、入力してください。 「ダイナミック WEP」、「WPA／WPA2 エンタープライズ」、「WPA2 エンタープライズ（Apple TV を除く iOS 8 以上）」、「WPA3 エンタープライズ（iOS 13 以上）」を選択した場合は、エンタープライズ設定の項目が表示されます。 「画面（エンタープライズ設定（プロトコル））」420 ページ 「画面（エンタープライズ設定（信頼））」422 ページ

項番	項目	説明
10	ネットワークのタイプ	ネットワークのタイプを以下の項目から選択します。 ●標準 標準ネットワークの場合に選択します。 ●レガシーホットスポット レガシーホットスポットの場合に選択します。 ●Passpoint Passpoint の場合に選択します。選択すると設定項目が表示されます。設定項目については、以下を参照してください。 ☞「画面（ネットワークのタイプ：Passpoint）」419 ページ
11	高速レーンの QoS マーキング	QoS マーキングを制限するかどうかを以下の項目から選択します。 ●QoS マーキングを制限しない QoS マーキングを制限しません。 ●QoS マーキングを制限する 選択すると、制限についての設定項目が表示されます。設定項目については、以下を参照してください。 ☞「画面（高速レーンの QoS マーキング：QoS マーキングを制限する）」422 ページ

◆画面（ネットワークのタイプ：Passpoint）

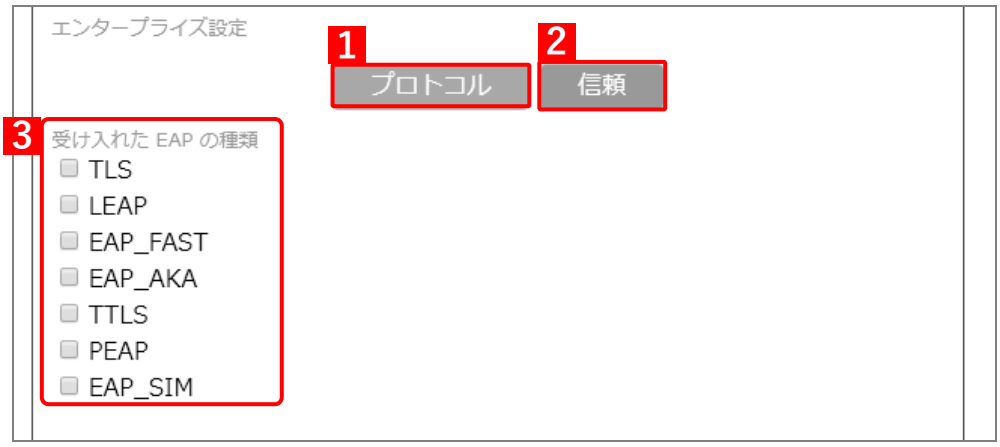
表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］



項番	項目	説明
1	プロバイダの表示名	プロバイダの表示名を入力します。
2	ドメイン名	ドメイン名を入力します。
3	ローミングコンソーシアム OI	ローミングコンソーシアムの組織識別子を登録します。＋ をクリックして 300 件まで登録できます。
4	NAI 保護領域名	ネットワークアクセス識別子の領域名を登録します。＋ をクリックして 300 件まで登録できます。
5	MCC/MNC	MCC を MNC と登録します。＋ をクリックして 300 件まで登録できます。
6	ローミングパートナーの Passpoint ネットワークに接続	チェックを入れると、ローミングパートナーの Passpoint ネットワークに接続できます。

◆画面（エンタープライズ設定（プロトコル））

表示操作［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］



項番	項目	説明
1	［プロトコル］	「画面（エンタープライズ設定（プロトコル））」を設定する場合に、クリックします。
2	［信頼］	「画面（エンタープライズ設定（信頼））」を設定する場合に、クリックします。
3	受け入れた EAP の種類	受け入れた EAP の種類にチェックを入れます。チェックを入れると種類対応した設定項目が表示されます。 固有名証明書のリストボックスに、表示される証明書の上限は 100 件です。［証明書ペイロードに証明書を追加］、［(機器に設定されているクライアント証明書)］、［登録済のクライアント証明書］から選択します。 ●TLS チェックを入れると、以下の項目が設定できるようになります。 ・固有名証明書 ・TLS の最小バージョン ・TLS の最大バージョン ●LEAP チェックを入れると、以下の項目が設定できるようになります。 ・ユーザ名 ・接続ごとにパスワードを使用 ・パスワード ●EAP_FAST チェックを入れると、以下の項目が設定できるようになります。 ・EAP-FAST

項番	項目	説明
		以下のチェック項目が表示されます。 ・PAC を使用 ・PAC をプロビジョニング 「PAC を使用」にチェックを入れると、チェックできるようになります。 ・PAC を匿名でプロビジョニング 「PAC を使用」にチェックを入れると、チェックできるようになります。 ・ユーザ名 ・接続ごとにパスワードを使用 ・パスワード ・固有名証明書 ・外部 ID ・TLS の最小バージョン ・TLS の最大バージョン ●EAP_AKA ●TTLS チェックを入れると、以下の項目が設定できるようになります。 ・ユーザ名 ・接続ごとにパスワードを使用 ・パスワード ・固有名証明書 ・内部認証 ・外部 ID ・TLS の最小バージョン ・TLS の最大バージョン ●PEAP チェックを入れると、以下の項目が設定できるようになります。 ・ユーザ名 ・接続ごとにパスワードを使用 ・パスワード ・固有名証明書 ・外部 ID ・TLS の最小バージョン ・TLS の最大バージョン ●EAP_SIM チェックを入れると、以下の項目が設定できるようになります。 ・EAP-T 以下のチェック項目が表示されます。 ・2 つの RAND を許可

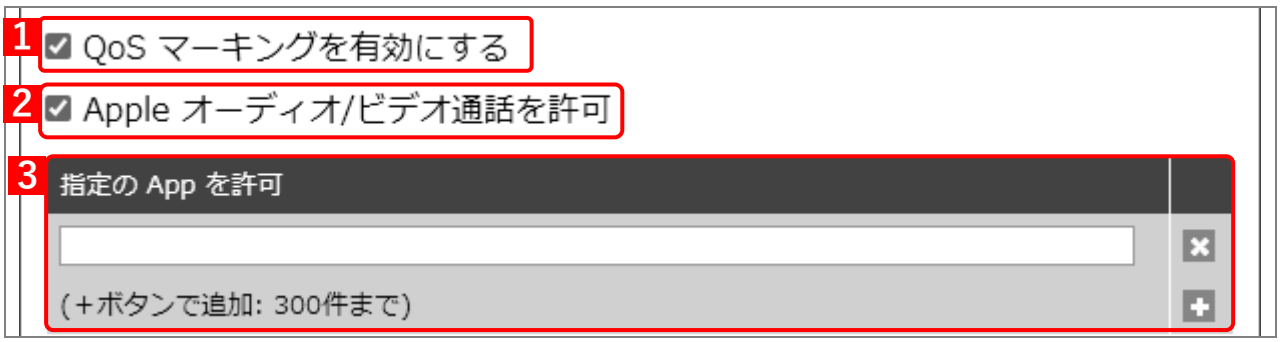
◆画面（エンタープライズ設定（信頼））

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］**

項番	項目	説明
1	［プロトコル］	「画面（エンタープライズ設定（プロトコル））」を設定する場合に、クリックします。
2	［信頼］	「画面（エンタープライズ設定（信頼））」を設定する場合に、クリックします。
3	信頼できる証明書	登録されている CA 証明書が表示されます。対象の CA 証明書にチェックを入れます。
4	信頼できるサーバ証明書の名前	サーバーの TLS 証明書の名前を登録します。＋ をクリックして 300 件まで登録できます。

◆画面（高速レーンの QoS マーキング：QoS マーキングを制限する）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［Wi-Fi 設定］タブ→［新規作成］または［編集］**



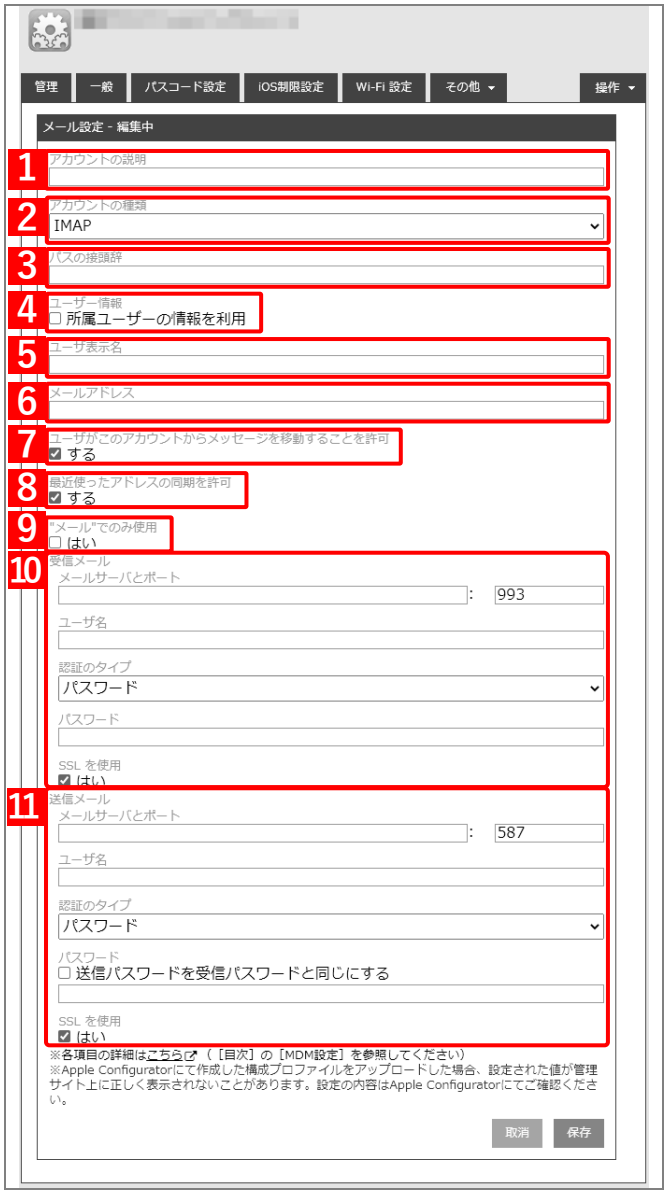
項番	項目	説明
1	QoS マーキングを有効にする	チェックを入れると QoS マーキングが有効になります。
2	Apple オーディオ/ビデオ通話を許可	チェックを入れると Apple オーディオおよびビデオ通話を許可します。
3	指定の App を許可	＋ をクリックして、許可するアプリのアプリケーション ID を 255 文字以内の半角英数字、ピリオド「.」、ハイフン「-」で入力します。 同じアプリケーション ID は、重複して登録できません。 空白で保存はできません。

8.3.1.6 ［その他▼］タブ／メール設定

メールに関する各種の設定を行います。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［メール設定］→［新規作成］または［編集］



項番	項目	説明
1	アカウントの説明	電子メールアカウントの説明を指定します。これが「Mail and Settings」アプリに表示されます。
2	アカウントの種類	このアカウントが用いるプロトコルを定義します。以下から選択します。 ●「IMAP」、「POP」
3	パスの接頭辞	パスの接頭辞を入力してください。
4	ユーザー情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用するか選択します。利用する場合は、チェックを入れます。
5	ユーザ表示名	アカウントのユーザー名称を入力してください。送信メッセージなどに埋め込まれます。

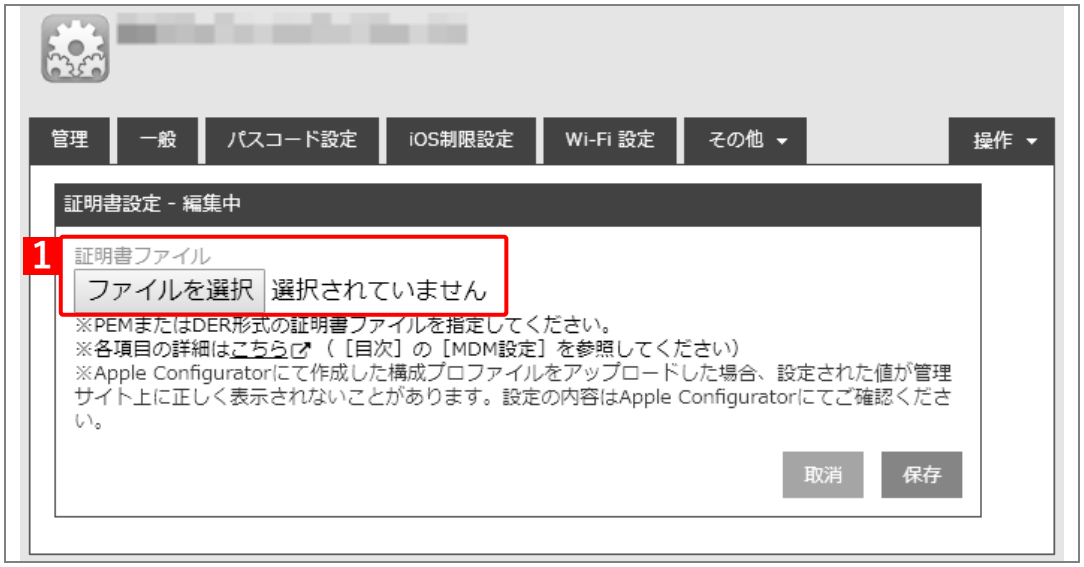
項番	項目	説明
6	メールアドレス	ユーザーのメールアドレスを入力してください。
7	ユーザがこのアカウントからメッセージを移動することを許可	●する チェックボックスのチェックを外すと、メールアカウント間でメールメッセージを移動できなくなります。
8	最近使ったアドレスの同期を許可	●する チェックボックスのチェックを外すと、最近使ったアドレスがデバイス間で同期されなくなります。
9	"メール"でのみ使用	●はい チェックボックスにチェックを入れると、このアカウントから他社製アプリでメールを送信できません。
10	受信メール	●メールサーバとポート ・メールサーバ 受信メールサーバーのホスト名（または IP アドレス）を入力してください。 ・ポート 受信メールサーバーのポート番号を半角数字で入力してください。 ●ユーザ名 電子メールアカウントのユーザー名称を入力してください。 ●認証のタイプ 受信メールの認証スキームを表します。以下から選択します。 ・「なし」、「パスワード」、「MD5 チャレンジ応答」、「NTLM」、「HTTP MD5 ダイジェスト」 ●パスワード 受信メールサーバーのパスワードを入力してください。 ●SSL を使用 ・はい 受信メールサーバーが認証用に SSL を利用するか否かを指定します。
11	送信メール	●メールサーバとポート ・メールサーバ 受信メールサーバーのホスト名（または IP アドレス）を入力してください。 ●ポート 受信メールサーバーのポート番号を半角数字で入力してください。 ●ユーザ名 電子メールアカウントのユーザー名称を入力してください。 ●送信メールの認証スキームを指定します。以下から選択します。 ・「なし」、「パスワード」、「MD5 チャレンジ応答」、「NTLM」、「HTTP MD5 ダイジェスト」 ●パスワード 送信メールサーバーのパスワードを入力してください。 ●送信パスワードを受信パスワードと同じにする 送信パスワードを受信パスワードと同じにするか選択します。 ●SSL を使用 ・はい 送信メールサーバーが認証用に SSL を利用するか否かを指定します。

8.3.1.7 ［その他▼］タブ／証明書設定

CA 証明書をアップロードします。

◆画面

表示操作 **［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［証明書設定］→［新規作成］または［編集］**



項番	項目	説明
1	証明書ファイル	アップロードする CA 証明書を指定します。［ファイルを選択］をクリックして、アップロードする CA 証明書を選択してください。なお、アップロードには PEM または DER 形式で、エンコードされた CA 証明書を指定してください。

8.3.1.8 ［その他▼］タブ／グローバル HTTP プロキシ設定

グローバル HTTP プロキシに関する各種の設定を行います。

プロキシタイプによって設定内容が異なります。

画面（プロキシタイプ：手動）

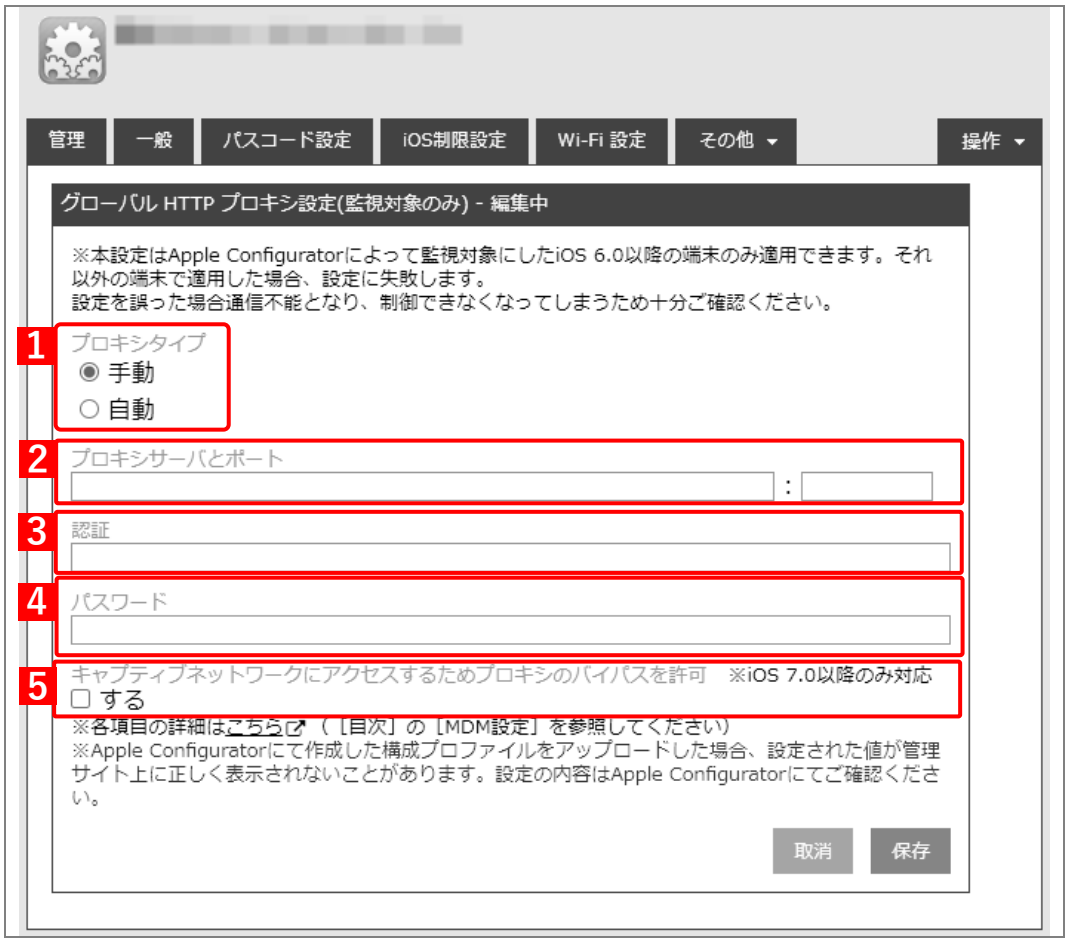
画面（プロキシタイプ：自動）

認証が必要なプロキシでは、プロキシタイプで［手動］を選択します。

iOS 6.0 以上の監視対象端末で設定できます。iOS 6.0 未満の端末の場合は通信不能となり、制御できなくなります。使用している端末を十分に確認してください。

◆画面（プロキシタイプ：手動）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［グローバル HTTP プロキシ設定］→［新規作成］または［編集］**

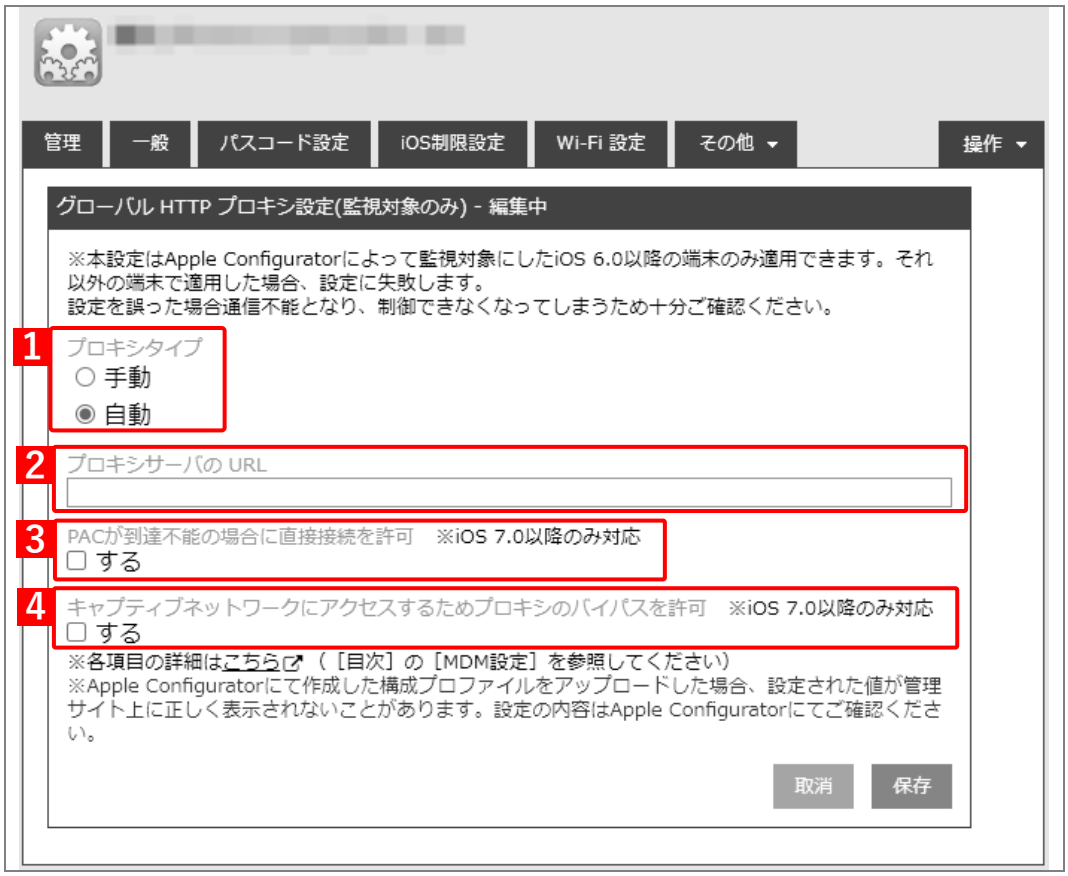


項番	項目	説明
1	プロキシタイプ	「手動」をクリックします。
2	プロキシサーバとポート	入力必須です。プロキシサーバーは半角英数字と記号で入力します。ポートは 0 以上 65,535 以下を半角数字で入力してください。 監視対象端末の場合のみ適用されます。
3	認証	「プロキシタイプ」が「手動」の場合にのみ、1 文字から 255 文字の半角英数字と記号で入力してください。 監視対象端末の場合のみ適用されます。

項番	項目	説明
4	パスワード	「プロキシタイプ」が「手動」の場合にのみ、1 文字から 255 文字の半角英数字と記号で入力してください。 監視対象端末の場合のみ適用されます。
5	キャプティブネットワークにアクセスするためプロキシのバイパスを許可	「する」にチェックを入れると、iOS デバイスは既知のワイヤレスネットワークにアクセスするためにプロキシ設定を無視できます。 監視対象端末の場合のみ適用されます。 iOS 7.0 以上のみ対応しています。

◆画面（プロキシタイプ：自動）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［グローバル HTTP プロキシ設定］→［新規作成］または［編集］



項番	項目	説明
1	プロキシタイプ	「自動」をクリックします。
2	プロキシサーバの URL	「プロキシタイプ」が「自動」の場合にのみ、1 文字から 255 文字の半角英数字と記号で入力してください。
3	PAC が到達不能の場合に直接接続を許可	「プロキシタイプ」が「自動」の場合にのみ、「する」のチェックを外すと、PAC ファイルに到達できない場合、デバイスはデスティネーションに直接接続できません。 iOS 7.0 以上のみ対応しています。
4	キャプティブネットワークにアクセスするためプロキシのバイパスを許可	「する」にチェックを入れると、iOS デバイスは既知のワイヤレスネットワークにアクセスするためにプロキシ設定を無視できます。 監視対象端末の場合のみ適用されます。

8.3.1.9 ［その他▼］タブ／DNS プロキシ設定

DNS プロキシに関する各種の設定を行います。

誤った設定値を入力すると、本設定が端末に反映されず、構成プロファイルのインストールに失敗する場合があります。設定値は DNS プロバイダまたはネットワークベンダーに確認してください。

iOS 14 以下の場合、監視対象のみ有効です。

◆画面

表示操作［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［DNS プロキシ設定］→［新規作成］または［編集］

項番	項目	説明
1	アプリケーション ID (Bundle Identifier)	DNS プロキシとして使用するアプリのバンドル ID を 255 文字以内で入力します。使用できる文字は、半角英数字と記号（「.」、「-」）です。入力必須です。 アプリケーション ID の確認方法は、以下を参照してください。 「アプリケーション ID の調べかた」544 ページ
2	プロバイダバンドル ID	使用する DNS プロキシネットワーク拡張のバンドル ID を 255 文字以内で入力します。使用できる文字は、半角英数字と記号（「.」、「-」）です。

項番	項目	説明
3	プロバイダ構成	ベンダー固有の設定項目がある場合、ベンダーから提供された plist ファイルをアップロードします。 本項目を編集することはできません。(A)［構成を削除］をクリックすると、アップロードした plist ファイルと入力内容が削除されます。 最大 100KB までの plist ファイルがアップロードできます。

8.3.1.10 ［その他▼］タブ／コンテンツフィルタ設定

コンテンツフィルタに関する各種の設定を行います。

画面（フィルタ・タイプ：アダルトコンテンツを制限）
画面（フィルタ・タイプ：指定した Web サイトのみ）
画面（フィルタ・タイプ：プラグイン（他社製 App））

◆画面（フィルタ・タイプ：アダルトコンテンツを制限）

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［コンテンツフィルタ設定］→［新規作成］または［編集］

項番	項目	説明
1	フィルタ・タイプ	「アダルトコンテンツを制限」をクリックします。
2	許可された URL	入力必須です。URL を追加すると、その Web サイトが自動フィルターによってアダルトとみなされた場合でもアクセスが許可されます。このリストを空のままにすると、「許可されていない URL」にリストされているものを除いて、すべての非アダルト Web サイトへのアクセスが許可されます。 監視対象端末の場合のみ適用されます。 ●URL 1 文字から 255 文字で入力します。 「http://」または「https://」で始めてください。 1,000 件以下にしてください。 重複しない URL を入力してください。 フィルタリングされる URL は、ドメイン名の最初の www を無視したサブドメインも対象となります。

項番	項目	説明
3	許可されていない URL	入力必須です。特定の Web サイトへのアクセスを拒否するには、サイトの URL をこのリストに追加します。ユーザーはこれらのサイトにアクセスできません（自動フィルターによって非アダルトとみなされた場合でも）。 監視対象端末の場合のみ適用されます。 ●URL 1 文字から 255 文字で入力します。 「http://」または「https://」で始めてください。 500 件以下にしてください。 重複しない URL を入力してください。 フィルタリングされる URL は、ドメイン名の最初の www を無視したサブドメインも対象となります。

◆画面（フィルタ・タイプ：指定した Web サイトのみ）

表示操作［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［コンテンツフィルタ設定］→［新規作成］または［編集］

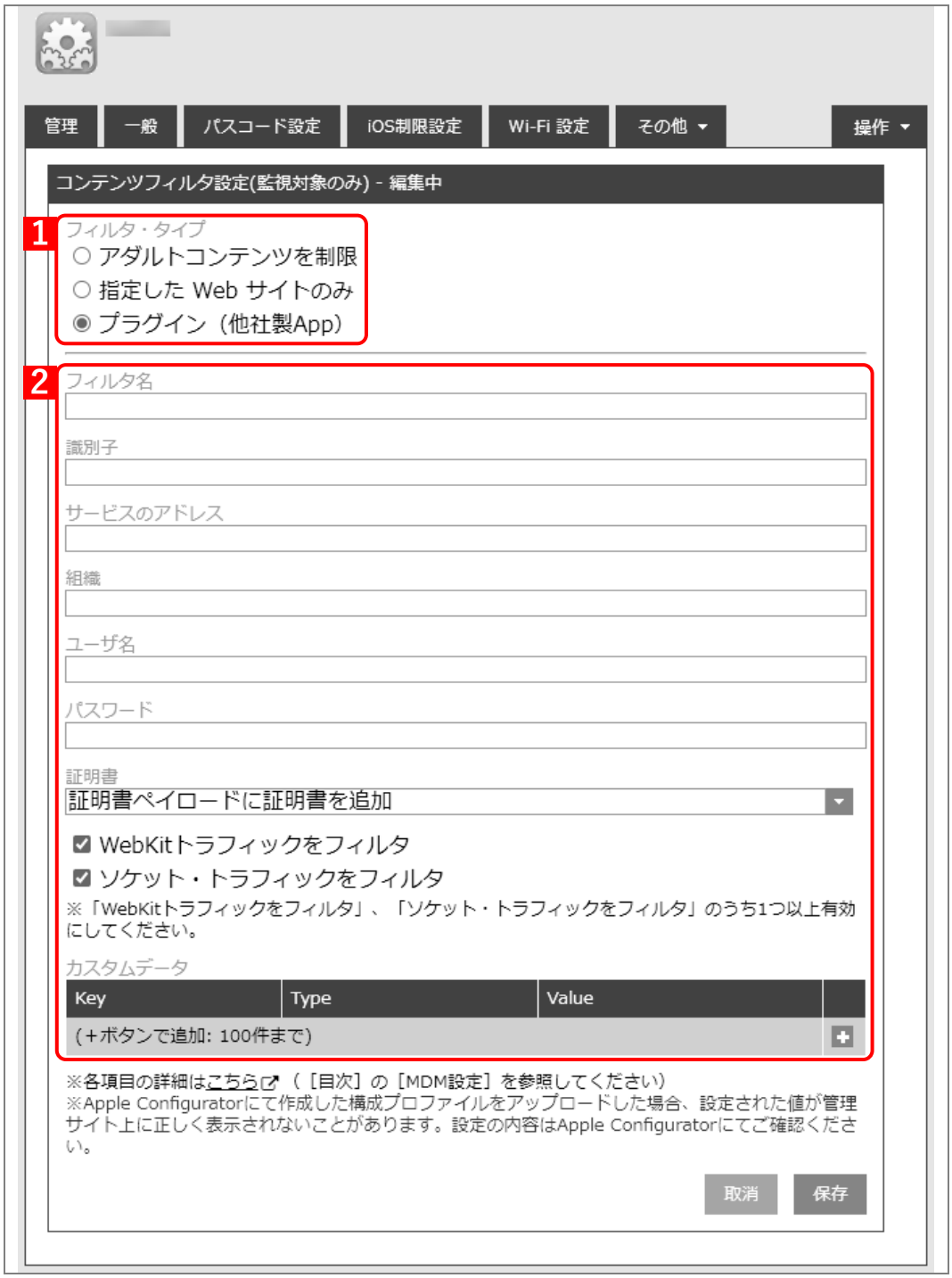
項番	項目	説明
1	フィルタ・タイプ	「指定した Web サイトのみ」をクリックします。
2	指定した Web サイト	アクセスを許可したい Web サイトを追加します。 ●URL Web サイトの URL を 1 文字から 255 文字で入力してください。「http://」または「https://」で始めてください。 ●名前 名前を 1 文字から 30 文字で入力してください。 監視対象端末の場合のみ適用されます。 「https://www.apple.com/」と「apple.com」を含んだ Web サイトは、本項目に追加しなくてもアクセスできることがあります。 フィルタリングされる URL は、ドメイン名の最初の www を無視したサブドメインも対象となります。

◆画面（フィルタ・タイプ：プラグイン（他社製 App））

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［コンテンツフィルタ設定］→［新規作成］または［編集］**

設定したい他社製アプリのサービス提供元に、設定値を確認してください。

Apple Configurator 2 で設定が可能な「カスタムデータ」の項目を利用したい場合は、Apple Configurator 2 で作成した構成プロファイルをアップロードしてください。



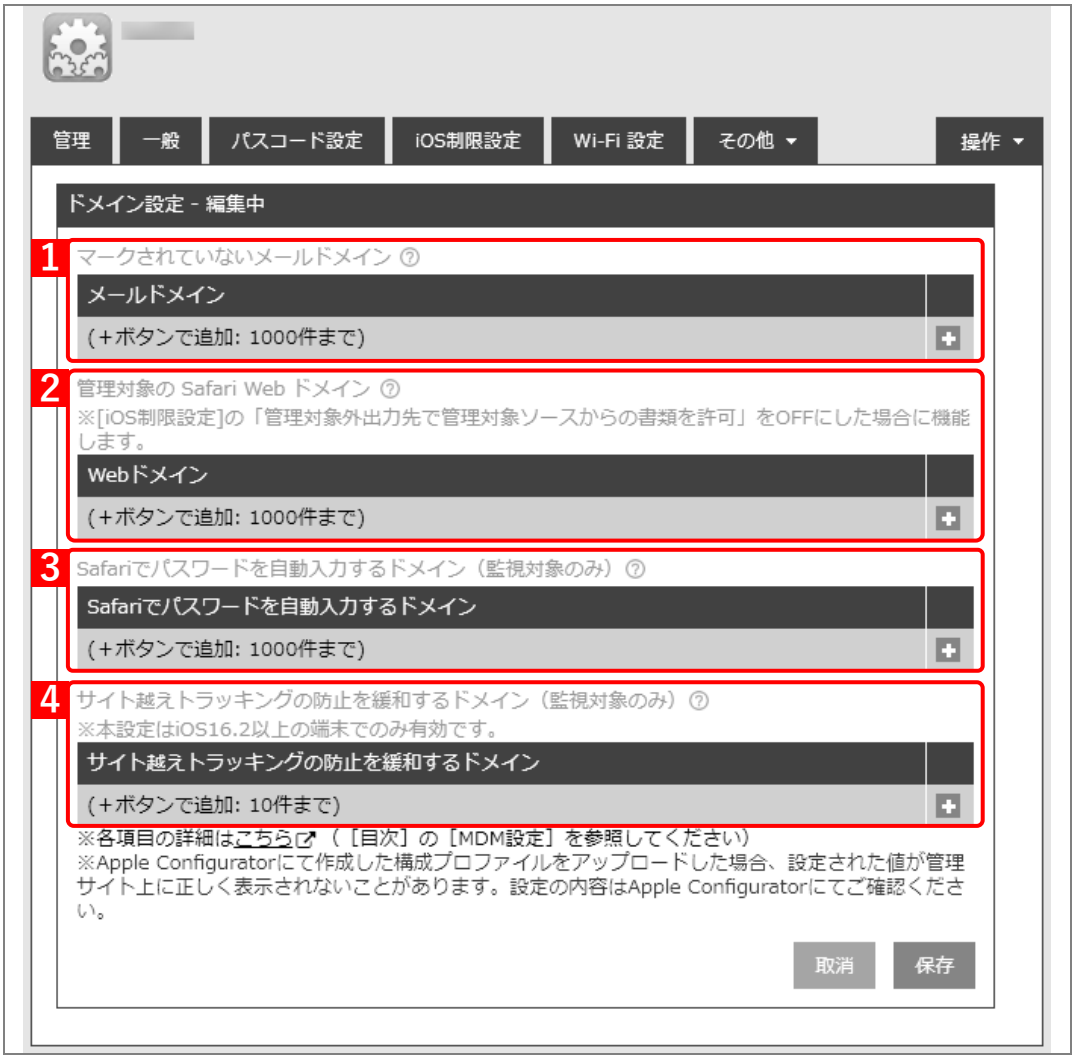
項番	項目	説明
1	フィルタ・タイプ	「プラグイン（他社製 App)」をクリックします。
2	設定値	以下の設定値を入力または選択します。 他社製アプリのサービス提供元に確認した内容を設定してください。 ●フィルタ名 ●識別子 フィルタ名、識別子は入力必須です。 ●サービスのアドレス ●組織 ●ユーザ名 ●パスワード ●証明書 ・証明書ペイロードに証明書を追加 ・(機器に設定されているクライアント証明書) Apple Configurator 2 で作成した構成プロファイルをアップロードした場合は、「証明書ペイロードに証明書を追加」を選択してアップロードすると、管理サイト画面の証明書に「(なし)」と表示されますが、証明書が削除されているわけではありません。 ●WebKit トラフィックをフィルタ ●ソケット・トラフィックをフィルタ 「WebKit トラフィックをフィルタ」「ソケット・トラフィックをフィルタ」は、デフォルトで 2 つとも有効になっています。必ず 1 つ以上有効にしてください。 ●カスタムデータ 以下の項目を任意の値で設定することができます。 ・Key Key を入力します。 ・Type Type を「String」、「Integer」、「Boolean」から選択します。 ・Value 「Type」で選択した Type に応じて、Value または変数を入力します。 「Type」で「Boolean」を選択した場合は、「false」または「true」を選択します。

8.3.1.11 ［その他▼］タブ／ドメイン設定

ドメインに関する各種の設定を行います。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［ドメイン設定］→［新規作成］または［編集］



項番	項目	説明
1	マークされていないメールドメイン	これらのドメインと一致しないメールアドレスは"メール"でマークされます。リストとして追加してください。1 つの設定セットにつき、1000 件まで登録できます。
2	管理対象の Safari Web ドメイン	［制限］タブの「管理対象外出力先で管理対象ソースからの書類を許可」が有効な場合に、管理対象となる Web コンテンツの URL を指定します。1 つの設定セットにつき、1000 件まで登録できます。 管理対象のコンテンツは、Safari からのアクセス時に外部アプリの起動を制限されます。詳細については、以下を参照してください。 ☞「画面（機能の制限）」400 ページ
3	Safari でパスワードを自動入力するドメイン（監視対象のみ）	パスワードの自動入力が有効な場合、パスワードを保存できる URL を指定します。1 つの設定セットにつき、1000 件まで登録できます。

項番	項目	説明
4	サイト越えトラッキングの防止を緩和するドメイン（監視対象のみ）	サイト越えトラッキングを防止する機能が有効な場合、サイト越えトラッキングができる URL を指定します。1 つの設定セットにつき、10 件まで登録できます。 iOS 16.2 以上で設定できます。

8.3.1.12 ［その他▼］タブ／VPN 設定

VPN に関する各種の設定を行います。

画面（接続タイプ：IKEv2）
画面（接続タイプ：IPSec）
画面（接続タイプ：L2TP）
画面（接続タイプ：PPTP（iOS 10 未満と OS X 10.12 未満））
画面（接続タイプ：Cisco AnyConnect）
画面（接続タイプ：Cisco Legacy AnyConnect（iOS12 未満））
画面（接続タイプ：Juniper SSL）
画面（接続タイプ：Pulse Secure）
画面（接続タイプ：F5 SSL）
画面（接続タイプ：SonicWALL Mobile Connect）
画面（接続タイプ：Aruba VIA）
画面（接続タイプ：Check Point Mobile VPN）
画面（接続タイプ：カスタム SSL）
画面（プロキシ設定：手動）
画面（プロキシ設定：自動）

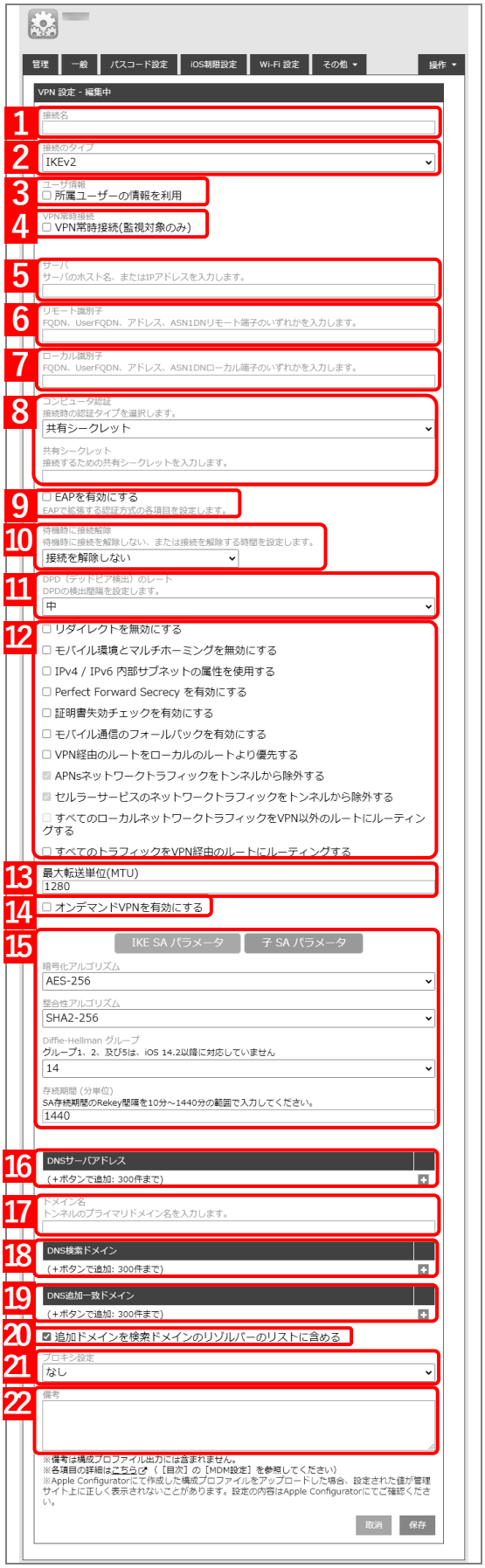
接続タイプの入力項目については、以下を参照してください。

「（設定－iOS）VPN 設定」94 ページ

本説明では、［新規作成］で開いたときに表示される項目の画像を例に使用しています。設定により表示される項目が異なります。

◆画面（接続タイプ：IKEv2）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力します。
2	接続のタイプ	「IKEv2」を選択します。
3	ユーザ情報	●［所属ユーザーの情報を利用］ 所属ユーザーの情報を利用する場合、チェックを入れます。
4	VPN 常時接続	VPN を常時接続する場合、設定します。
	［VPN 常時接続（監視対象のみ）］	VPN を常時接続する場合、チェックを入れます。 チェックを入れると、以下の項目が設定できます。 ●［モバイル通信］ モバイル通信でトンネル構成を設定する場合、選択します。以下の項目が設定できます。 ・サーバ ・リモート識別子 ・ローカル識別子 ・コンピュータ認証 ・EAP を有効にする ・デバイスのスリープ中も NAT KeepAlive を有効にする ・NAT KeepAlive の間隔（秒単位） ・DPD（デッドピア検出）のレート ・リダイレクトを無効にする ・モバイル環境とマルチホーミングを無効にする ・IPv4 / IPv6 内部サブネットの属性を使用する ・Perfect Forward Secrecy を有効にする ・証明書失効チェックを有効にする ・モバイル通信のフォールバックを有効にする ・VPN 経由のルートをローカルのルートより優先する ・APNs ネットワークトラフィックをトンネルから除外する ・セルラーサービスのネットワークトラフィックをトンネルから除外する ・すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする ・すべてのトラフィックを VPN 経由のルートにルーティングする ●［Wi-Fi 接続］ Wi-Fi 接続でトンネル構成を設定する場合選択します。以下の項目が設定できます。 ・サーバ ・リモート識別子 ・ローカル識別子 ・コンピュータ認証 ・EAP を有効にする ・デバイスのスリープ中も NAT KeepAlive を有効にする ・NAT KeepAlive の間隔（秒単位） ・DPD（デッドピア検出）のレート ・リダイレクトを無効にする ・モバイル環境とマルチホーミングを無効にする ・IPv4 / IPv6 内部サブネットの属性を使用する ・Perfect Forward Secrecy を有効にする ・証明書失効チェックを有効にする ・モバイル通信のフォールバックを有効にする

項番	項目		説明
			・VPN 経由のルートをローカルのルートより優先する ・APNs ネットワークトラフィックをトンネルから除外する ・セルラーサービスのネットワークトラフィックをトンネルから除外する ・すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする ・すべてのトラフィックを VPN 経由のルートにルーティングする ●デバイスのスリープ中も NAT KeepAlive を有効にする デバイスのスリープ中も NAT KeepAlive を有効にする場合は、チェックを入れます。 ●NAT KeepAlive の間隔（秒単位） NAT KeepAlive の間隔を 20 秒～1440 秒の範囲で入力します。 ●サービスの例外 以下の項目を設定します。［トンネル経由のトラフィックを許可］、［トンネル外からのトラフィックを許可］、［トラフィックを禁止］から選択します。 ・ボイスメール ・AirPrint ・モバイル通信サービス ●［VPN トンネル外からのキャプティブ Web シートのトラフィックを許可］ VPN トンネル外からのキャプティブ Web シートのトラフィックを許可する場合は、チェックを入れます。 ●［VPN トンネル外からのすべてのキャプティブネットワーク App のトラフィックを許可］ VPN トンネル外からのすべてのキャプティブネットワーク App のトラフィックを許可する場合は、チェックを入れます。 ●キャプティブネットワーク App のバンドル ID キャプティブネットワーク App のバンドル ID を 255 文字以内の半角英数字と記号で入力します。 ［VPN トンネル外からのすべてのキャプティブネットワーク App のトラフィックを許可］にチェックが入っていない場合、表示されます。 ●例外的に通信を許可するアプリケーション 例外的に通信を許可したいアプリがある場合、以下を設定します。 ・バンドル ID 例外的に通信を許可するアプリケーションのバンドル ID を 255 文字以内の半角英数字と記号で入力します。 ・通信を許可するプロトコル 通信を許可するプロトコルが「UDP」の場合、チェックを入れます。
		［ユーザーによる自動接続を無効化］	ユーザーによる VPN の自動接続を無効化する場合、チェックを入れます。 本項目は［VPN 常時接続（監視対象のみ）］にチェックを入れると、表示されます。
		［モバイルデータ通信と Wi-Fi 接続に同じトンネル構成を使用］	モバイル通信と Wi-Fi 接続で同じトンネル構成を設定する場合、チェックを入れます。 以下の項目が設定できます。 ●サーバ ●リモート識別子 ●ローカル識別子 ●コンピュータ認証 ●EAP を有効にする ●デバイスのスリープ中も NAT KeepAlive を有効にする ●NAT KeepAlive の間隔（秒単位） ●DPD（デッドピア検出）のレート

項番	項目	説明
		●リダイレクトを無効にする ●モバイル環境とマルチホーミングを無効にする ●IPv4 / IPv6 内部サブネットの属性を使用する ●Perfect Forward Secrecy を有効にする ●証明書失効チェックを有効にする ●モバイル通信のフォールバックを有効にする ●VPN 経由のルートをローカルのルートより優先する ●APNs ネットワークトラフィックをトンネルから除外する ●セルラーサービスのネットワークトラフィックをトンネルから除外する ●すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする ●すべてのトラフィックを VPN 経由のルートにルーティングする 本項目は［VPN 常時接続（監視対象のみ）］にチェックを入れると、表示されます。
5	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力します。
6	リモート識別子	FQDN、UserFQDN、アドレス、ASN1DN リモート端子のいずれかを入力します。
7	ローカル識別子	FQDN、UserFQDN、アドレス、ASN1DN リモート端子のいずれかを入力します。
8	コンピュータ認証	接続時の認証タイプを以下の項目から選択します。 ●［なし］ ●［証明書］ 以下の項目が表示されます。 ・固有名証明書 設定する証明書を選択します。 ・証明書のタイプ 発行された証明書の種類を選択します。 ・サーバ証明書発行者のコモンネーム サーバー証明書発行者のコモンネームを 255 文字以内の半角英数字と記号で入力します。 ・サーバ証明書のコモンネーム サーバー証明書のコモンネームを 255 文字以内の半角英数字と記号で入力します。 ●［共有シークレット］ 接続するための共有シークレットの入力欄が表示されます。255 文字以内の半角英数字と記号で入力します。
9	［EAP を有効にする］	EAP で拡張する認証方式を設定する場合は、チェックを入れます。 チェックを入れると、「EPA 認証」が表示されます。 チェックを入れない場合は、項番 8「コンピュータ認証」で［証明書］または［共有シークレット］を選択してください。
	EAP 認証	接続時の認証タイプを以下のいずれかを選択します。 ●［ユーザー名／パスワード］ 選択すると、以下が表示されます。 ・アカウント 接続を認証するためのユーザーのアカウントを 255 文字以内の半角英数字と記号で入力します。 ・パスワード 接続を認証するためのパスワードを 255 文字以内の半角英数字と記号で入力します。 ●［証明書］ 選択すると、以下が表示されます。 ・証明書のタイプ

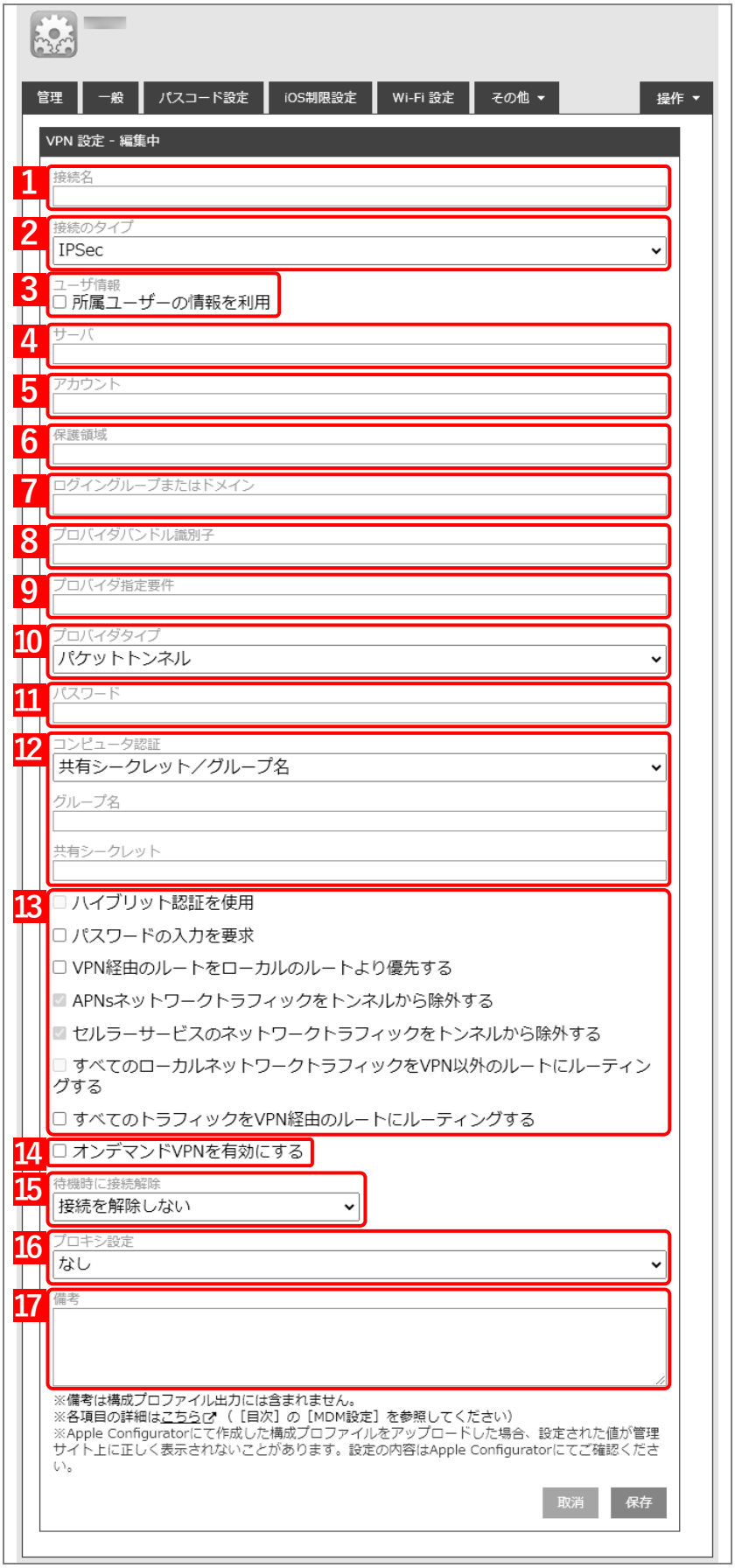
項番	項目	説明
		［RSA］、［ECDSA256］、［ECDSA384］、［ECDSA521］、［Ed25519］から選択します。 ・サーバ証明書発行者のコモンネーム サーバー証明書発行者のコモンネームを 255 文字以内の半角英数字と記号で入力します。 ・サーバ証明書のコモンネーム サーバー証明書のコモンネームを 255 文字以内の半角英数字と記号で入力します。 ・TLS の最小バージョン ［1.0］、［1.1］、［1.2］から選択します。 ・TLS の最大バージョン ［1.0］、［1.1］、［1.2］から選択します。 ・固有名証明書 リストボックスから設定する証明書を選択します。
10	待機時に接続解除	待機時に接続を解除しない、または接続を解除する時間を設定します。以下のいずれかを選択します。 ●［接続を解除しない］ ●［一定期間後］ 「分」「秒」を入力します。 項番 4「VPN 常時接続」の［VPN 常時接続（監視対象のみ）］にチェックが入っていないとき、本項目の設定ができます。
11	DPD（デッドピア検出）のレート	DPD の検出間隔を以下の項目から選択します。 ●［なし］、［低］、［中］、［高］
12	［リダイレクトを無効にする］	リダイレクトを無効にする場合は、チェックを入れます。
	［モバイル環境とマルチホーミングを無効にする］	モバイル環境とマルチホーミングを無効にする場合は、チェックを入れます。
	［IPv4 / IPv6 内部サブネットの属性を使用する］	IPv4 / IPv6 内部サブネットの属性を使用する場合は、チェックを入れます。
	［Perfect Forward Secrecy を有効にする］	Perfect Forward Secrecy を有効にする場合は、チェックを入れます。
	［証明書失効チェックを有効にする］	証明書失効チェックを有効にする場合は、チェックを入れます。
	［モバイル通信のフォールバックを有効にする］	モバイル通信のフォールバックを有効にする場合は、チェックを入れます。
	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、

項番	項目	説明
	VPN 経由のルートにルーティングする］	チェックを入れます。
13	最大転送単位（MTU）	最大転送単位（MTU）を 1280（最小値）～1400（最大値）の範囲で入力します。
14	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力
15	パラメーター	通信を確立するための制御値を設定します。 ●［IKE SA パラメータ］ 1 回目の通信を確立するとき ●［子 SA パラメータ］ 2 回目以降の通信を確立するとき
	暗号化アルゴリズム	以下の項目から選択します。 ●［DES］、［3DES］、［AES-128］、［AES-256］、［AES-128-GCM］、［AES-256-GCM］、［ChaCha20Poly1305］
	整合性アルゴリズム	以下の項目から選択します。 ●［SHA1-96］、［SHA1-160］、［SHA2-256］、［SHA2-384］、［SHA2-512］ 「暗号化アルゴリズム」で［AES-128-GCM］、［AES-256-GCM］を選択

項番	項目		説明
			した場合は、本項目は無効になります。
		Diffie-Hellman グループ	以下の項目から選択します。 ●［1］、［2］、［5］、［14］、［15］、［16］、［17］、［18］、［19］、［20］、［21］、［31］、［32］ iOS 14.2 以上の端末の場合、［1］、［2］、［5］は対応していません。
		存続期間（分単位）	SA 存続期間の Rekey 間隔を 10 分～1440 分の範囲で入力します。
16	DNS サーバアドレス		DNS サーバーのアドレスを追加します。255 文字以内の半角英数字と記号で入力します。
17	ドメイン名		トンネルのプライマリドメイン名を 255 文字以内の半角英数字と記号で入力します。
18	DNS 検索ドメイン		DNS 検索ドメインを追加します。255 文字以内の半角英数字と記号で入力します。
19	DNS 追加一致ドメイン		DNS 追加一致ドメインを追加します。255 文字以内の半角英数字と記号で入力します。
20	［追加ドメインを検索ドメインのリゾルバーのリストに含める］		追加ドメインを検索ドメインのリゾルバーのリストに含める場合は、チェックを入れます。
21	プロキシ設定		以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
22	備考		設定に関する内容など保存しておきたい場合、入力します。 備考は構成プロファイルには出力されません。

◆画面（接続タイプ：IPSec）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



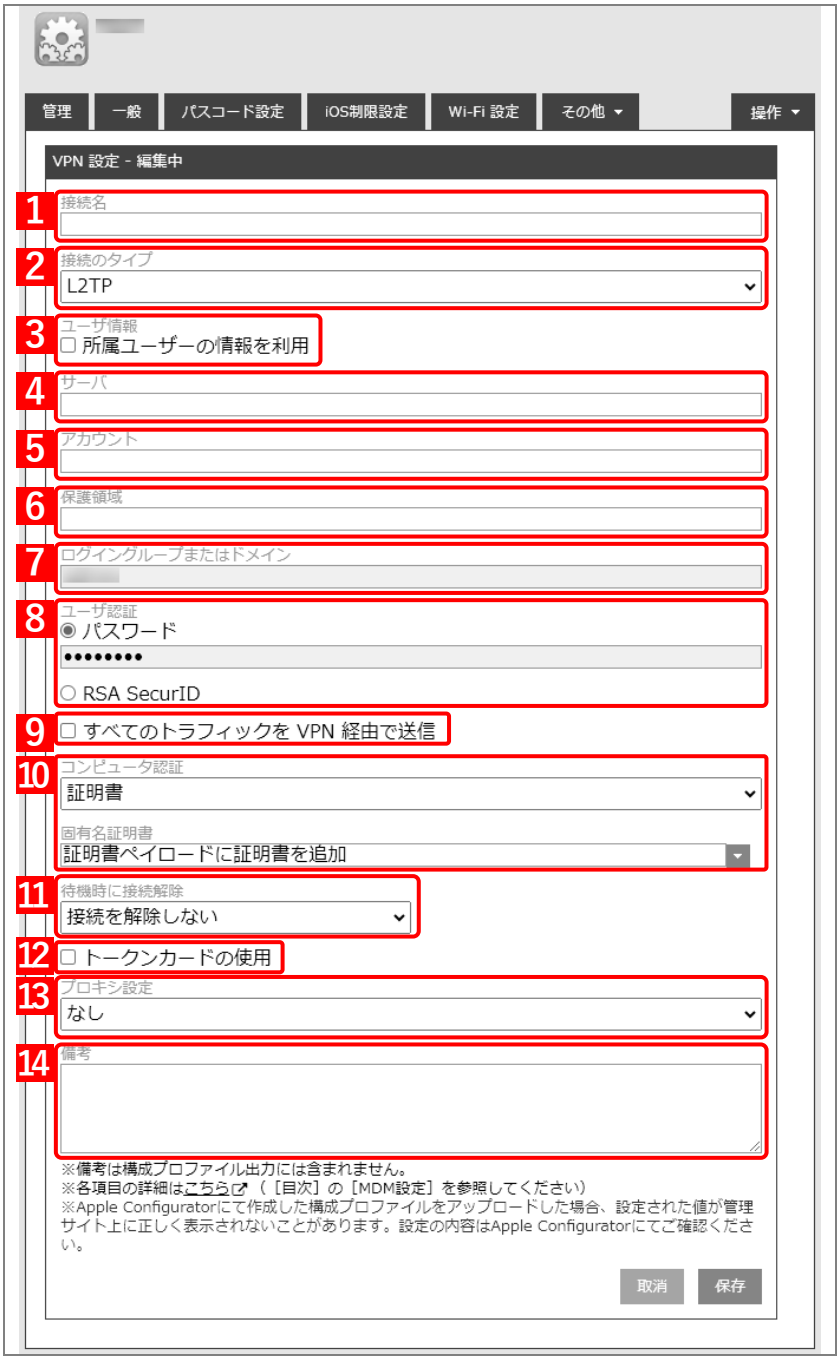
項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「IPSec」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
7	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力してください。
12	コンピュータ認証	接続時の認証タイプを以下の項目から選択します。 ●［証明書］ 以下の項目が表示されます。 ・固有名証明書 ［証明書ペイロードに証明書を追加］、［(機器に設定されているクライアント証明書)］、［登録済のクライアント証明書］から選択します。 ●［共有シークレット／グループ名］ 以下の項目が表示されます。 ・グループ名 接続するためのグループ名の入力欄が表示されます。255 文字以内の半角英数字と記号で入力します。 ・共有シークレット 接続するための共有シークレットの入力欄が表示されます。255 文字以内の半角英数字と記号で入力します。
13	［ユーザ PIN を含む］	必要な場合は、チェックを入れます。 項番 12「コンピュータ認証」で［証明書］を選択した場合に表示されます。
	［ハイブリッド認証を使用］	ハイブリッド認証を使用する場合は、チェックを入れます。 項番 12「コンピュータ認証」で［共有シークレット／グループ名］を選択した場合に表示されます。
	［パスワードの入力を要求］	パスワードの入力を要求する場合は、チェックを入れます。 項番 12「コンピュータ認証」で［共有シークレット／グループ名］を選択した場合に表示されます。
	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネッ	セルラーサービスのネットワークトラフィックをトンネルから除外する場

項番	項目	説明
	トワークトラフィックをトンネルから除外する］	合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
14	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 12「コンピュータ認証」で［証明書］を選択した場合は、「オンデマンド VPN(非推奨)」も表示されます。
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場

項番	項目	説明
		合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
15	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
16	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
17	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：L2TP）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**

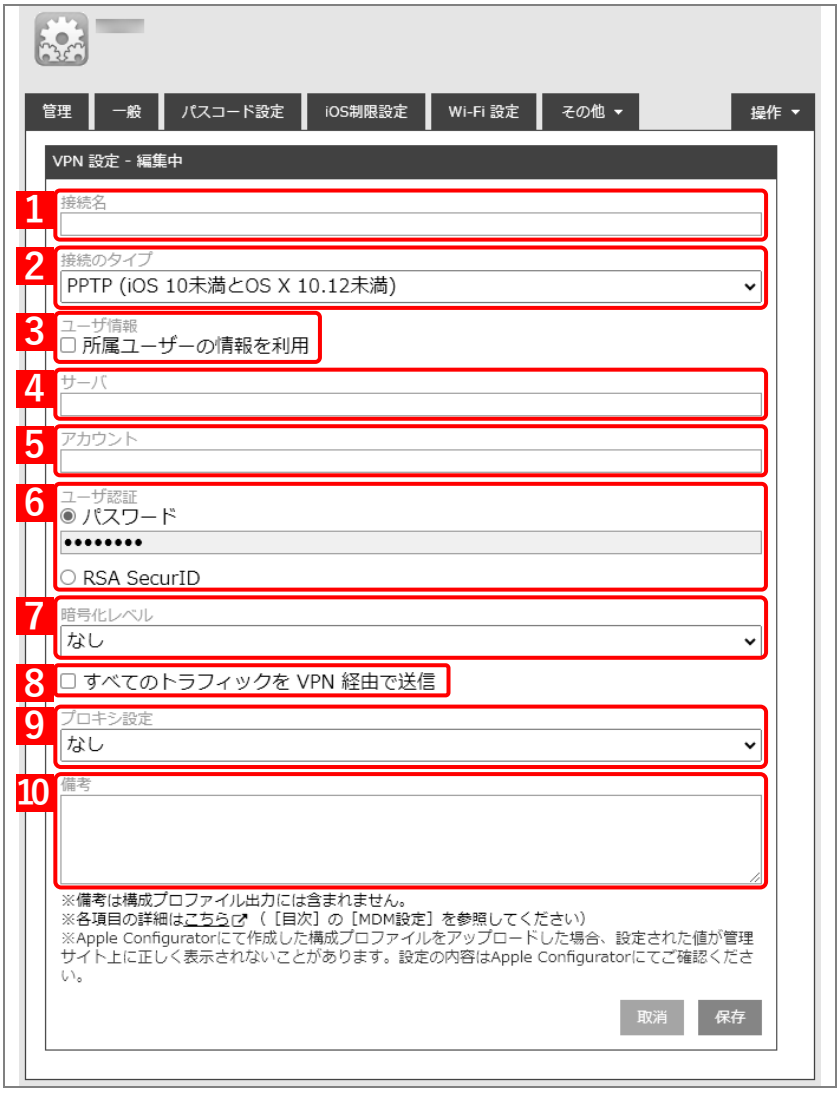


項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「L2TP」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。

項番	項目	説明
7	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
8	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［RSA SecurID］ ［パスワード］を選択した場合は、255 文字以内の半角英数字と記号で入力します。
9	すべてのトラフィックを VPN 経由で送信	●すべてのトラフィックを VPN 経由で送信 すべてのトラフィックを VPN 経由で送信する場合は、「すべてのトラフィックを VPN 経由で送信」にチェックを入れます。
10	コンピュータ認証	接続時の認証タイプを以下の項目から選択します。 ●［証明書］ 以下の項目が表示されます。 ・固有名証明書 ［証明書ペイロードに証明書を追加］、［(機器に設定されているクライアント証明書)］、［登録済のクライアント証明書］から選択します。 ●［共有シークレット］ 以下の項目が表示されます。 ・共有シークレット 接続するための共有シークレットの入力欄が表示されます。255 文字以内の半角英数字と記号で入力します。
11	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
12	トークンカードの使用	トークンカードを使用する場合は、「トークンカードの使用」にチェックを入れます。
13	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
14	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：PPTP（iOS 10 未満と OS X 10.12 未満））

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］

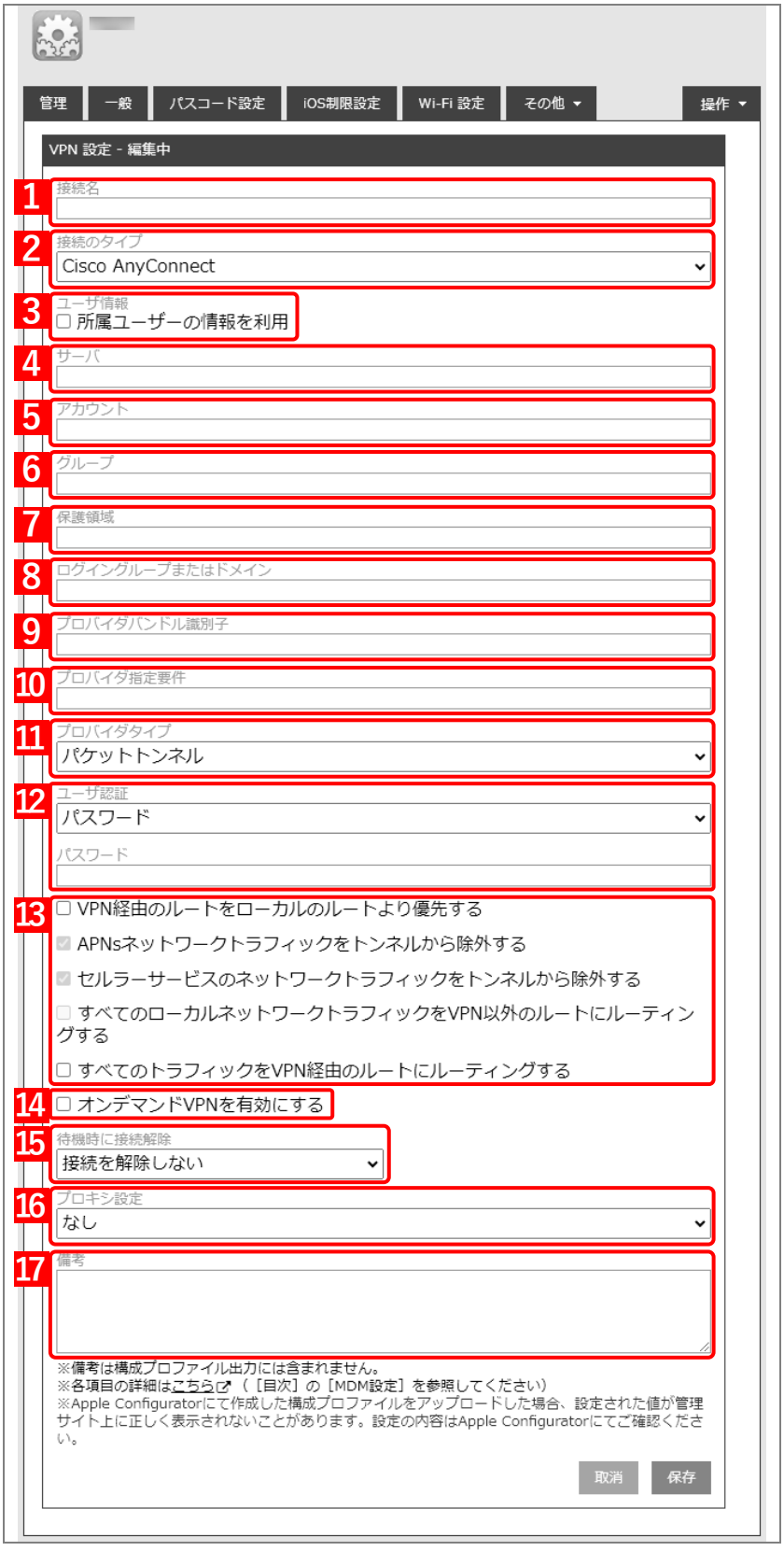


項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「PPTP（iOS 10 未満と OS X 10.12 未満）」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	ユーザ認証	以下の項目から選択します。 ● ［パスワード］ ● ［RSA SecurID］ ［パスワード］を選択した場合は、255 文字以内の半角英数字と記号で入力します。
7	暗号化レベル	以下の項目から選択します。 ● ［なし］ ● ［自動］ ● ［最大(128bit)］

項番	項目	説明
8	すべてのトラフィックを VPN 経由で送信	●すべてのトラフィックを VPN 経由で送信 すべてのトラフィックを VPN 経由で送信する場合は、「すべてのトラフィックを VPN 経由で送信」にチェックを入れます。
9	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 ☞「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 ☞「画面（プロキシ設定：自動）」484 ページ
10	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Cisco AnyConnect）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



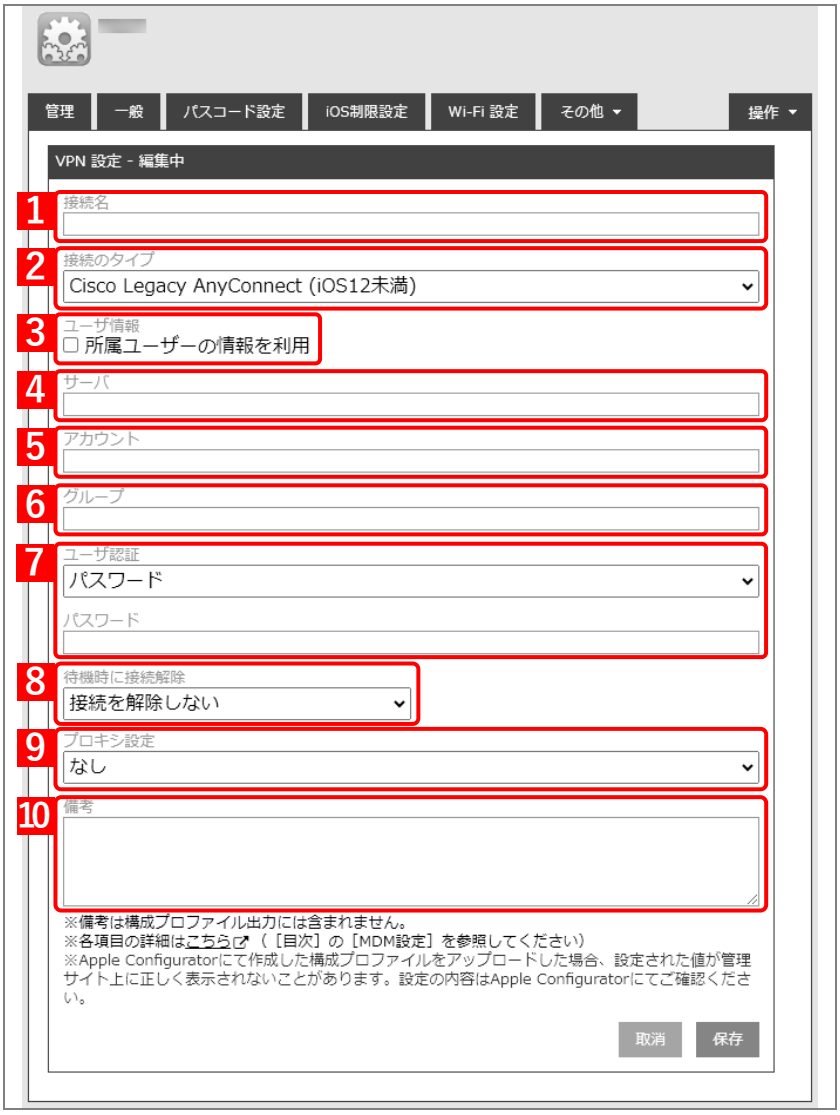
項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「Cisco AnyConnect」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	グループ	グループの名称を 255 文字以内の半角英数字と記号で入力してください。
7	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
8	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
9	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
11	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
12	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］ ●［パスワード+証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］または［パスワード+証明書］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
13	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルー	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。

項番	項目	説明
	ティングする］	
14	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 12「ユーザー認証」で［証明書］または［パスワード+証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。

項番	項目		説明
			インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
		待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 15「待機時に接続解除」は、自動的に［一定期間後］が選択されます。
15	待機時に接続解除		以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
16	プロキシ設定		以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
17	備考		設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Cisco Legacy AnyConnect（iOS12 未満））

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**

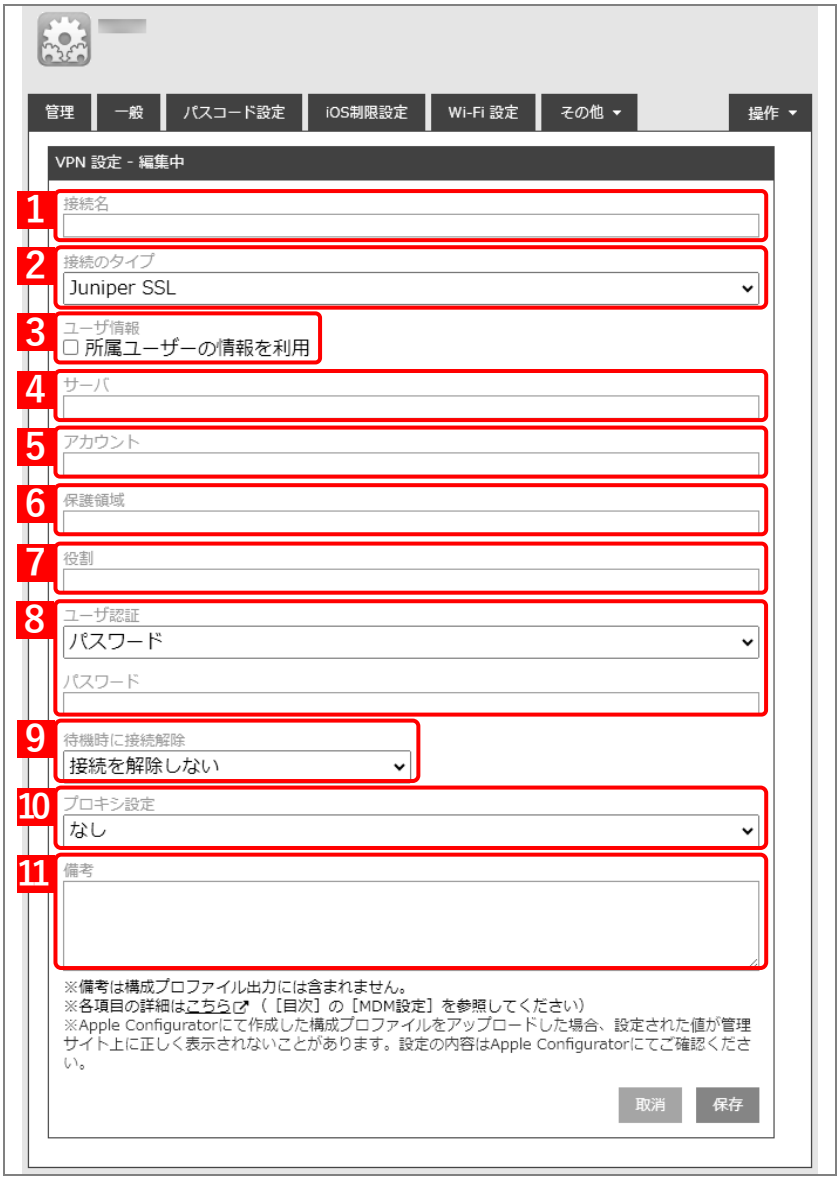


項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「Cisco LegacyAnyConnect（iOS12 未満）」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	グループ	グループの名称を 255 文字以内の半角英数字と記号で入力してください。
7	ユーザ認証	以下の項目から選択します。 ●「パスワード」 ●「証明書」 ●「パスワード+証明書」

項番	項目		説明
		パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］または［パスワード+証明書］を選択した場合に表示されます。
		資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
		［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にするは、チェックを入れます。チェックを入れると、以下の項目が表示されます。 ●該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ●要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。 ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
		待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 8「待機時に接続解除」は、自動的に［一定期間後］が選択されます。 ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
8	待機時に接続解除		以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
9	プロキシ設定		以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動)」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動)」484 ページ
10	備考		設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Juniper SSL）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］

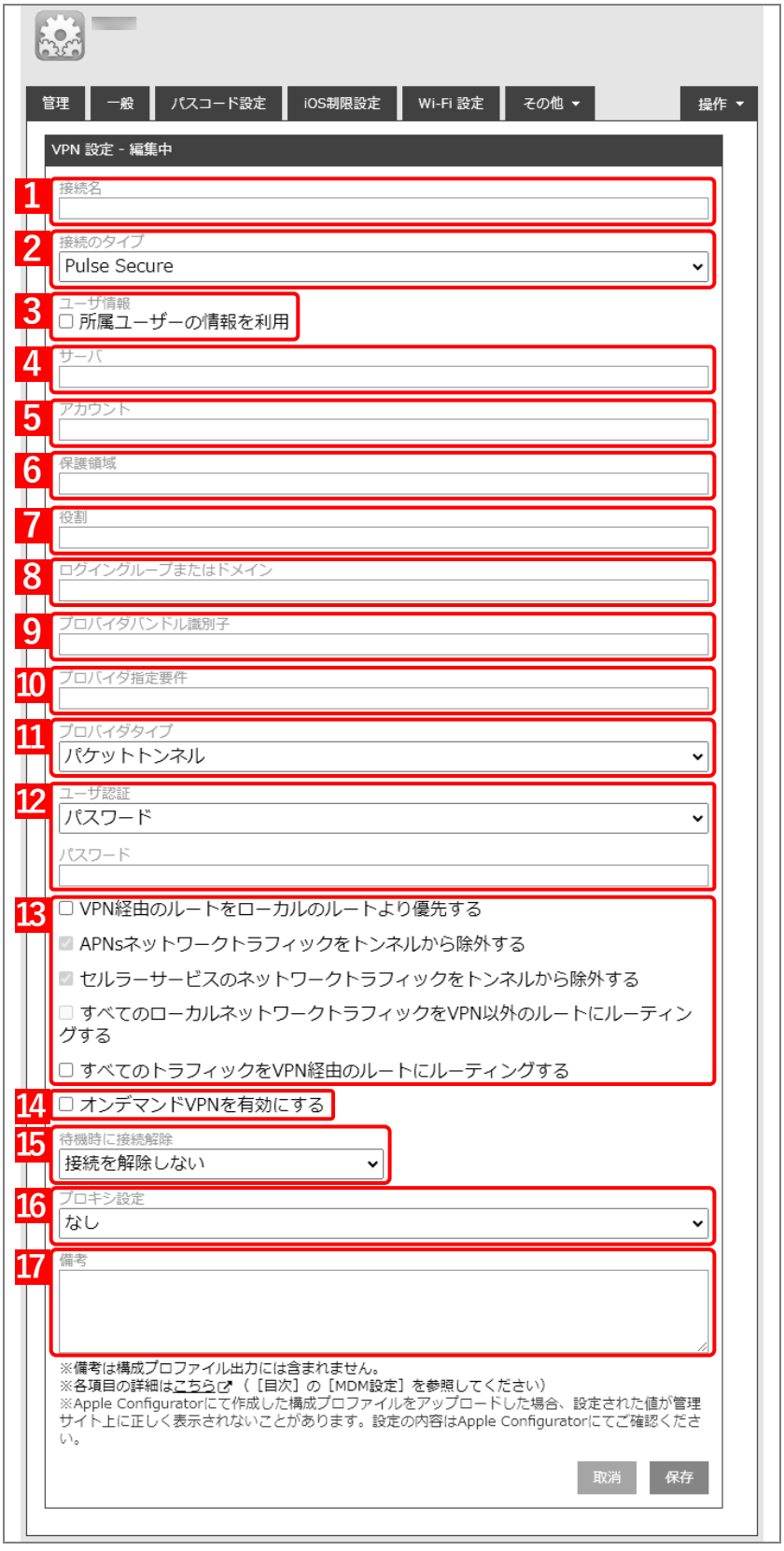


項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「Juniper SSL」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力してください。
7	役割	Juniper SSL で設定した役割を 255 文字以内の半角英数字と記号で入力してください。

項番	項目	説明
8	ユーザ認証	以下の項目から選択します。 ●「パスワード」 ●「証明書」 ●「パスワード+証明書」
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］または［パスワード+証明書］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にするは、チェックを入れます。チェックを入れると、以下の項目が表示されます。 ●該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ●要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。 ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
	待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 9「待機時に接続解除」は、自動的に［一定期間後］が選択されます。 ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
9	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
10	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動)」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動)」484 ページ
11	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Pulse Secure）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「Pulse Secure」を選択します。

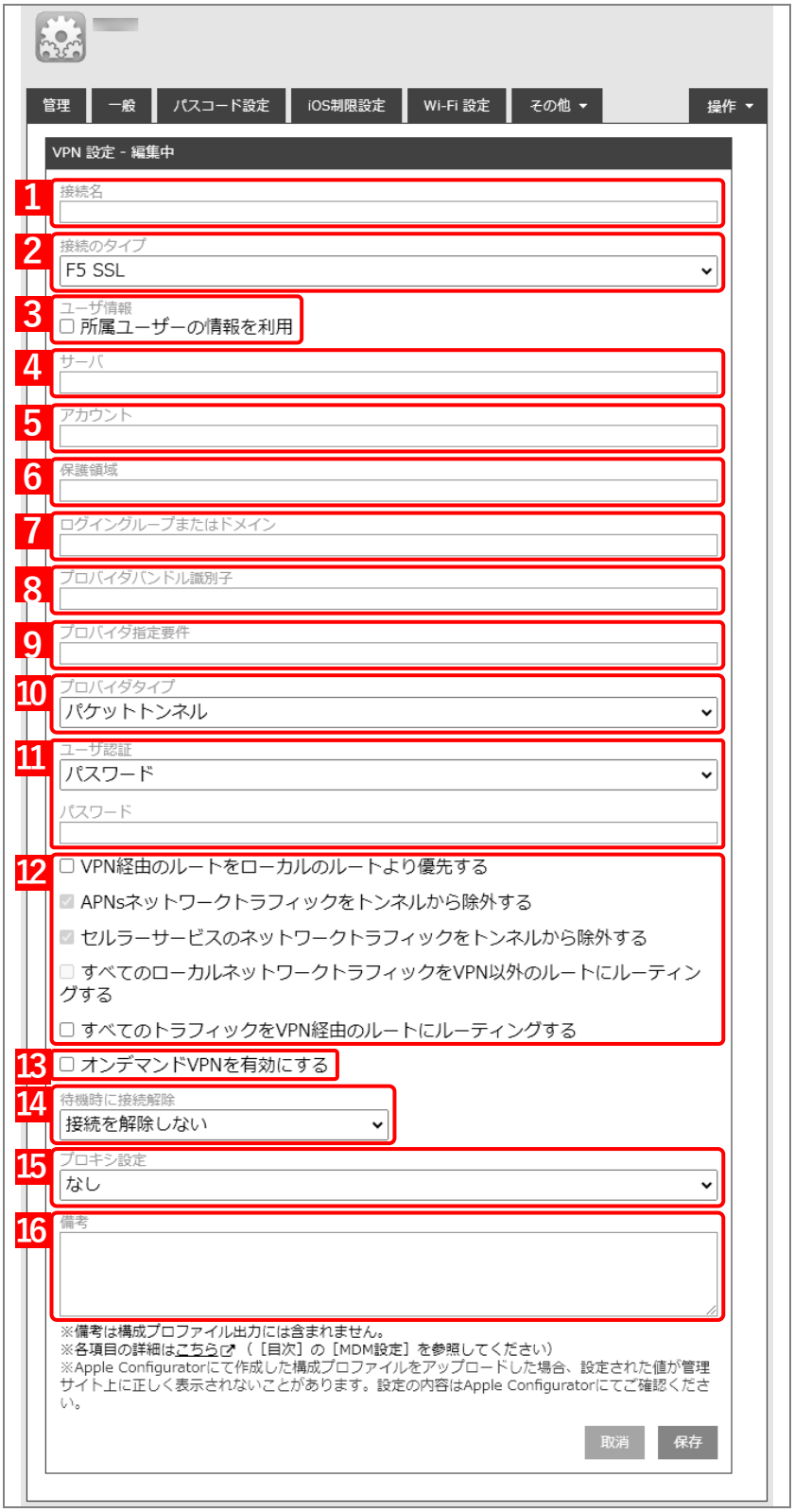
項番	項目	説明
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力してください。
7	役割	Pulse Secure で設定した役割を 255 文字以内の半角英数字と記号で入力してください。
8	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
9	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
11	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
12	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］ ●［パスワード+証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］または［パスワード+証明書］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
13	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
14	［オンデマンド VPN を有	オンデマンド VPN を有効にする場合は、チェックを入れます。

項番	項目	説明
	効にする］	✎チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 12「ユーザー認証」で［証明書］または［パスワード+証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、✖ をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 ✎非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ✎ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ✎ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 ✎インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 ✎インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 ✎インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。

項番	項目	説明
	待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 15「待機時に接続解除」は、自動的に［一定期間後］が選択されます。
15	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
16	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
17	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：F5 SSL）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



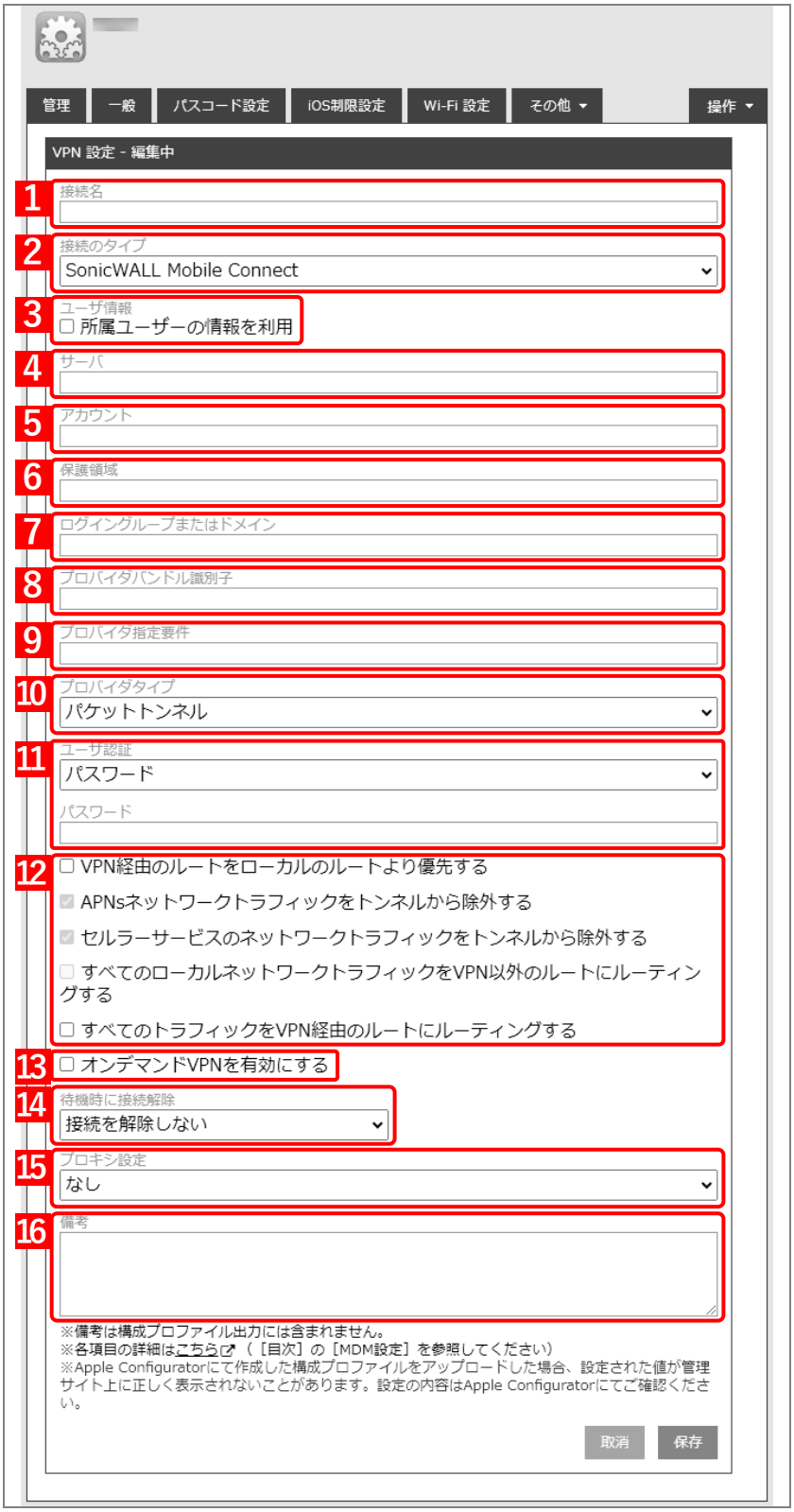
項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「F5 SSL」を選択します。
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
7	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］ ●［パスワード+証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］または［パスワード+証明書］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］または［パスワード+証明書］を選択した場合に表示されます。
12	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。

項番	項目	説明
13	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 11「ユーザー認証」で［証明書］または［パスワード+証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。

項番	項目	説明
		●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
	待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 14「待機時に接続解除」は、自動的に［一定期間後］が選択されます。
14	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
15	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
16	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：SonicWALL Mobile Connect）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「SonicWALL Mobile Connect」を選択します。

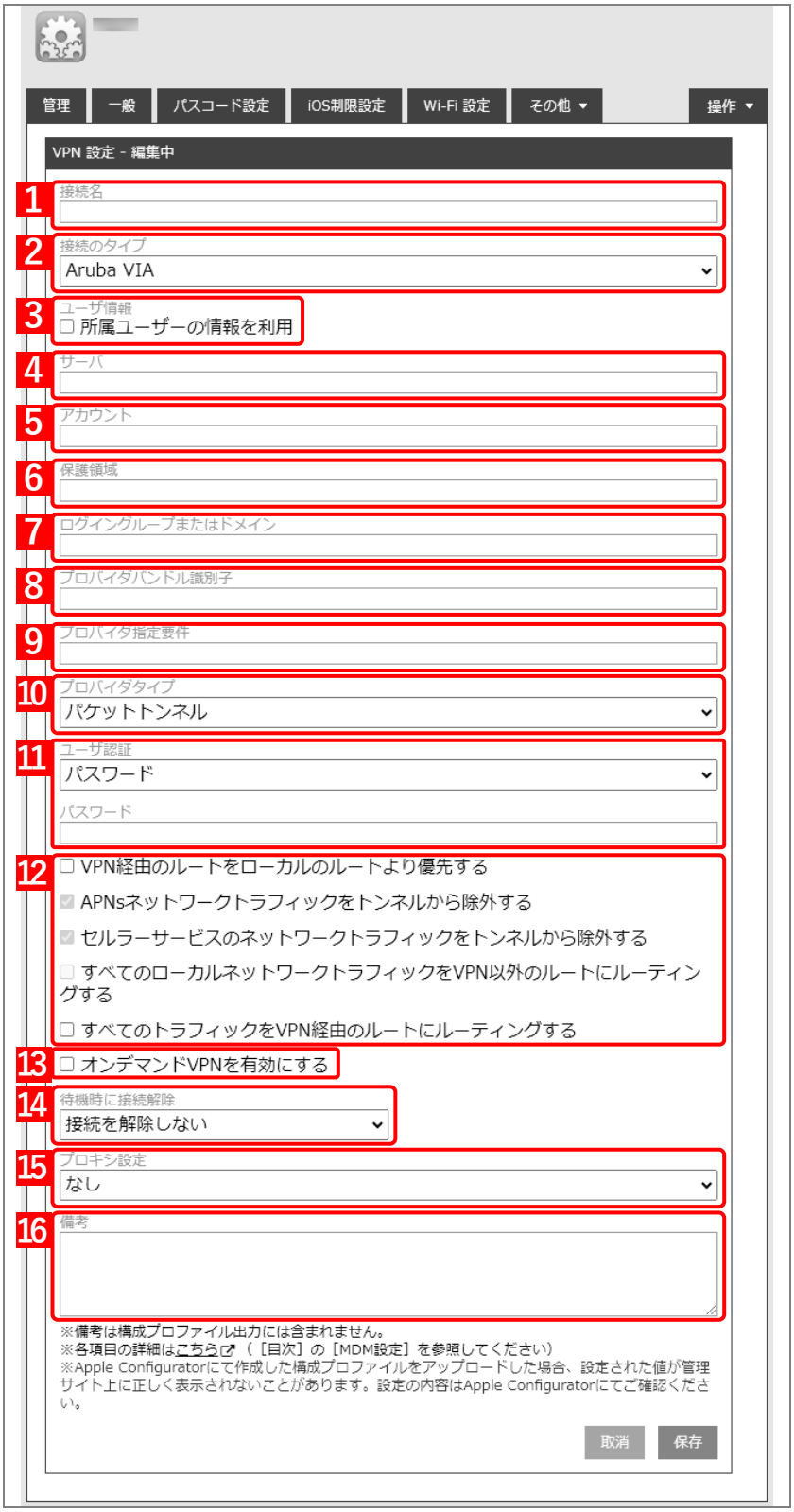
項番	項目	説明
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
7	ログイングループまたはドメイン	ログイングループまたはドメインの名称 255 文字以内の半角英数字と記号で入力してください。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］を選択した場合に表示されます。
12	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
13	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 11「ユーザー認証」で［証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。

項番	項目		説明
		［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
		オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を、「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
		オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
		待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 14「待機時に接続解除」は、自動的に［一定期間後］が選択されます。

項番	項目	説明
14	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
15	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
16	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Aruba VIA）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続タイプ	「Aruba VIA」を選択します。

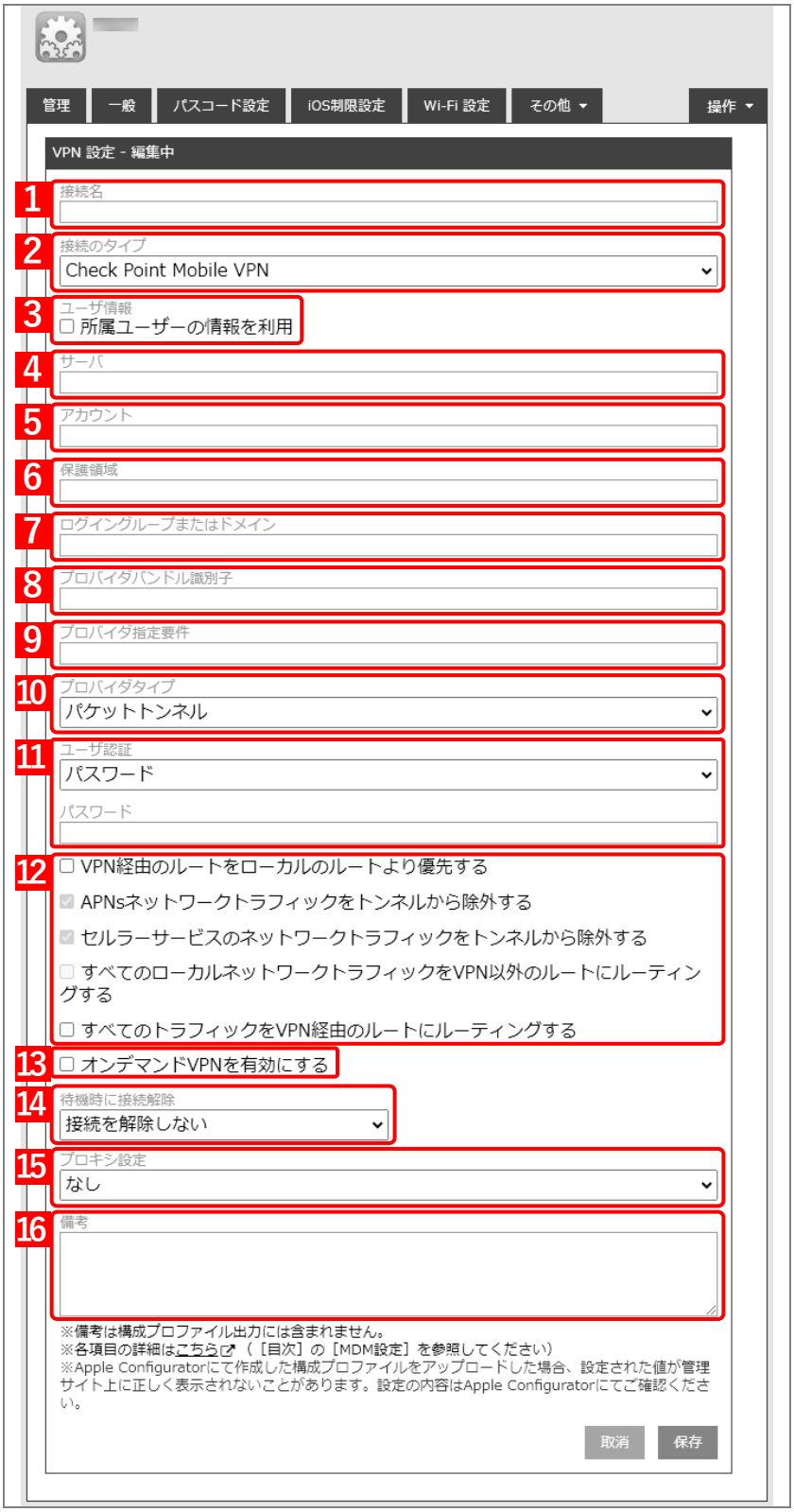
項番	項目	説明
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
7	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］を選択した場合に表示されます。
12	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
13	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 11「ユーザー認証」で［証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。

項番	項目		説明
		［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
		オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
		オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
		待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 14「待機時に接続解除」は、自動的に［一定期間後］が選択されます。

項番	項目	説明
14	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
15	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
16	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：Check Point Mobile VPN）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「Check Point Mobile VPN」を選択します。

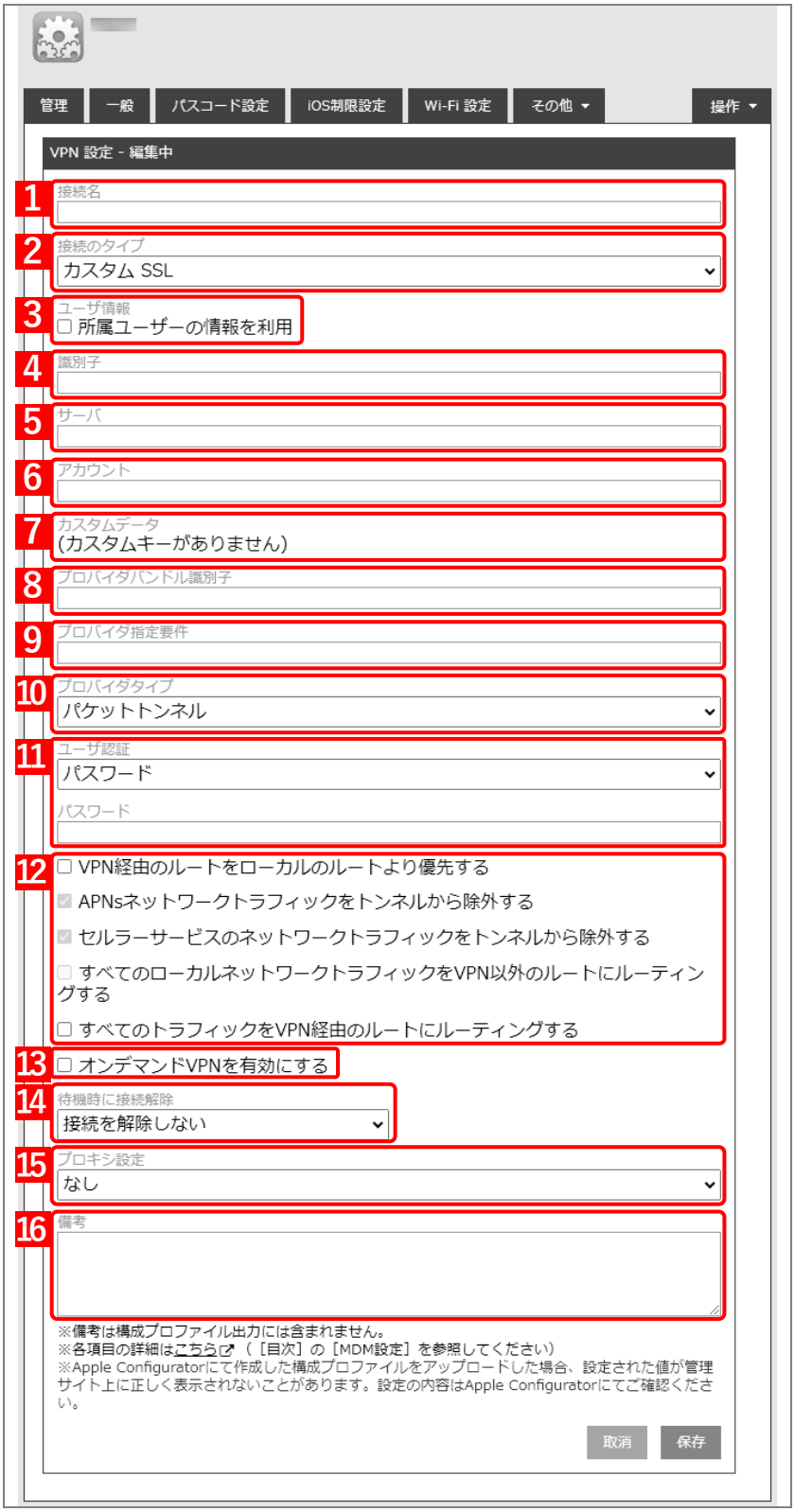
項番	項目	説明
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
5	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
6	保護領域	保護領域を 255 文字以内の半角英数字と記号で入力します。
7	ログイングループまたはドメイン	ログイングループまたはドメインを 255 文字以内の半角英数字と記号で入力します。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］を選択した場合に表示されます。
12	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
13	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 11「ユーザー認証」で［証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。

項番	項目		説明
		［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
		オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
		オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
		待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 14「待機時に接続解除」は、自動的に［一定期間後］が選択されます。

項番	項目	説明
14	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を入力してください。
15	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
16	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（接続タイプ：カスタム SSL）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］



項番	項目	説明
1	接続名	接続の名称を 255 文字以内の半角英数字と記号で入力してください。
2	接続のタイプ	「カスタム SSL」を選択します。

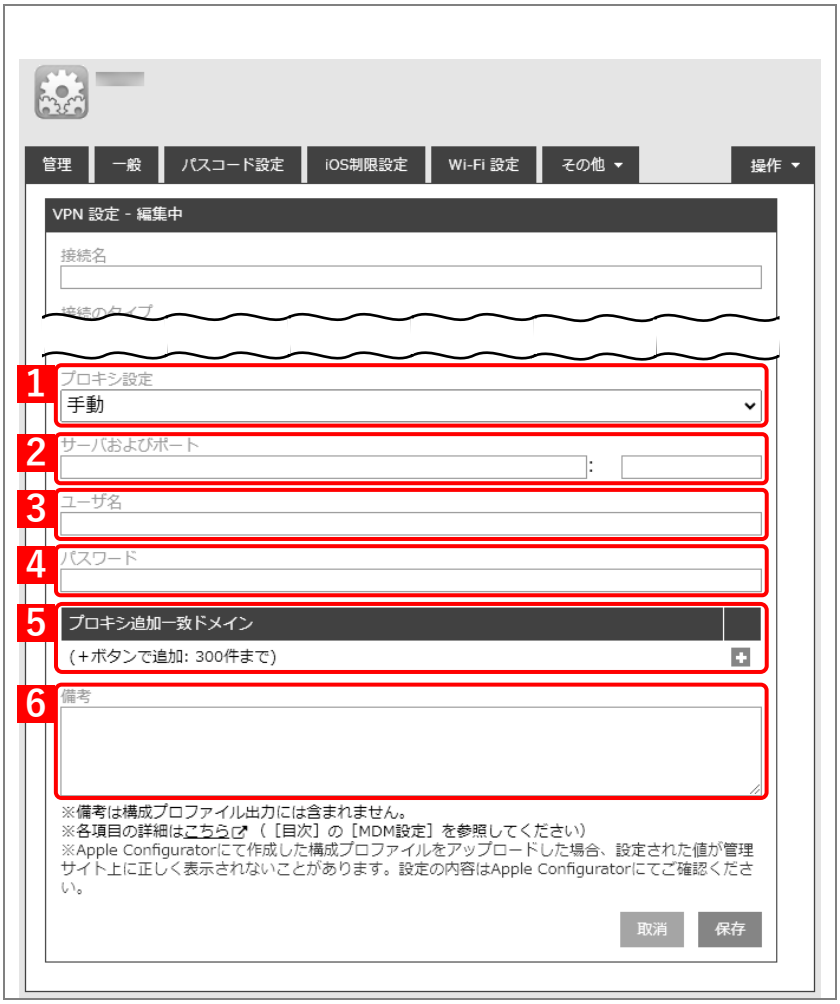
項番	項目	説明
3	ユーザ情報	●所属ユーザーの情報を利用 所属ユーザーの情報を利用する場合は、「所属ユーザーの情報を利用」にチェックを入れます。
4	識別子	識別子を入力します。
5	サーバ	サーバーの名称を 255 文字以内の半角英数字と記号で入力してください。
6	アカウント	アカウントの名称を 255 文字以内の半角英数字と記号で入力してください。
7	カスタムデータ	カスタムデータをキーと値の組み合わせで入力します。
8	プロバイダバンドル識別子	プロバイダバンドル識別子を 255 文字以内の半角英数字と記号で入力します。
9	プロバイダ指定要件	プロバイダ指定要件を 255 文字以内の半角英数字と記号で入力します。
10	プロバイダタイプ	以下の項目から選択します。 ●［パケットトンネル］ ●［App プロキシ］
11	ユーザ認証	以下の項目から選択します。 ●［パスワード］ ●［証明書］
	パスワード	パスワードを 255 文字以内の半角英数字と記号で入力します。 ［パスワード］を選択した場合に表示されます。
	資格情報	以下の項目から選択します。 ●［証明書ペイロードに証明書を追加］ ●［(機器に設定されているクライアント証明書)］ ●［登録済みのクライアント証明書］ ［証明書］を選択した場合に表示されます。
12	［VPN 経由のルートをローカルのルートより優先する］	VPN 経由のルートをローカルのルートより優先する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、無効になります。
	［APNs ネットワークトラフィックをトンネルから除外する］	APNs ネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［セルラーサービスのネットワークトラフィックをトンネルから除外する］	セルラーサービスのネットワークトラフィックをトンネルから除外する場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする］	すべてのローカルネットワークトラフィックを VPN 以外のルートにルーティングする場合は、チェックを入れます。 本項目は［すべてのトラフィックを VPN 経由のルートにルーティングする］にチェックが入っていると、有効になります。
	［すべてのトラフィックを VPN 経由のルートにルーティングする］	すべてのトラフィックを VPN 経由のルートにルーティングする場合は、チェックを入れます。
13	［オンデマンド VPN を有効にする］	オンデマンド VPN を有効にする場合は、チェックを入れます。 チェックを入れると、［ユーザーによるオンデマンド VPN の切り替えを無効にする］、「オンデマンド VPN ルール」が表示されます。項番 11「ユーザー認証」で［証明書］を選択した場合は、「オンデマンド VPN(非推奨)」、「待機時に接続解除」も表示されます。

項番	項目	説明
	［ユーザーによるオンデマンド VPN の切り替えを無効にする］	ユーザーによるオンデマンド VPN の切り替えを無効にする場合は、チェックを入れます。
	オンデマンド VPN(非推奨)	本項目に表示されているオンデマンド VPN は Apple で推奨されていないため、 をクリックして削除し、Apple 推奨のオンデマンド VPN を「オンデマンド VPN ルール」に追加してください。 非推奨のオンデマンド VPN を使用すると、動作に不具合が生じる場合があります。やむを得ず非推奨のオンデマンド VPN を追加する場合は、以下の項目を入力、選択してください。 ・該当ドメイン／ホスト 255 文字以内の半角英数字、全角ひらがな・カタカナ・漢字、ピリオド「.」、ハイフン「-」で入力します。 ・要求があったときの処理 ［常に確立］、［確立しない］、［必要に応じて確立］から選択します。
	オンデマンド VPN ルール	オンデマンド VPN ルールを追加します。以下の項目を選択、入力します。 ●アクション ［接続する］、［切断する］、［通信時に判定して接続する］、［次回の接続を無効にする］から選択します。 ●アクションパラメータ アクションで［通信時に判定して接続する］を選択した場合、表示されます。 ・ドメインアクション ［必要に応じて確立］、［確立しない］から選択します。 ・ドメイン ドメインを 255 文字以内の半角英数字と記号で入力します。 ・DNS サーバアドレスドメイン DNS サーバーのアドレスドメインを 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ・プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。 ドメインアクションで［必要に応じて確立］を選択した場合、表示されます。 ●インターフェースタイプ ［Ethernet］、［WiFi］、［Cellular］から選択します。 ●DNS ドメイン DNS ドメインを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●DNS サーバアドレス DNS サーバーのアドレスを 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［Ethernet］または［WiFi］に選択した場合、表示されます。 ●SSID SSID を 255 文字以内の半角英数字と記号で入力します。 インターフェースタイプを［WiFi］に選択した場合、表示されます。 ●プローブ URL プローブ URL を 255 文字以内の半角英数字と記号で入力します。
	待機時に接続解除	［接続を解除しない］、［1 分］、［2 分］、［5 分］、［15 分］、［30 分］、［1 時間］から選択します。 ［接続を解除しない］以外を選択した場合、項番 14「待機時に接続解除」は、自動的に［一定期間後］が選択されます。

項番	項目	説明
14	待機時に接続解除	以下の項目から選択します。 ●［接続を解除しない］ ●［一定期間後］ ［一定期間後］を選択した場合は、「分」と「秒」を設定する欄が表示されます。
15	プロキシ設定	以下の項目から選択します。 ●［なし］ ●［手動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：手動）」483 ページ ●［自動］ 詳細については、以下を参照してください。 「画面（プロキシ設定：自動）」484 ページ
16	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（プロキシ設定：手動）

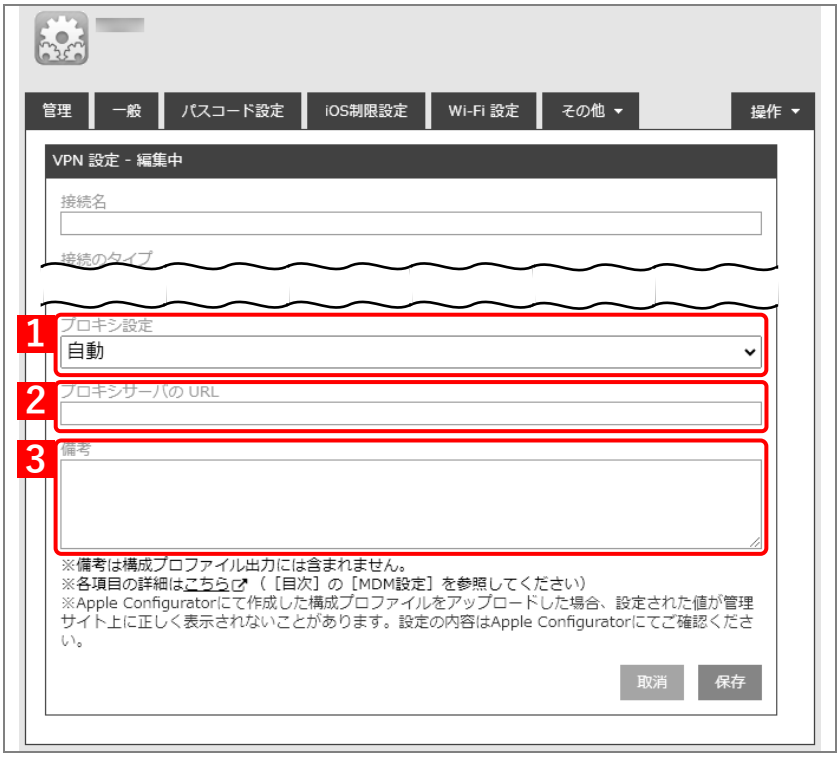
表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



項番	項目	説明
1	プロキシ設定	「手動」を選択します。
2	サーバおよびポート	プロキシ設定で手動を選択した場合、入力必須です。 サーバーは 255 文字以内の半角英数字、記号で入力します。 ポートは 0 以上 65535 以下の半角数字で入力してください。
3	ユーザ名	プロキシ接続ユーザーの名称を 255 文字以内の半角英数字と記号で入力してください。
4	パスワード	プロキシ接続パスワードを 255 文字以内の半角英数字と記号で入力してください。
5	プロキシ追加一致ドメイン	プロキシ追加一致ドメインを 255 文字以内の半角英数字と記号で入力します。
6	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

◆画面（プロキシ設定：自動）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［VPN 設定］→［新規作成］または［編集］**



項番	項目	説明
1	プロキシ設定	「自動」を選択します。
2	プロキシサーバの URL	プロキシ設定取得 URL を 255 文字以内の半角英数字と記号で入力してください。
3	備考	設定に関する内容など保存しておきたい場合にご利用ください。 備考は構成プロファイル出力に含まれません。

8.3.1.13 ［その他▼］タブ／カレンダー設定

iOS 標準のカレンダーアプリに、CalDAV アカウントの設定を行います。CalDAV アカウントを設定すると、カレンダーアプリに登録したアカウントの予定表の共有や同期ができます。

本設定は、1 つの構成プロファイルアップロードに 10 件まで設定できます。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［カレンダー設定］→［新規作成］または［編集］

項番	項目	説明
1	アカウントの説明	カレンダーの説明を 255 文字以内で入力します。
2	アカウントのホスト名とポート	●ホスト名 入力必須です。CalDAV サーバーのホスト名を 255 文字以内の半角英数字、記号で入力します。 ●ポート CalDAV サーバーに接続するポートを 0 から 65535 の整数を半角数字で入力します。
3	プリンシパル URL	プリンシパル URL を 255 文字以内の半角英数字、記号で入力します。
4	アカウントのユーザ名	アカウントのユーザー名を 255 文字以内で入力します。 本項目は入力必須ではありませんが、構成プロファイルを配信したあとに端末で設定することはできません。ユーザー名を設定する場合は、必ず入力してください。
5	アカウントのパスワード	アカウントのパスワードを 255 文字以内の半角英数字、記号で入力します。
6	SSL を使用	SSL を使用する場合は、チェックを入れます。

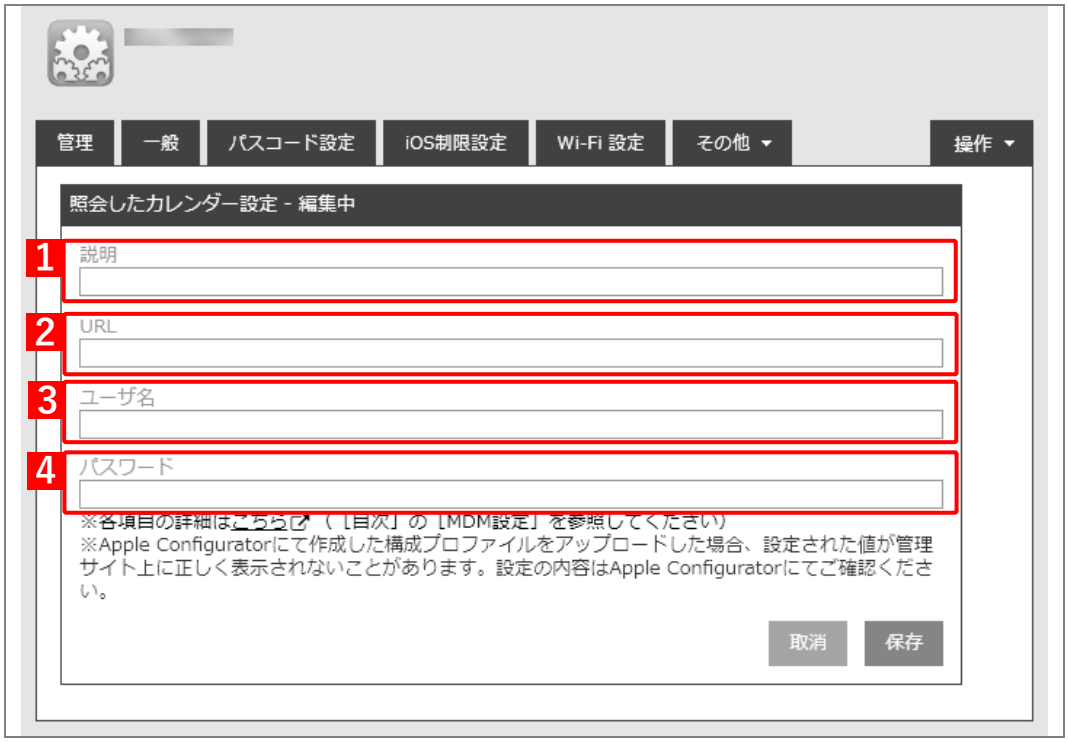
8.3.1.14 ［その他▼］タブ／照会したカレンダー設定

iOS 標準のカレンダーアプリに、照会したカレンダーのアカウントの設定を行います。照会したカレンダーのアカウントを設定すると、カレンダーアプリでアカウントの予定を閲覧できます。

本設定は、1 つの構成プロファイルアップロードに 10 件まで設定できます。

◆画面

表示操作 **［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［照会したカレンダー設定］→［新規作成］または［編集］**



項番	項目	説明
1	説明	カレンダー照会の説明を 255 文字以内で入力します。
2	URL	入力必須です。照会するカレンダーファイルの URL を 255 文字以内の半角英数字、記号で入力します。
3	ユーザ名	照会のユーザー名を 255 文字以内で入力します。
4	パスワード	照会のパスワードを 255 文字以内の半角英数字、記号で入力します。

8.3.1.15 ［その他▼］タブ／連絡先設定

iOS 標準の連絡先アプリに、CardDAV アカウントの設定を行います。CardDAV アカウントを設定すると、連絡先アプリに登録したアカウントの連絡先の共有や同期ができます。

本設定は、1 つの構成プロファイルアップロードに 10 件まで設定できます。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［連絡先設定］→［新規作成］または［編集］

項番	項目	説明
1	アカウントの説明	連絡先の説明を 255 文字以内で入力します。
2	アカウントのホスト名とポート	●ホスト名 入力必須です。CardDAV サーバーのホスト名を 255 文字以内の半角英数字、記号で入力します。 ●ポート CardDAV サーバーに接続するポートを 0 から 65535 の整数を半角数字で入力します。
3	プリンシパル URL	プリンシパル URL を 255 文字以内の半角英数字、記号で入力します。
4	アカウントのユーザ名	アカウントのユーザー名を 255 文字以内で入力します。 本項目は入力必須ではありませんが、構成プロファイルを配信したあとに端末で設定することはできません。ユーザー名を設定する場合は、必ず入力してください。
5	アカウントのパスワード	アカウントのパスワードを 255 文字以内の半角英数字、記号で入力します。

項番	項目	説明
6	SSL を使用	SSL を使用する場合は、チェックを入れます。
7	通信サービスルール	本設定で配信した連絡先と通話するときに使用するデフォルトアプリのアプリケーション ID を 255 文字以内の半角英数字、記号（「.」、「-」）で入力します。

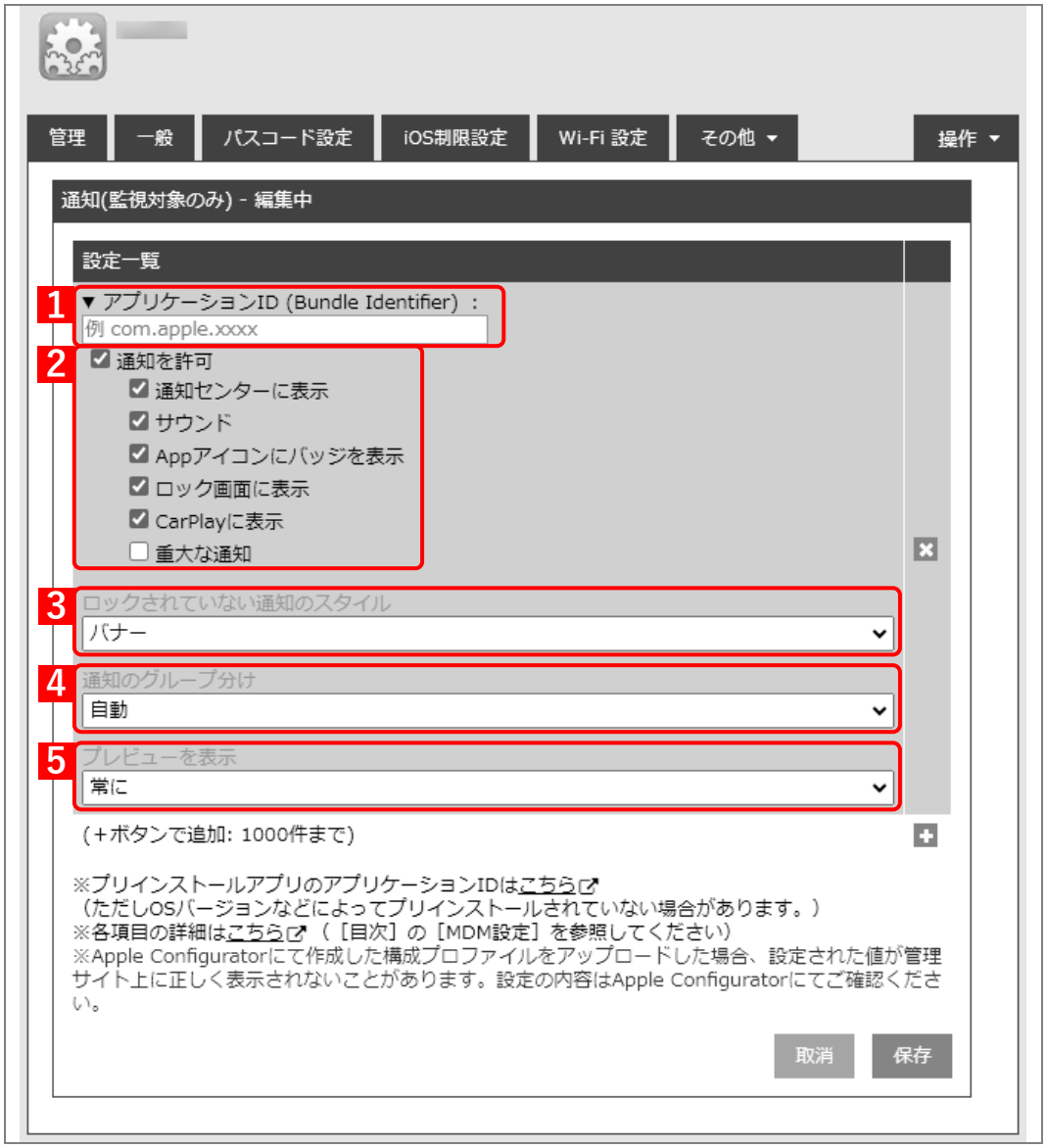
8.3.1.16 ［その他▼］タブ／通知

通知に関する各種の設定を行います。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［通知］→［新規作成］または［編集］→設定一覧の＋

通知を制御するアプリは、最大 1,000 件まで設定できます。



項番	項目	説明
1	アプリケーション ID (Bundle Identifier)	通知を制御するアプリのアプリケーション ID を 255 文字以内で入力します。使用できる文字は、半角英数字と記号（「.」、「-」）です。入力必須です。 オリジナルアプリのアプリケーション ID を入力すると、オリジナルアプリの通知も制御することができます。
2	通知を許可	チェックを入れると、アプリケーションの通知を許可します。また、以下の項目にチェックを入れることができます。 ●通知センターに表示 チェックを入れると、通知センターに通知を表示します。 ●サウンド チェックを入れると、サウンドありで通知します。 ●App アイコンにバッジを表示 チェックを入れると、指定したアプリのアイコンに通知件数を表示します。 ●ロック画面に表示 チェックを入れると、通知をロック画面に表示します。 ●CarPlay に表示 チェックを入れると、通知を CarPlay に表示します。 ●重大な通知 チェックを入れると、重大な通知を許可します。
3	ロックされていない通知のスタイル	ロックされていないときの通知の表示形式を指定します。以下の項目から選択します。 ●なし 通知を表示しない。 ●バナー 通知を画面の上部に一時的に表示します。操作をしなくても一定の時間が経過すると通知が表示されなくなります。 ●通知 確認操作を必要とするスタイルで、通知を表示します。通知を確認するまで、表示は消えません。
4	通知のグループ分け	通知をどのようにグループ分けするかを指定します。以下の項目から選択します。 ●自動 通知を自動的にグループ化します。 ●App 別 アプリ別に通知をグループ化します。 ●オフ 通知をグループ化しません。 通知をすべて表示したい場合は、オフを選択してください。
5	プレビューを表示	通知の内容を表示するかを指定します。以下の項目から選択します。 ●常に 通知の内容を常に表示します。 ●ロックされていないときのみ 通知の内容をロックされていないときに表示します。ロックされているときは表示しません。 ●しない 通知の内容を常に表示しません。

8.3.1.17 ［その他▼］タブ／Web クリップ設定

Web クリップに関する各種の設定を行います。

利用を推奨している Web ページ（自社ホームページ・ブックマーク）や、普段馴染みのない緊急連絡先・サポートデスクの電話番号を、指定のアイコンとともに設定し、Web クリップとして管理している端末に配信することができます。

管理している端末に配信された Web ページや電話番号のアイコンが、Web クリップとして表示され、端末利用者は少ないステップで目的のページや電話番号にたどりつけます。

- Web クリップを配信していても、Web ページによってはページ内で指定されたアイコンが強制的に適用される場合があります。
- 本機能で新規作成、および編集した Web クリップは、iOS 端末の操作で削除できません。
- 1 つの構成プロファイルに、Web クリップは 5 つまで設定できます。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［Web クリップ］→［新規作成］または［編集］

項番	項目	説明
1	ラベル	Web クリップの名称を 255 文字以内で入力してください。入力必須です。
2	URL	配信用のページの URL を 255 文字以内で入力してください。入力必須です。
3	削除を許可	●Web クリップを取り除くことを許可 チェックを入れると、端末で Web クリップを削除できます。
4	アイコン	［ファイルを選択］をクリックして、GIF、JPEG、PNG 形式の画像を指定してください。 画像のファイルサイズは、10KB より大きいサイズに対応していません。
5	作成済みアイコン	●視覚エフェクトなしでアイコンを表示 視覚エフェクトなしでアイコンを表示する場合にチェックを入れます。
6	フルスクリーン	●Web クリップをフルスクリーンアプリケーションとして表示 チェックを入れると、「フルスクリーンアプリケーション」が Web アプリとして、端末にインストールされ、Web クリップが「フルスクリーンアプリケーション」として表示します。 Web クリップのサイトを起動するアプリは、 ブラウザーなしで URL や検索バー、ブックマークのない Web アプリとして表示されます。そのため Safari を制限していても、Web クリップは制限されません。 Web ページによってはページ内で指定されたアイコンが強制的に適応されることを回避できます。ただし、Apple の仕様により適応されてしまう場合もあります。
7	マニフェストの範囲を無視	●マニフェストに含まれていない Web ページに、フルスクリーンモードでの読み込みを許可 チェックを入れると、指定した Web ページから他のページへ遷移してもフルスクリーンを維持します。 本項目は、項番 6「フルスクリーン」にチェックが入っている場合に有効になります。
8	アプリケーション ID (Bundle Identifier)	URL を表示するためのアプリケーション ID を 255 文字以内で入力します。使用できる文字は、半角英数字と記号（「.」、「-」）です。

8.3.1.18 ［その他▼］タブ／モバイル通信設定

モバイル通信に関する各種の設定を行います。

画面（構成する APN のタイプ：デフォルト APN）

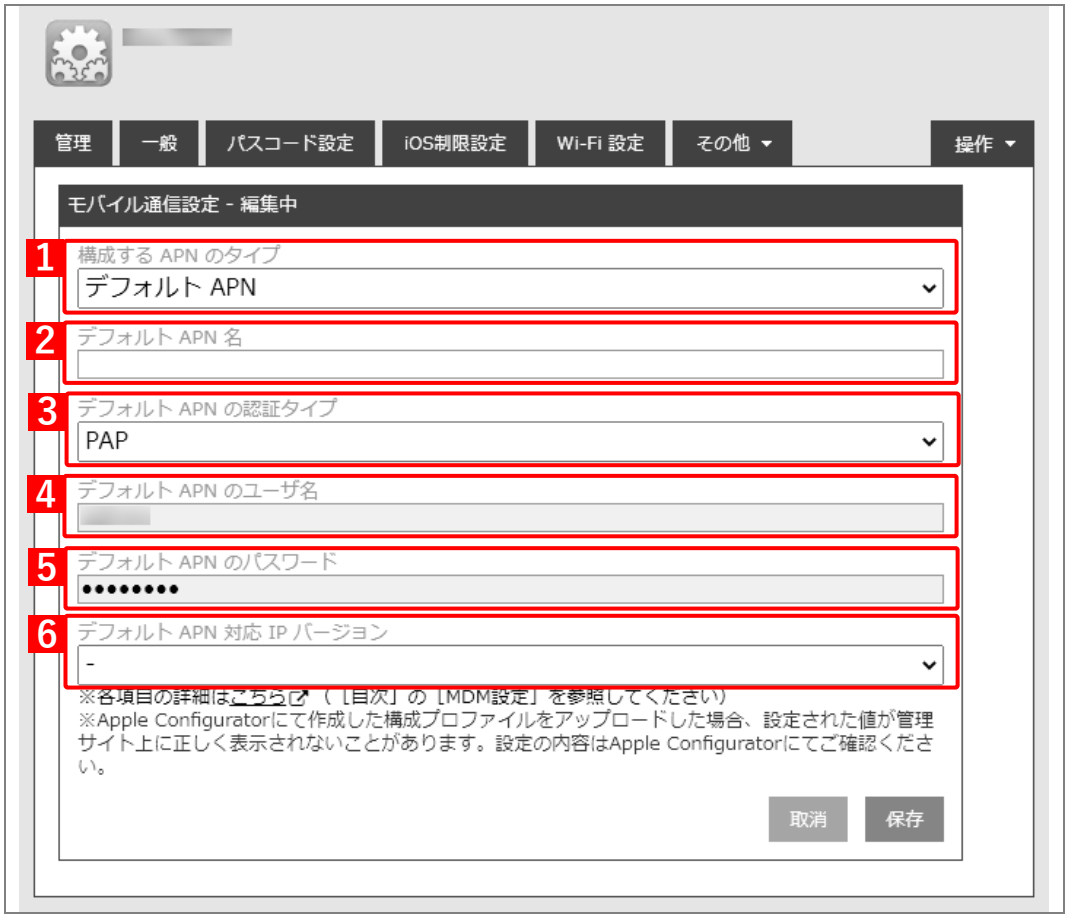
画面（構成する APN のタイプ：データ APN）

画面（構成する APN のタイプ：デフォルト APN とデータ APN）

本設定を含んだ構成プロファイルを端末に配信したあと、端末のモバイル通信を使用して他の構成プロファイルに変更することはできません。構成プロファイルの情報を変更する場合は、配信済みの構成プロファイルを変更するか、Wi-Fi を使用して他の構成プロファイルを配信してください。

◆画面（構成する APN のタイプ：デフォルト APN）

表示操作　［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［モバイル通信設定］→［新規作成］または［編集］



項番	項目	説明
1	構成する APN のタイプ	「デフォルト APN」を選択します。
2	デフォルト APN 名	デフォルト APN の名称を 255 文字以内の半角英数字と記号で入力してください。
3	デフォルト APN の認証タイプ	以下の項目から選択します。 ●「PAP」、「CHAP」
4	デフォルト APN のユーザ名	デフォルト APN のユーザー名称を 255 文字以内の半角英数字と記号で入力してください。
5	デフォルト APN のパスワード	デフォルト APN のパスワードを 255 文字以内の半角英数字と記号で入力してください。

項番	項目	説明
6	デフォルトAPN対応IPバージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」

◆画面（構成する APN のタイプ：データ APN）

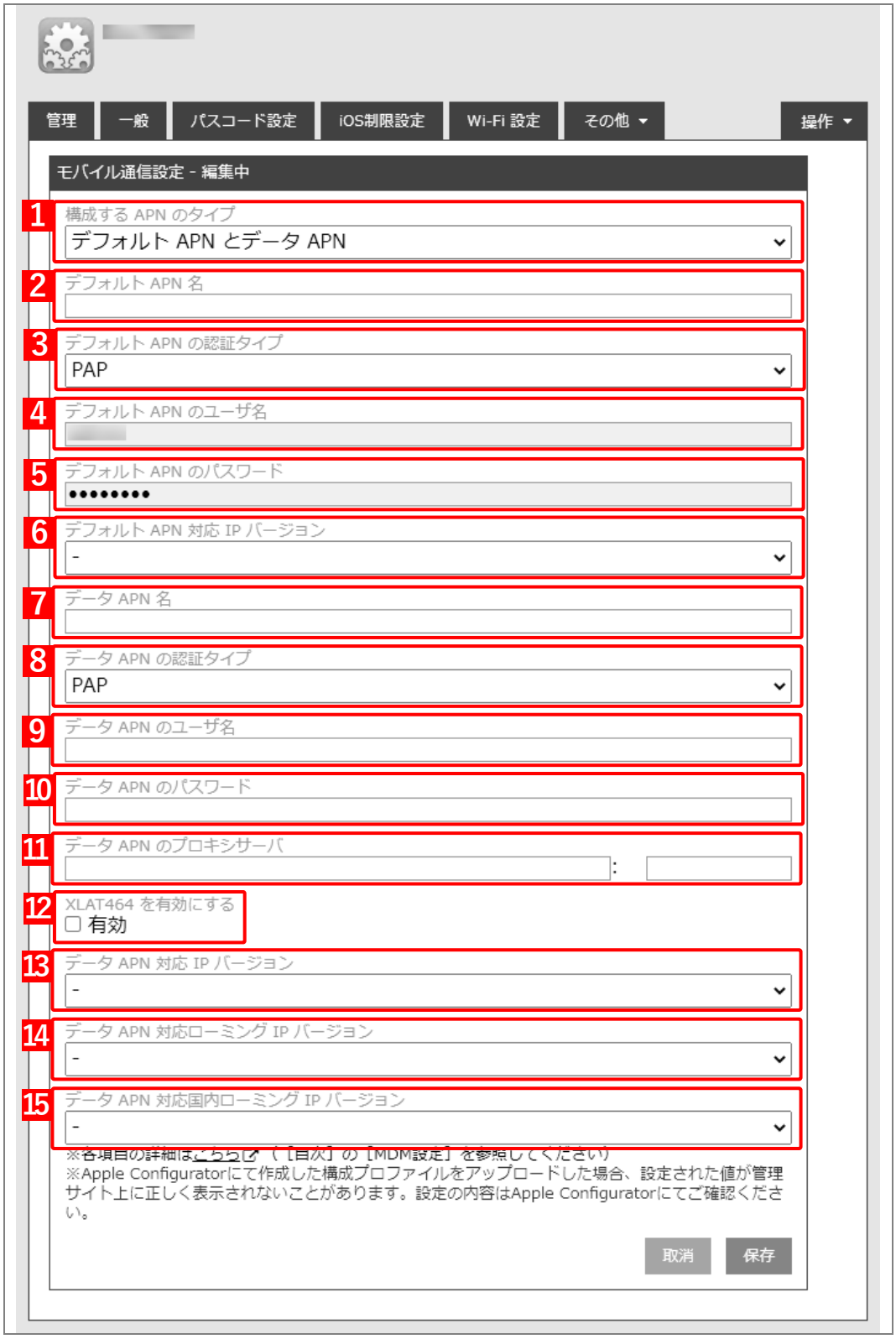
表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［モバイル通信設定］→［新規作成］または［編集］**

項番	項目	説明
1	構成する APN のタイプ	「データ APN」を選択します。
2	データ APN 名	データ APN の名称を 255 文字以内の半角英数字と記号で入力してください。
3	データ APN の認証タイプ	以下の項目から選択します。 ●「PAP」、「CHAP」
4	データ APN のユーザ名	データ APN のユーザー名称を 255 文字以内の半角英数字と記号で入力してください。

項番	項目	説明
5	データ APN のパスワード	データ APN のパスワードを 255 文字以内の半角英数字と記号で入力してください。
6	データ APN のプロキシサーバ	データ APN のプロキシサーバーを 255 文字以内の半角英数字と記号で入力してください。 ポート番号は 0 以上 65535 以下を半角数字で入力してください。
7	XLAT464 を有効にする	●有効 XLAT464 を有効にする場合は、「有効」にチェックを入れます。
8	データ APN 対応 IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」
9	データ APN 対応ローミング IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」
10	データ APN 対応国内ローミング IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」

◆画面（構成する APN のタイプ：デフォルト APN とデータ APN）

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］タブ→［モバイル通信設定］→［新規作成］または［編集］**



項番	項目	説明
1	構成する APN のタイプ	「デフォルト APN とデータ APN」を選択します。
2	デフォルト APN 名	デフォルト APN の名称を 255 文字以内の半角英数字と記号で入力してください。

項番	項目	説明
3	デフォルト APN の認証タイプ	以下の項目から選択します。 ●「PAP」、「CHAP」
4	デフォルト APN のユーザ名	デフォルト APN のユーザー名称を 255 文字以内の半角英数字と記号で入力してください。
5	デフォルト APN のパスワード	デフォルト APN のパスワードを 255 文字以内の半角英数字と記号で入力してください。
6	デフォルト APN 対応 IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」
7	データ APN 名	データ APN の名称を 255 文字以内の半角英数字と記号で入力してください。
8	データ APN の認証タイプ	以下の項目から選択します。 ●「PAP」、「CHAP」
9	データ APN のユーザ名	データ APN のユーザー名称を 255 文字以内の半角英数字と記号で入力してください。
10	データ APN のパスワード	データ APN のパスワードを 255 文字以内の半角英数字と記号で入力してください。
11	データ APN のプロキシサーバ	データ APN のプロキシサーバーを 255 文字以内の半角英数字と記号で入力してください。 ポート番号は 0 以上 65535 以下を半角数字で入力してください。
12	XLAT464 を有効にする	●有効 XLAT464 を有効にする場合は、「有効」にチェックを入れます。
13	データ APN 対応 IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」
14	データ APN 対応ローミング IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」
15	データ APN 対応国内ローミング IP バージョン	以下の項目から選択します。 ●「-」、「IPv4」、「IPv6」、「IPv4 と IPv6」

8.3.1.19 ［その他▼］タブ／ロック画面のメッセージ

ロック画面のメッセージに関する各種の設定を行います。

◆画面

表示操作 ［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［ロック画面のメッセージ］→［新規作成］または［編集］

項番	項目	説明
1	メッセージ	端末のロック画面の下部に表示するメッセージを 255 字以内で入力します。 特殊文字は使用できません。 長文の場合、端末によっては見切れて表示される場合もあります。
2	管理タグ情報	端末のロック画面の下部に表示する管理タグの情報を 255 字以内で入力します。 特殊文字は使用できません。 長文の場合、端末によっては見切れて表示される場合もあります。

8.3.1.20 ［その他▼］タブ／変数項目と反映状況

本機能では、構成プロファイルに特定の変数が含まれている場合に、変数名と変数の件数を表示し、構成プロファイル内で特定の変数が使用されていることを確認できます。

構成プロファイル内の記述（値）を特定の変数に書き換えることで、使用できる外部サービスがあります。書き換えた構成プロファイルを各端末に配信することで、端末が保持している値に自動的に置き換わり、個々に配信する構成プロファイルを一括で設定することができます。

構成プロファイルをアップロードしていない場合や特定の変数が含まれていない場合は、0 件と表示されます。構成プロファイルのアップロードについては、以下を参照してください。

「［管理］タブ」393 ページ

変数を使用する場合は、テスト端末で変数が正しく置換されていることを確認してください。テスト端末で問題がなければ、すべての端末に設定してください。

◆画面

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイルアップロード］→一覧から対象を選択→［その他▼］→［変数項目と反映状況］**

項番	項目	説明
1	シリアル番号	構成プロファイルに含まれる「%SERIAL_NUMBER%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくシリアル番号に変換されます。
2	端末 GUID	構成プロファイルに含まれる「%DEVICE_GUID%」の件数が表示されます。 構成プロファイルを配信する端末に紐づく GUID に変換されます。

項番	項目	説明
3	ユーザーの姓名	構成プロファイルに含まれる「%USER_FULL_NAME%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくユーザーの姓とユーザーの名の間に半角スペースを入れた値に変換されます。
4	ユーザーの姓	構成プロファイルに含まれる「%USER_LAST_NAME%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくユーザーの姓に変換されます。
5	ユーザーの名	構成プロファイルに含まれる「%USER_FIRST_NAME%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくユーザーの名に変換されます。
6	ユーザーID	構成プロファイルに含まれる「%USER_ NAME%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくユーザーの ID に変換されます。
7	ユーザーEmail	構成プロファイルに含まれる「%USER_EMAIL%」の件数が表示されます。 構成プロファイルを配信する端末に紐づくユーザーのメールアドレスに変換されます。
8	機器名	構成プロファイルに含まれる「%DEVICE_NAME%」の件数が表示されます。 構成プロファイルを配信する端末に紐づく機器名に変換されます。

8.3.2 構成プロファイル

「構成プロファイルアップロード」で管理サイト上に作成した構成プロファイルを使用して、構成プロファイルの設定セットを作成します。

構成プロファイルアップロードについては、以下を参照してください。

☞「構成プロファイルアップロード」393 ページ

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

☞「(設定－iOS) 設定の割り当て」83 ページ
☞「全機器一括設定」200 ページ

設定セットは、最大 300 件まで作成できます。

◆画面

表示操作　**［設定］→［iOS］→［構成プロファイル］→［構成プロファイル］→＋（一覧から対象を選択→［編集］）**

項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	構成プロファイル	構成プロファイルを選択します。1 つの設定セットにつき、10 件まで登録できます。また、合わせて「削除防止」を設定します。チェックを入れて「削除禁止」に設定すると、インストールされたプロファイルを端末側で削除できなくなります。(端末の「設定」－「一般」－「プロファイル」の画面で、削除の操作ができなくなります。) 構成プロファイルのアップロード方法は、以下を参照してください。 ☞「構成プロファイルアップロード」393 ページ なお、削除防止を指定すると構成プロファイルのインストールに機器側の操作が必要となります。 をクリックすると、入力行が追加されます。 をクリックすると、入力行が削除されます。 「削除防止」を設定した場合は、構成プロファイルのインストール時に端末側での操作が必要になります。 ●プロファイル名 リストボックスを表示すると「構成プロファイルアップロード」で登録した構成プロファイルが表示されます。適用する構成プロファイルを指定してください。 ☞「構成プロファイルアップロード」393 ページ 本項目で指定したプロファイル名の順番は関係ありません。「構成プロファイルアップロード」で作成した順番で、端末に反映されます。 ●削除防止 (A) チェックボックスにチェックを入れると、以下の項目が指定できます。 ・削除禁止 構成プロファイルの削除を禁止することができます。 Apple Configurator 2 で初期化が必要となります。 ・パスワード パスワードは、255 文字以内の半角英数字と記号（「.」、「-」）で指定してください。指定することで、構成プロファイルの削除を禁止することができます。端末からパスワードを入力することで、構成プロファイルを削除することができます。 iOS 13.0 以上の場合は、監視対象端末のみパスワードの設定が有効です。 (A) チェックボックスにチェックを入れない（削除防止を設定しない）場合は、MDM 構成プロファイルに、構成プロファイルが含まれます。

◆構成プロファイルの削除方法

作成方法に応じた構成プロファイルの削除方法は、以下のとおりです。

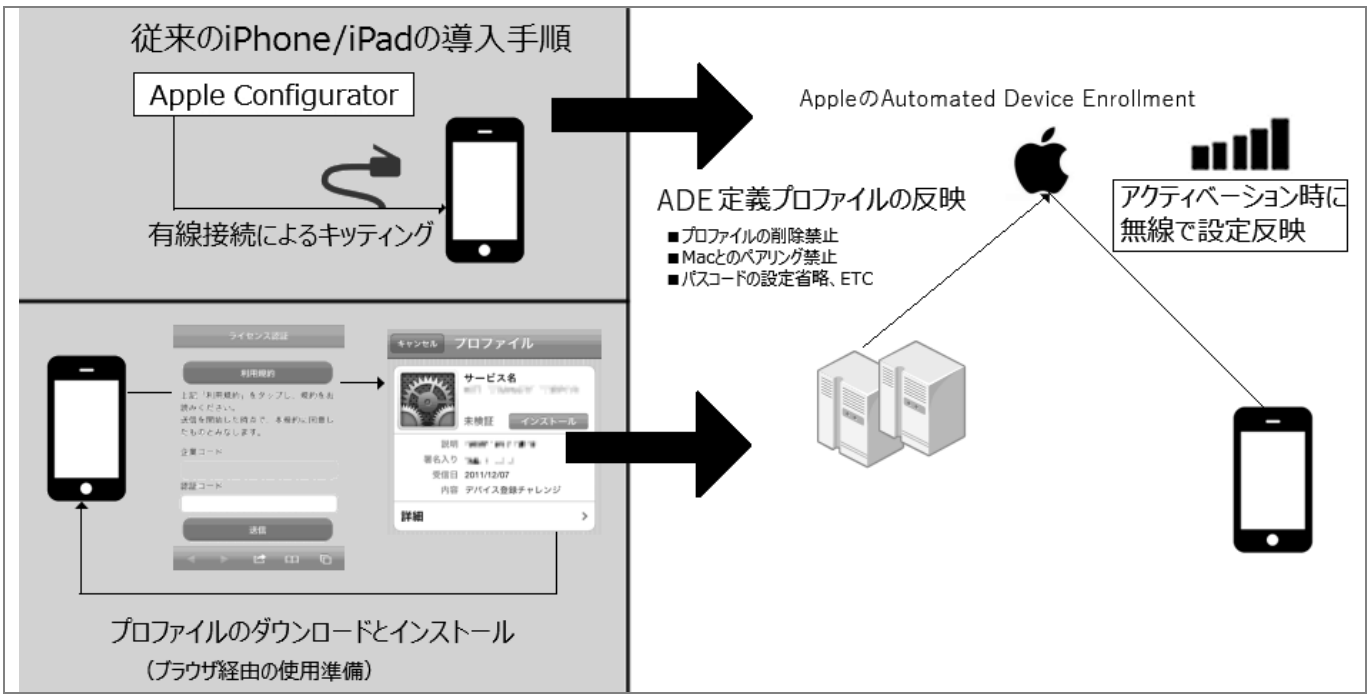
項番	項目	説明
1	通常の構成プロファイル（削除防止機能なし）	●機器一括設定または機器ごとの設定で「(設定なし)」を適用する。 ●機器から MDM 構成プロファイルを削除する（あわせて削除される)。 MDM 構成プロファイルは、iOS 端末のライセンス認証を行ったときにインストールされる構成プロファイルのことです。
2	削除禁止を指定した構成プロファイル	ワイプまたは Apple Configurator 2 で削除してください。
3	パスワードを指定した構成プロファイル	端末からパスワードを入力して削除する。

8.4 ADE

Automated Device Enrollment（ADE）とは、Apple Business Manager（ABM）によって提供されている iOS 端末管理のための機能です。

企業や教育機関用に iOS 端末を導入する場合に ADE を利用すると、関連する作業を簡略化できます。ADE の設定は、端末のアクティベーション時に Over-The-Air（無線通信経由）で反映されるため、端末に対して個別に行っていた煩雑な導入手順（Apple Configurator 2 を利用した有線接続によるアクティベーションや、プロファイルのインストール）が不要になります。また、より安全な端末管理ができる監視対象モードを利用したり、端末使用者が端末から MDM 構成プロファイルを削除することを禁止することもできます。

本設定では、ADE トークンの登録、ADE 定義プロファイル作成のほか、端末や ADE の情報管理などを行います。



8.4.1 ADE トークン登録

サーバー公開鍵証明書をダウンロード、ABM サイトへサーバー公開鍵証明書をアップロードして ADE トークンをダウンロード、ADE トークンの管理サイトへのアップロードまでを行います。

画面（新規登録）

画面（登録後）

詳細については、以下のマニュアルを参照してください。

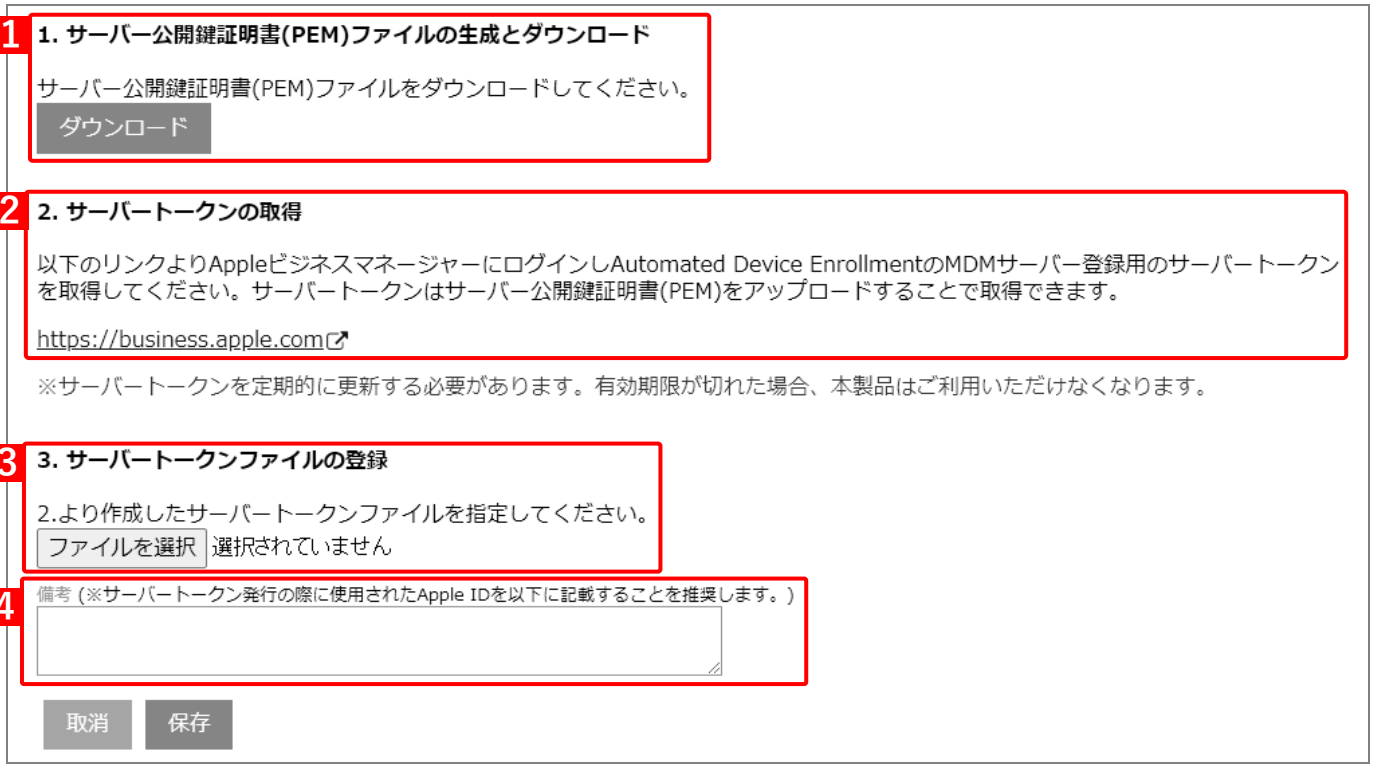
『iOS キッティングマニュアル』の「ADE を利用してライセンス認証を行う」

ダウンロードした ADE トークンは、速やかに管理サイトにアップロードしてください。アップロードせずに長時間経過すると、管理サイトとの通信ができなくなることがあります。詳細については、以下のマニュアルを参照してください。

『iOS キッティングマニュアル』の「ADE を利用してライセンス認証を行う」－「ADE を利用するための準備をする」－「ADE トークンを準備する」

◆画面（新規登録）

表示操作［設定］→［iOS］→［ADE］→［ADE トークン登録］→［編集］



項番	項目	説明
1	サーバー公開鍵証明書(PEM)ファイルの生成とダウンロード	［ダウンロード］をクリックして、サーバー公開鍵証明書（PEM）ファイルを入手します。
2	サーバートークンの取得	Apple の Apple Business Manager で MDM サーバー登録用のトークンを取得してください。トークンは、項番 1 の「サーバー公開鍵証明書(PEM)ファイルの生成とダウンロード」でダウンロードしたサーバー公開鍵証明書（PEM）をアップロードして取得できます。
3	サーバートークンファイルの登録	項番 2 の「サーバートークンの取得」で取得したサーバートークンを［ファイルを選択］をクリックして指定します。

項番	項目	説明
4	備考	ADE トークン取得時の Apple ID、および ADE トークン取得日の入力をお勧めします。 1 年ごとに ADE トークンを更新するときに、ADE トークン取得時の Apple ID が必要になります。ADE トークンの有効期限が切れると、本機能は利用できなくなるため、十分に注意してください。

◆画面（登録後）

表示操作　［設定］→［iOS］→［ADE］→［ADE トークン登録］

項番	項目	説明
1	［編集］	登録した内容を編集したい場合にクリックします。
2	［トークンを削除］	現在登録されている ADE トークンを削除します。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。
3	［ADE 機器再読込］	ADE 機器を再読み込みします。これにより、ADE トークンの情報や現在割り当てられている端末数など、ADE ライセンスに関連する情報がすべて更新されます。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 ライセンス情報の更新は、通常の ADE 機器管理画面で［ADE と同期］が使用されますが、このボタンは前回から変更された情報しか取得しないため、ADE ライセンス設定画面の内容と実際のライセンス割り当て状況の間に誤差が発生してしまう場合があります。この場合は、［ADE 機器再読込］を使用して ADE 機器情報を更新してください。 再読み込みの処理は管理サイトの通信負荷を増大させる原因となるため、必要な場合のみ実行してください。

8.4.2 ADE 定義プロファイル

ADE を利用する端末に対してさまざまな設定を適用するために、それらをまとめた ADE 定義プロファイルの設定セットを作成します。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

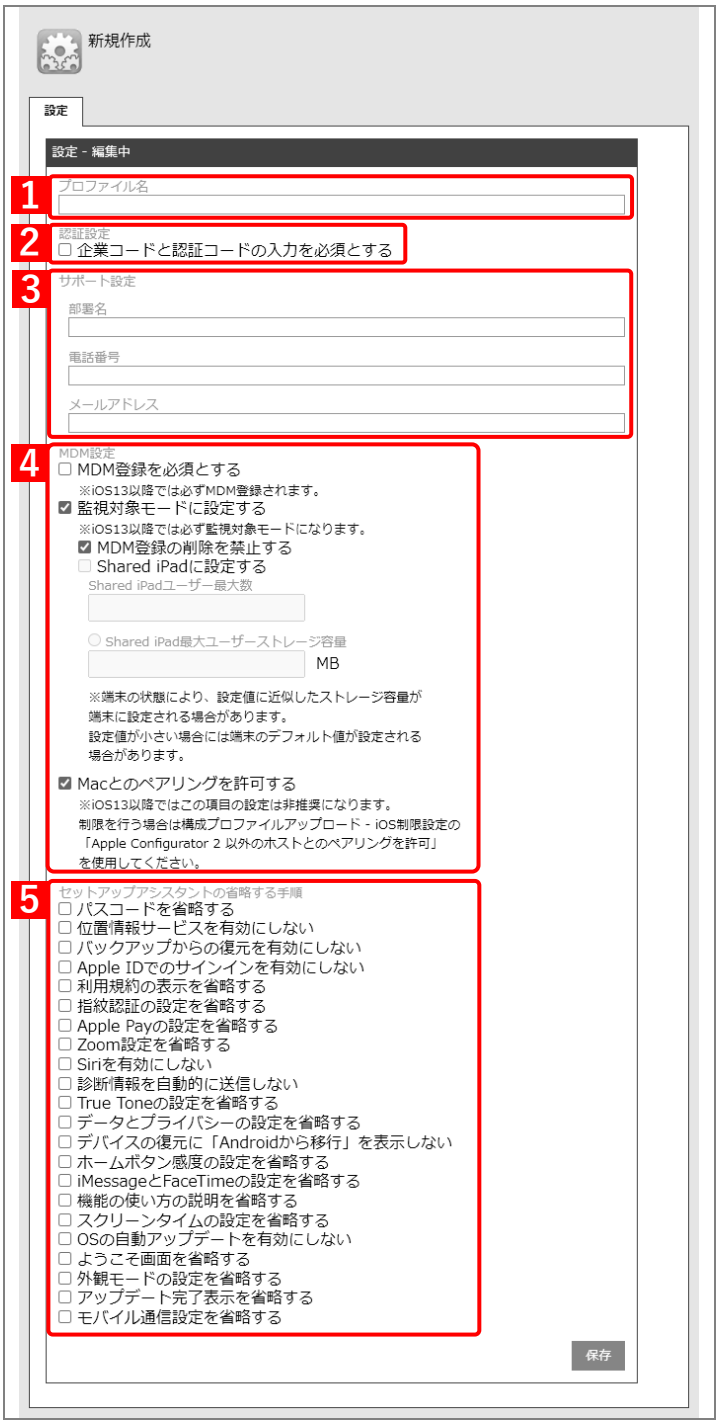
「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［iOS］→［ADE］→［ADE 定義プロファイル］→ ＋



項番	項目	説明
1	プロファイル名	ADE 定義プロファイルの名前を入力します。
2	認証設定	●企業コードと認証コードの入力を必須とする ユーザーに企業コードと認証コードを入力するように要求します。 チェックが入っていない場合は、ADE による自動設定が行われます。
3	サポート設定	●部署名 プロファイルに含まれる部署名を入力します。 ●電話番号 プロファイルに含まれる電話番号を入力します。 ●メールアドレス プロファイルに含まれるメールアドレスを入力します。 「部署名」はアクティベーション中の iOS 端末にのみ表示され、アクティベーション完了後に確認することはできません。
4	MDM 設定	●MDM 登録を必須とする チェックを入れると iOS 端末の初期設定時に MDM 構成プロファイルのインストールが必須になります。 iOS 13.0 以上の端末では、チェックを入れなくても必ず MDM 構成プロファイルがインストール（ライセンス認証）されます。 ●監視対象モードに設定する MDM 構成プロファイルにより、iOS 端末が「監視対象」になります。これにより、AirDrop、iMessage、Apple Books などの許可設定やコンテンツフィルタ設定などの幅広い設定を適用して管理できるようになります。 iOS 13.0 以上の端末では、チェックを入れなくても必ず監視対象モードになります。 ・MDM 登録の削除を禁止する 端末利用者による MDM 構成プロファイルの削除を禁止します。 「監視対象モードに設定する」にチェックが入っていない場合は、本設定にチェックを入れることはできません。 この設定を有効にしたとき、以下の状態になると MDM サーバーとの通信および再認証ができなくなります。その場合、再度端末を管理できるようにするには、端末を初期化する必要があります。 ・管理サイトで端末が削除されている。 ・MDM 構成プロファイルが同期不可になっている。 初期化を禁止している場合は、端末を工場出荷時の状態に戻す必要があります。この方法については、Apple へ問い合わせてください。 誤った HTTP プロキシ設定が端末にインストールされている場合は、通信ができなくなる可能性があります。 Apple Configurator 2 で ABM に追加したとき、Apple の仕様で 30 日の暫定期間は、端末から MDM を削除することができます。端末には「リモートマネージメントから離れる」と表示されます。 ・Shared iPad に設定する 端末を Shared iPad（共有 iPad）に設定します。 「MDM 登録を必須とする」と「監視対象モードに設定する」の両方にチェックが入っていない場合は、本設定にチェックを入れることはできません。 「Shared iPad ユーザー最大数」は、本製品の仕様では 50,000 です。ただし、端末の仕様により 50,000 以下になることがあります。 「Shared iPad 最大ユーザーストレージ容量」は、本製品の仕様で 1 メガバイト以上で設定します。端末の状態によっては設定値に近いストレージ容量が設定される場合があります。また、設定値が小さいと端末のデフォルト値が設定される場合があります。 ●Mac とのペアリングを許可する iOS 端末と Mac OS 端末とのペアリングができるようになります。 iOS 13 以上の端末では、本設定は非推奨です。「構成プロファイルアップロード」－「iOS 制限設定」－「機能の制限」の「Configurator 以外のホストとのペアリングを許可(監視対象のみ)」を使用してください。詳細は、以

項番	項目	説明
		下を参照してください。 ☞「画面（機能の制限）」400 ページ この設定にチェックが入っていない場合は、Apple の仕様により Windows 端末に接続できません。
5	セットアップアシスタントの省略する手順	●パスコードを省略する 初期設定時のパスコード設定が省略されます。 ●パスコード設定を省略する場合は、「Apple Pay の設定を省略する」、および「指紋認証の設定を省略する」を有効にしてください。 ●iCloud から復元する場合は、パスコード設定は省略されません。 ●位置情報サービスを有効にしない 位置情報サービスが自動的に無効になります。設定画面もスキップされます。 ●設定画面をスキップするには、初期設定時に Wi-Fi 接続を使用してください。 モバイルデータ通信を使用している場合は、設定画面が表示されることがあります。 ●バックアップからの復元を有効にしない バックアップからの復元が自動的に無効になります。設定画面もスキップされます。 ●設定画面をスキップするには、初期設定時に Wi-Fi 接続を使用してください。 モバイルデータ通信を使用している場合は、設定画面が表示されることがあります。 ●Apple ID でのサインインを有効にしない Apple ID でのサインインが自動的に無効になります。設定画面もスキップされます。 ●利用規約の表示を省略する 初期設定時の利用規約表示が省略されます。 ●指紋認証の設定を省略する 初期設定時の指紋認証設定が省略されます。 ●指紋認証設定を省略する場合は、「Apple Pay の設定を省略する」も有効にしてください。 ●iCloud から復元する場合は、指紋認証設定は省略されません。 ●Apple Pay の設定を省略する 初期設定時の Apple Pay 設定が省略されます。 ●Zoom 設定を省略する 初期設定時の Zoom 設定が省略されます。 ●Siri を有効にしない Siri が自動的に無効になります。設定画面もスキップされます。 ●診断情報を自動的に送信しない 診断情報の自動送付が無効になります。設定画面もスキップされます。 ●True Tone の設定を省略する True Tone の設定が自動的に有効になります。設定画面もスキップされます。 ●データとプライバシーの設定を省略する データとプライバシーの設定が自動的に有効になります。設定画面もスキップされます。 ●デバイスの復元に「Android から移行」を表示しない バックアップから復元画面で、「Android から移行」が表示されず、選択できなくなります。 ●ホームボタン感度の設定を省略する ホームボタン感度の設定が省略されます。 ●iMessage と FaceTime の設定を省略する iMessage と FaceTime の設定が省略されます。 ●機能の使い方の説明を省略する 機能の使い方の説明が省略されます。 ●スクリーンタイムの設定を省略する スクリーンタイムの設定が省略されます。 ●OS の自動アップデートを有効にしない

項番	項目	説明
		OS の自動アップデートの設定が省略されます。 自動アップデートの設定は、端末により異なります。 ●ようこそ画面を省略する ようこそ画面が省略されます。 ●外観モードの設定を省略する 外観モードの設定が省略されます。 ●アップデート完了表示を省略する ソフトウェアのアップデートが完了したとき、完了表示が省略されます。 ●モバイル通信設定を省略する モバイル通信設定が省略されます。 初期設定時に App とデータ画面で「Android からデータを移行」を選択した場合、設定画面はスキップされません。

◆エラー一覧

文言	発生契機	対処方法
⚠ADE との通信に失敗しました。 もう一度やり直してください。	ADE のトークン更新時に、Apple サーバーとの通信で負荷が高い、認証が通らないなど、何らかのエラーが発生している。	時間をおいて再度実施してください。

8.4.3 ADE 機器管理

機器情報、登録情報、ADE 情報を確認することができます。

また、ADE 定義プロファイルの設定を組織や機器に割り当てたあとに［ADE と同期］をクリックすると、管理対象の端末に ADE 設定を反映することができます。

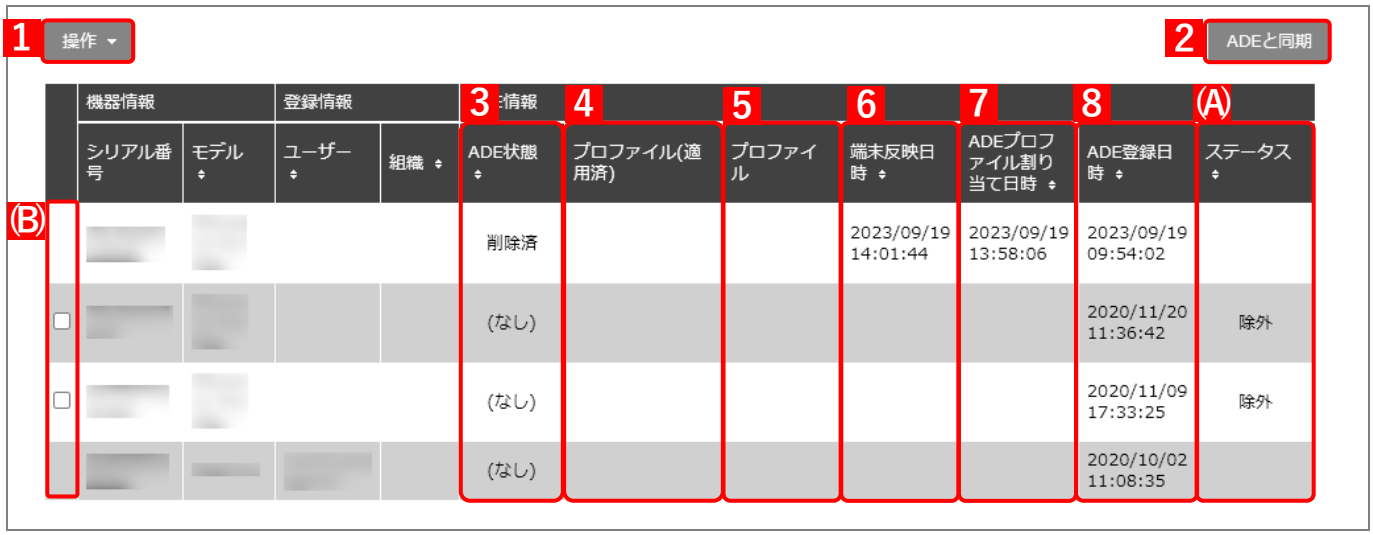
- ADE 機器管理画面の情報（ADE 状態、プロファイル（適用済）、プロファイル、端末反映日時）は、［機器］の詳細画面で同期を行っても更新されません。［ADE と同期］をクリックして同期を実行してください。
- iOS 端末の初期設定を開始する前に、該当端末の「ADE 状態」が「適用済」または「端末反映済」になっていることを確認してください。このステータス以外の場合はプロファイルの設定が正しく反映されません。
- iPhone モデルは、機器管理画面では「iPhone_U」と表示されます。
- 登録日時、端末反映日時は日本標準時（JST）で記録されます。
- ADE 機器を購入すると、ライセンス認証待ち機器として機器一覧に表示されます。管理外にしたい機器は、ライセンス認証前であれば、本画面で除外にします。除外にした ADE 機器は、機器一覧に表示されません。
  機器一覧については、以下を参照してください。
  「機器一覧」54 ページ

ADE 機器を利用するには、Apple Push 証明書が必要です。

『Apple Push 証明書年次更新マニュアル』

◆画面

表示操作　［設定］→［iOS］→［ADE］→［ADE 機器管理］



項番	項目	説明
1	［操作］	ライセンス認証前の ADE 機器を管理外機器にできます。 クリックすると、以下のメニューが表示されます。 ●全てにチェックを入れる すべてのチェックボックスにチェックが入ります。 ●全てのチェックをはずす すべてのチェックボックスからチェックを外します。 ●除外 管理外機器にする ADE 機器を除外します。(A) ステータスに「除外」と表示されます。 以下の場合も（A）ステータスに「除外」と表示されます。 ・機器一覧で削除した機器 「画面（一括削除)」57 ページ 「機器の個別削除」73 ページ ・「CSV で削除」で削除した機器 ・機器ライセンス数が上限に達している状態で、新規で追加した機器 ●除外解除 除外を解除します。(A) ステータスは空白になります。 （B）チェックボックスは、以下の場合に表示されます。 ・ライセンス認証待ち機器 ・機器一覧で削除した機器 「画面（一括削除)」57 ページ 「機器の個別削除」73 ページ ・「CSV で削除」で削除した機器 ・機器ライセンス数が上限に達している状態で、新規で追加した機器
2	［ADE と同期］または［ADE から機器情報を取得］	ADE と同期します。ログインしているユーザー種別によって、表示されるボタン名、処理が異なります。 ・ユーザー種別が管理者および操作の場合 ［ADE と同期］と表示されます。 ADE サーバーから ADE トークンに紐づいている機器一覧の差分を取得します。また、ADE 定義プロファイル（適用済）と ADE 定義プロファイルが異なる機器について、ADE 定義プロファイルを ADE 機器に紐づける処理を行います。 ・ユーザー種別が閲覧者の場合 ［ADE から機器情報を取得］と表示されます。 ADE サーバーから ADE トークンに紐づいている機器一覧の差分を取得します。
3	ADE 状態	●なし ADE 適用前の状態です。 次回の端末初期設定時は通常のアクティベーションとなります。 ●適用済 ADE にプロファイルが登録された状態です。 次回の端末初期設定時にプロファイルの設定が適用されます。 ●削除済 ADE からプロファイルが削除された状態です。ステータスを「適用済」に戻すには、ADE 定義プロファイルを再度割り当て、［ADE と同期］を実行してください。ステータスが「適用済」に移行したら、端末のアクティベーションが完了次第「端末反映済」に移行します。 次回の端末初期設定時は通常のアクティベーションとなります。 ●端末反映済 ADE にプロファイルが登録され、端末のアクティベーションも完了している状態です。 次回の端末初期設定時にプロファイルの設定が適用されます。

項番	項目	説明
4	プロファイル(適用済)	ADE 機器に「ADE 定義プロファイル」を割り当てたあと、項番 2［ADE と同期］を実行すると、割り当てた「ADE 定義プロファイル」のプロファイル名が表示されます。項番 3「ADE 状態」は「適用済」になります。 設定の割り当てについては、以下を参照してください。 「（設定－iOS）設定の割り当て」83 ページ
5	プロファイル	ADE 機器に「ADE 定義プロファイル」を割り当てると、割り当てた「ADE 定義プロファイル」のプロファイル名が表示されます。 設定の割り当てについては、以下を参照してください。 「（設定－iOS）設定の割り当て」83 ページ
6	ADE 登録日時	ABM で ADE 機器のシリアル番号を MDM サーバーに割り当てが完了した日時が、項番 2［ADE と同期］を実行すると表示されます。 MDM サーバーへの割り当てについては、以下を参照してください。 『iOS キッティングマニュアル』の「ADE を利用してライセンス認証を行う」－「ADE を利用するための準備をする」－「ABM で端末をサーバーに割り当てる」
7	ADE プロファイル割り当て日時	ABM が ADE 機器にプロファイルを割り当てた日時が、項番 2［ADE と同期］を実行すると表示されます。
8	端末反映日時	ABM で ADE 機器のアクティベーションが完了した日時が、項番 2［ADE と同期］を実行すると表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠ 除外対象となる機器がありません。	ADE 機器管理ですでに「除外」のステータスになっているときに「除外」の操作を行っている。	すでに除外されている機器に対して「除外」の操作を行わないでください。
⚠ 除外解除対象となる機器がありません。	ADE 機器管理でチェックボックスにチェックを入れた機器が、すでに認証待ち機器として表示されているときに「除外解除」の操作を行っている。	すでに除外されている機器に対して「除外」の操作を行わないでください。
⚠ ライセンスが不足しているため、一部の機器の除外解除に失敗しました。	機器ライセンスが上限に達している状態で「除外解除」の操作を行っている。	登録できる機器ライセンス数を増やす、もしくは不要な機器を削除してライセンス数を確保したうえで「除外解除」の操作を行ってください。
⚠ ADE との同期を行いましたが、一部の機器へのプロファイル割り当てまたは割り当ての解除に失敗しました。	［ADE と同期］をクリックした際に、Apple サーバーとの通信で ADE 定義プロファイルの割り当てもしくは削除が失敗している。 ［ADE と同期］をクリックした際に、Apple サーバーへのアクセス許可が得られていない。	ABM 上でデバイスが正しく割り当たっていることを確認のうえ、時間をおいて再度［ADE と同期］をクリックしてください。 それでも改善しない場合は Apple に問い合わせてください。

8.5 Shared iPad セキュリティ

Shared iPad（共有 iPad）端末として設定した場合、ユーザーログイン後のセキュリティーに関する設定セットを作成します。

本設定は、Shared iPad（共有 iPad）に設定された iPad 端末のみ有効です。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

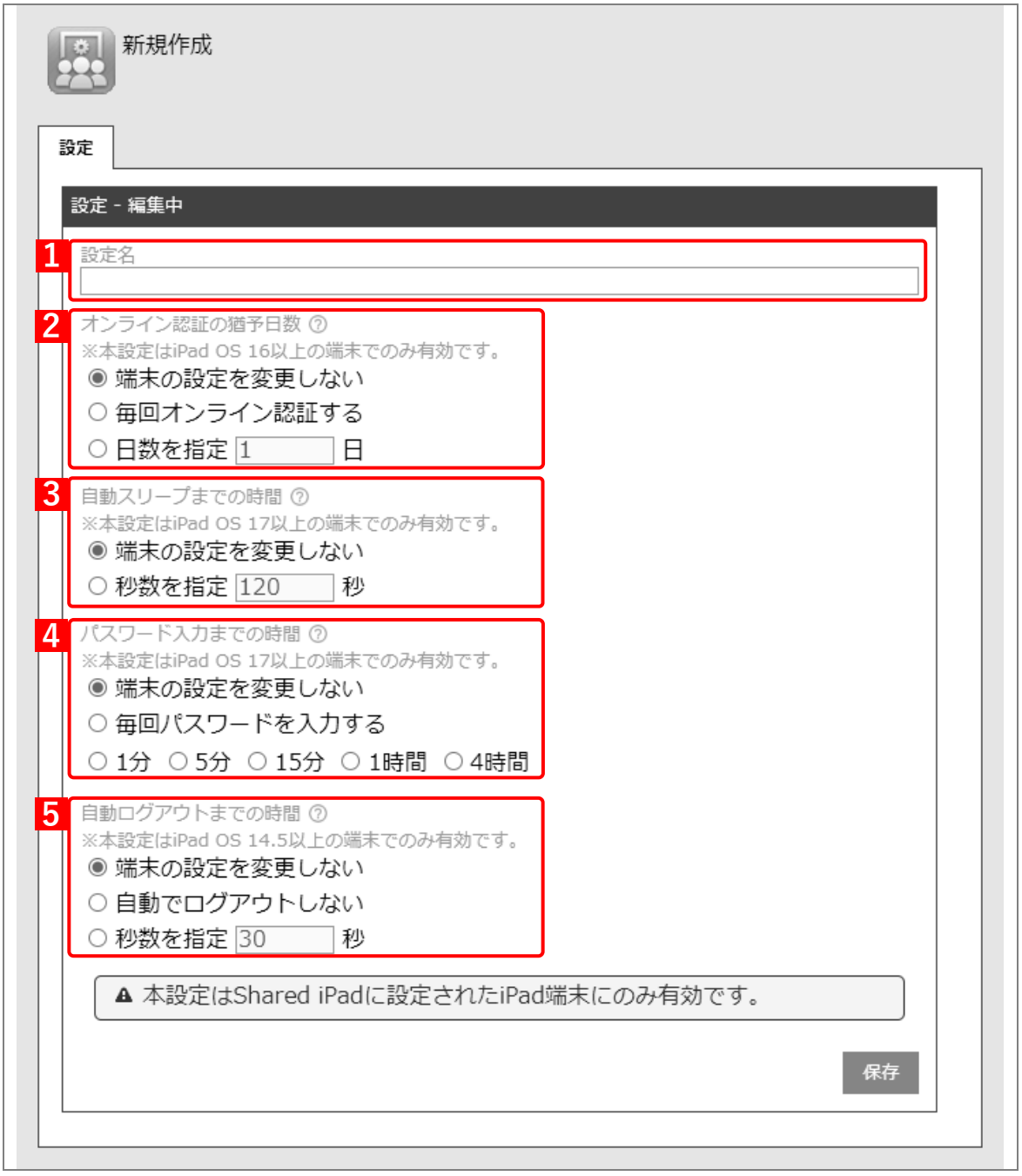
「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［iOS］→［Shared iPad セキュリティ］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で指定します。
2	オンライン認証の猶予日数	前回のオンライン認証から指定した日数が経過すると、Apple へオンライン認証します。猶予日数の設定を以下から選択します。 iPad OS 16.0 以上の端末で有効です。 ●［端末の設定を変更しない］ 現在の設定を変更しません。 ●［毎回オンライン認証する］ ログイン時、毎回 Apple の ID サーバーとオンライン認証します。 管理対象 AppleID のパスワードをリセットした場合、次回ログイン時は新しいパスワードで認証します。 ●［日数を指定○日］ 前回のオンライン認証後、Apple の ID サーバーへのオンライン認証が必要になるまでの日数を 1 から 2147483647 までの整数を入力します。 管理対象 AppleID のパスワードをリセットした場合に、前回のオンライン認証から指定した日数が経過するまではリセット前のパスワードでログインができます。
3	自動スリープまでの時間	端末がアイドル状態から指定した秒数が経過すると、スリープに移行します。自動スリープまでの設定を以下から選択します。 iPad OS 17.0 以上の端末で有効です。 ●［端末の設定を変更しない］ 現在の設定を変更しません。 ●［秒数を指定○秒］ 端末を操作しない状態が続いた場合、端末をスリープ状態にするまでの秒数を 120 から 2147483647 までの整数で入力します。
4	パスワード入力までの時間	端末がスリープ状態から指定した時間が経過すると、パスワードを入力します。パスワード入力の設定を以下から選択します。 iPad OS 17.0 以上の端末で有効です。 ●［端末の設定を変更しない］ 現在の設定を変更しません。 ●［毎回パスワードを入力する］ 端末がスリープ状態になった場合、復帰したとき必ずパスワードを入力します。 ●［1 分］ ●［5 分］ ●［15 分］ ●［1 時間］ ●［4 時間］ ［1 分］～［4 時間］を選択して端末がスリープ状態になった場合、選択した時間が経過後にパスワードを入力します。
5	自動ログアウトまでの時間	端末が非アクティブ状態から指定した時間が経過すると、自動でログアウトします。自動ログアウトの設定を以下から選択します。 iPad OS 14.5 以上の端末で有効です。 ●［端末の設定を変更しない］ 現在の設定を変更しません。 ●［自動でログアウトしない］ 端末を操作しない状態が続いた場合でもユーザーログアウトしません。 ●［秒数を指定○秒］ 端末を操作しない状態が続いた場合、自動でユーザーログアウトするまでの秒数を 30 から 2147483647 までの整数で入力します。

8.6 アプリケーション

iOS 端末のアプリに関連する設定、および設定セットを作成します。本機能では、App Store のアプリや書籍のライセンス管理、アプリの配信、端末にインストールされた特定のアプリの検知などを行います。また、「アプリケーション配信」、「アプリケーション検知」は、作成した設定セットを、個別または複数の端末に一括で割り当てることができます。

8.6.1 「App とブック」ライセンス

Apple が提供する「App とブック」を利用して、「App とブック」場所のトークンを管理サイトにアップロードし、「App とブック」ライセンス設定として保存すると、App Store のアプリや書籍のライセンスを管理することができます。

「App とブック」場所のトークンに記録されたライセンス情報は、指定した「App とブック」ライセンス設定に紐づけられて管理されます。

本設定では、管理サイトと「App とブック」場所のトークンの紐づけや、アプリと書籍のライセンス残数、付与状況の確認を行うことができます。

- 「App とブック」ライセンスを管理するには、ABM から「App とブック」場所のトークンをダウンロードしてください。
- 「App とブック」場所のトークンの詳細については、Apple の「App とブック」に関する情報を参照してください。
- 端末への「App とブック」ライセンスの割り当ては、iOS 9.0 以上の端末に対応しています。iOS 9.0 以下の端末にライセンスを割り当てても、「App とブック」のアプリおよび書籍は配信できません。
- 「App とブック」の書籍は、ユーザーにのみ配信でき、端末には配信できません。書籍を配信する場合は、あらかじめユーザーと端末を紐づけてください。
- 「App とブック」場所のトークンは、500 件まで登録できます。
- 「App とブック」の利用に関連したその他の設定については、以下を参照してください。
  - 「「App とブック」設定テンプレート」520 ページ
  - 「管理対象アプリポリシー」523 ページ
  - 「アプリケーション配信」530 ページ
  - 「(設定－iOS)「App とブック」設定」100 ページ
  - 「[「App とブック」設定］タブ」262 ページ
  - 「[その他▼］タブ／「App とブック」」289 ページ
- 設定セットは、最大 500 件まで作成できます。

8.6.1.1 ［管理］タブ

「新規作成」画面では、「App とブック」場所のトークンを管理サイトにアップロードして紐づけを行い、「App とブック」ライセンス設定として保存します。

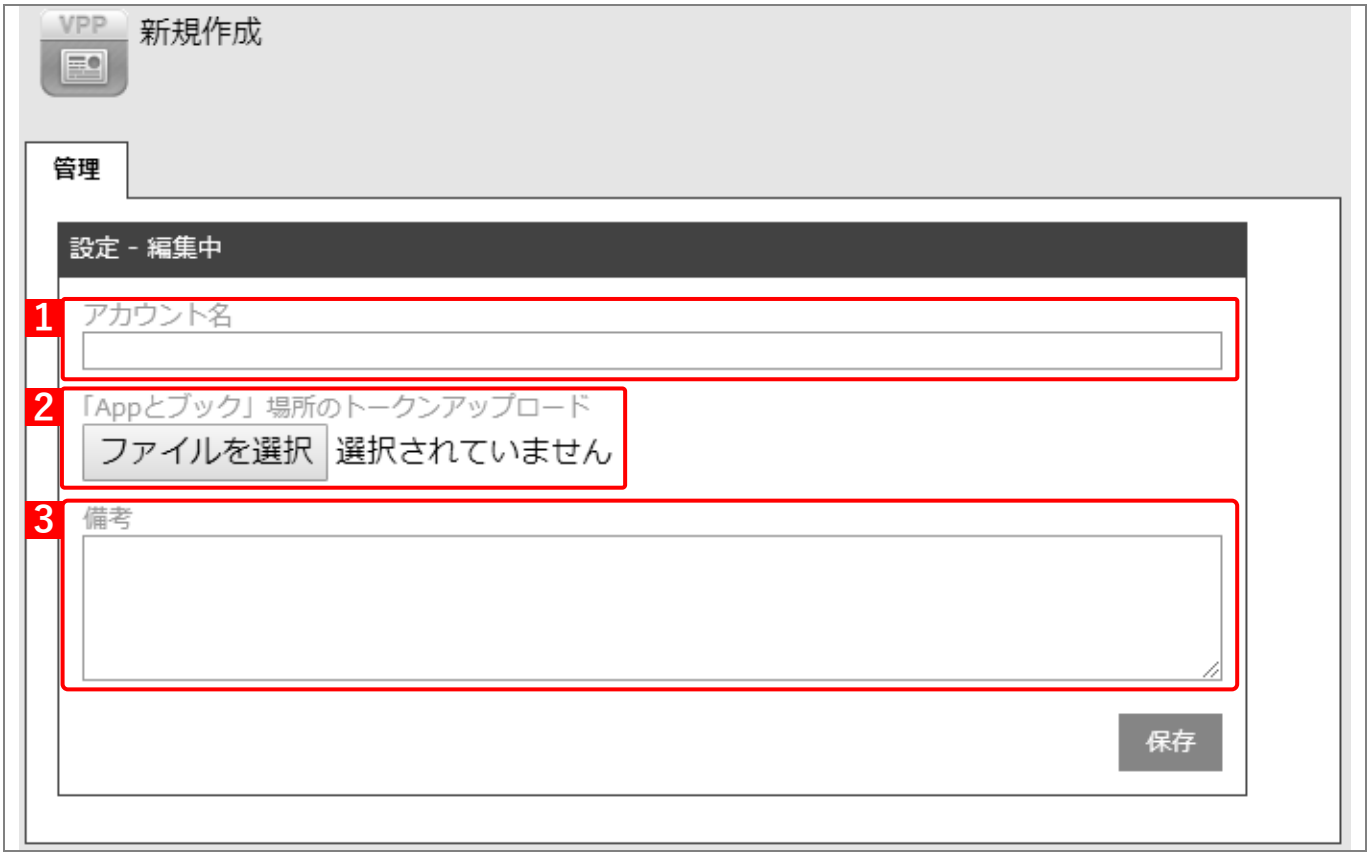
保存後の画面では、設定セットに紐づけされている「App とブック」ライセンスの情報が表示されます。必要に応じて、情報を編集することもできます。

画面（新規作成）

画面（編集）

◆画面（新規作成）

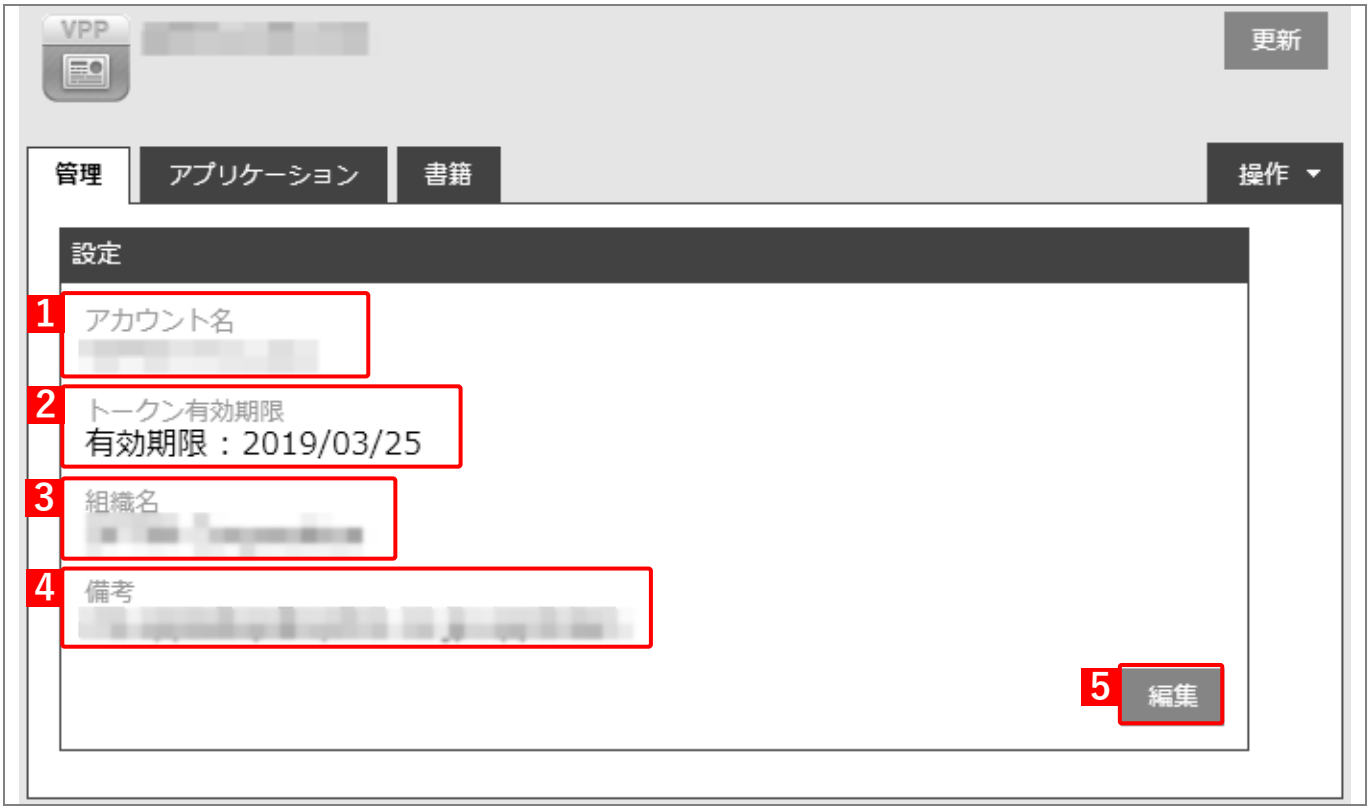
表示操作［設定］→［iOS］→［アプリケーション］→［「App とブック」ライセンス］→ ＋



項番	項目	説明
1	アカウント名	「App とブック」ライセンスに紐づけるアカウントの名称を 30 文字以内で指定します。設定内で重複はできません。
2	「App とブック」場所のトークンアップロード	［ファイルを選択］をクリックして、アップロードする「App とブック」場所のトークンを指定します。
3	備考	「App とブック」場所のトークンの取得に使用した Apple ID を入力します。200 文字以内で入力してください。

◆画面（編集）

表示操作　**［設定］→［iOS］→［アプリケーション］→［「App とブック」ライセンス］→一覧から対象を選択→［管理］タブ**



項番	項目	説明
1	アカウント名	「App とブック」ライセンスに紐づけられたアカウント名が表示されます。
2	トークン有効期限	「App とブック」場所のトークンの有効期限が表示されます。
3	組織名	「App とブック」場所のトークンに紐づけられた組織名が表示されます。
4	備考	「App とブック」ライセンス編集画面の「備考」に入力した情報が表示されます。
5	編集	「App とブック」ライセンスの情報を編集します。詳細については、以下を参照してください。 ☞「画面（新規作成）」515 ページ

◆エラー一覧

以下のエラー文言が表示されると、「「App とブック」場所のトークンアップロード」に［強制的にアップロードする］のチェックボックスが表示されます。

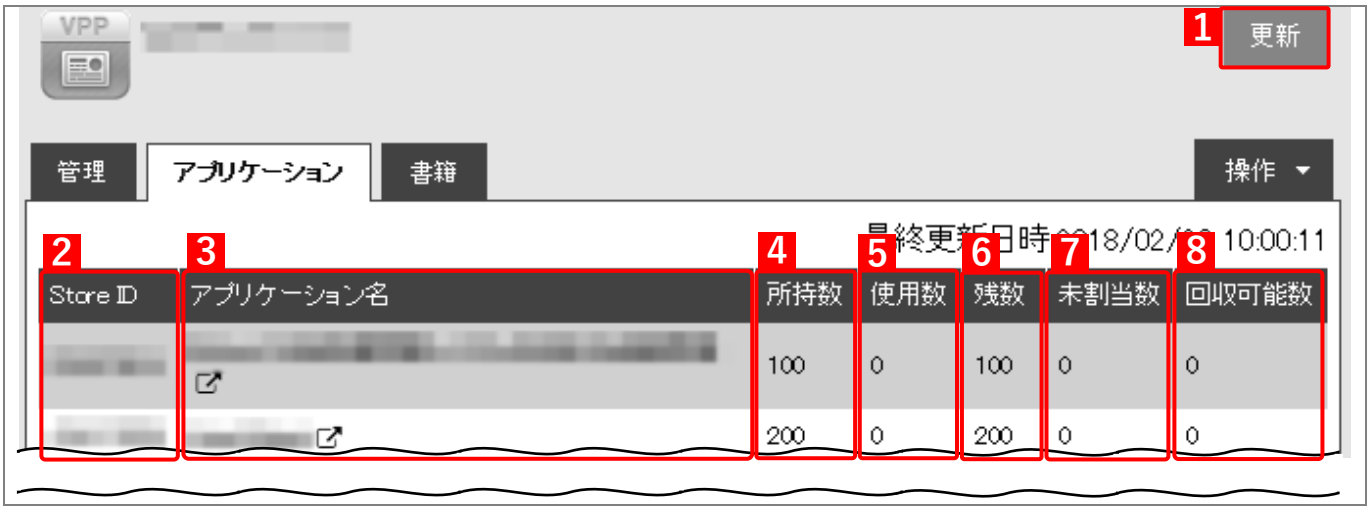
文言	発生契機	対処方法
⚠ このトークンは他のサービスで利用されています。このトークンを利用する場合、他のサービスで行われた設定の影響を受ける可能性があります。他のサービスでトークンの利用状況を確認した後、本サービスでこのトークンを利用することに同意する場合は「強制的にアップロードする」にチェックを入れて設定を保存してください。	「App とブック」場所のトークンが他のサービスで利用されている。	他のサービスでの「App とブック」場所のトークンの利用状況を確認してください。 ［強制的にアップロードする］にチェックを入れて、［保存］をクリックします。
⚠ トークンの有効期限が切れているため、現在使用している「App とブック」場所のトークンと同一のトークンであること、および他のサービスの利用状況が確認できませんでした。「App とブック」場所のトークンのダウンロード元の場所が一致しているか、また、他のサービスで利用していないかを確認したのち、本サービスでこのトークンを利用することに同意する場合は「強制的にアップロードする」にチェックを入れて設定を保存してください。	「App とブック」場所のトークンの有効期限が切れている。	「App とブック」場所のトークンのダウンロード元の場所が一致しているか、他のサービスでの利用していないかを確認してください。 ［強制的にアップロードする］にチェックを入れて、［保存］をクリックします。
⚠ 更新前のトークンが revoke されているため、現在使用している「App とブック」場所のトークンと同一のトークンであること、および他のサービスの利用状況が確認できませんでした。「App とブック」場所のトークンのダウンロード元の場所が一致しているか、また、他のサービスで利用していないかを確認した後、本サービスでこのトークンを利用することに同意する場合は「強制的にアップロードする」にチェックを入れて設定を保存してください。	「App とブック」場所のトークンが revoke されている。	「App とブック」場所のトークンのダウンロード元の場所が一致しているか、他のサービスでの利用していないかを確認してください。 ［強制的にアップロードする］にチェックを入れて、［保存］をクリックします。

8.6.1.2 ［アプリケーション］タブ

アプリ名、所持数など、ライセンスに含まれるアプリの情報を表示します。また、ライセンスが仮割当のユーザー（機器、組織を含む）にライセンスを割り当てたり、回収することもできます。

◆画面

表示操作 ［設定］→［iOS］→［アプリケーション］→［「App とブック」ライセンス］→一覧から対象を選択→［アプリケーション］タブ



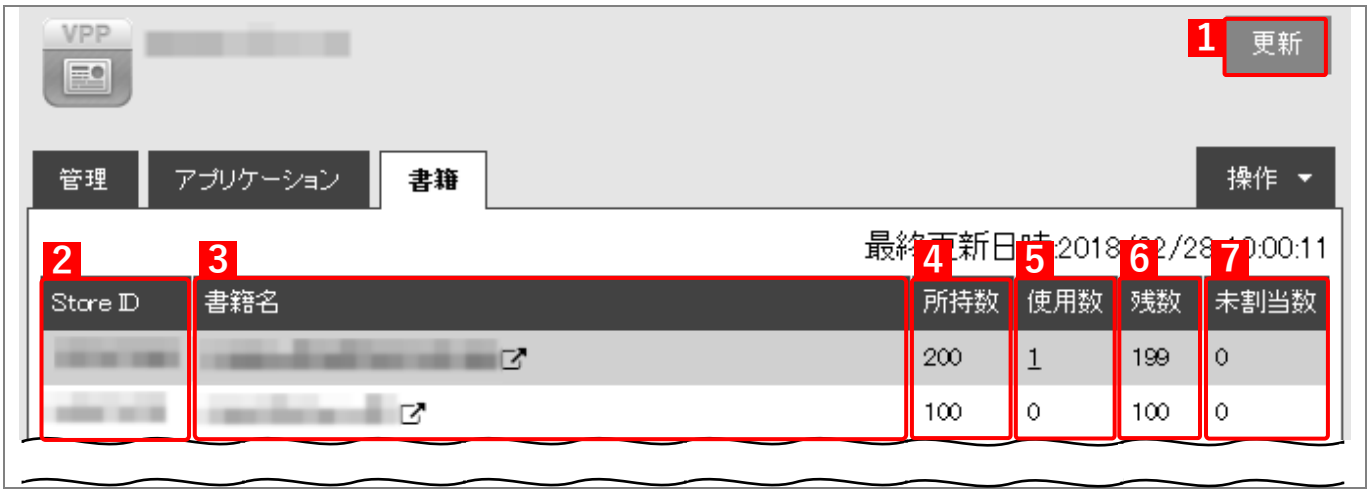
項番	項目	説明
1	［更新］	「App とブック」ライセンスの割り当て、回収、または同期を行います。「未割当数」としてカウントされているユーザーまたは端末に「App とブック」ライセンスが本割り当てされ、更新完了後に「使用数」のユーザーまたは端末としてカウントされます。また、「回収可能数」としてカウントされている「App とブック」ライセンスは回収（「App とブック」ライセンスの割り当てが解除）され、更新完了後に「残数」としてカウントされます。 Apple サーバーの処理状況によっては、情報の反映までに時間がかかる場合があります。反映されない場合は、時間をおいて再度［更新］をクリックしてください。
2	Store ID	アプリの Store ID が表示されます。
3	アプリケーション名	「App とブック」場所のトークンに含まれるアプリの名前が表示されます。
4	所持数	保有するライセンスの総数が表示されます。
5	使用数	保有するライセンスのうち、ユーザーまたは機器に割り当てられたライセンスの数が表示されます。使用数をクリックすると、使用数の内訳（ユーザー使用数、機器使用数）が表示されます。内訳のリンクから、該当ユーザー、該当機器の一覧を表示できます。
6	残数	保有ライセンスの数から、割り当て済みのライセンス数を除いた残数が表示されます。
7	未割当数	［ユーザー］、［機器］、および［組織］の［「App とブック」設定］タブから、ライセンスを仮割り当てされたユーザーの数が表示されます。項番 1 の［更新］をクリックして、ライセンスを本割り当てしてください。
8	回収可能数	［ユーザー］または［機器］や［組織］の［「App とブック」設定］タブから、削除されたライセンスの数が表示されます。項番 1 の［更新］をクリックして、ライセンスを回収してください。

8.6.1.3 ［書籍］タブ

書籍名、所持数など、ライセンスに含まれる書籍の情報が表示されます。また、ライセンスが仮割当のユーザーにライセンスを割り当てることもできます。

◆画面

表示操作 **［設定］→［iOS］→［アプリケーション］→［「App とブック」ライセンス］→一覧から対象を選択→［書籍］タブ**



項番	項目	説明
1	［更新］	「App とブック」ライセンスの割り当て、または同期を行います。「未割当数」としてカウントされているユーザーにライセンスが本割り当てされ、更新完了後に「使用数」のユーザーとしてカウントされます。 「App とブック」による書籍配信の場合は、管理者によって一度配布された書籍を削除したり、書籍のライセンスを回収したりすることはできません。特に有償の書籍については誤って配信しないように、配信先に十分に注意してください。 Apple サーバーの処理状況によっては、情報の反映までに時間がかかる場合があります。反映されない場合は、時間をおいて再度［更新］をクリックしてください。
2	Store ID	書籍の Store ID が表示されます。
3	書籍名	「App とブック」場所のトークンに含まれる書籍の名前が表示されます。
4	所持数	保有するライセンスの総数が表示されます。
5	使用数	保有するライセンスのうち、ユーザーに割り当てられたライセンスの数が表示されます。使用数をクリックすると、使用数の内訳（ユーザー使用数）が表示されます。内訳のリンクから、該当ユーザーの一覧を表示できます。
6	残数	保有ライセンスの数から、割り当て済みのライセンス数を除いた残数が表示されます。
7	未割当数	［ユーザー］の［「App とブック」設定］タブから、ライセンスを仮割り当てされたユーザーの数が表示されます。項番 1 の［更新］をクリックして、ライセンスを本割り当てしてください。

8.6.2 「App とブック」設定テンプレート

アプリや書籍の「App とブック」ライセンス設定を割り当てるための設定テンプレートを作成します。「App とブック」設定テンプレート利用すると、ユーザー、端末、または組織に対して「App とブック」ライセンスを簡単に割り当てることができます。

画面（［アプリケーション］選択時）

画面（［書籍］選択時）

「App とブック」設定テンプレートを作成するには、「App とブック」ライセンス設定を作成してください。

「「App とブック」ライセンス」514 ページ

「App とブック」の利用に関連したその他の設定については、以下を参照してください。

「管理対象アプリポリシー」523 ページ
「アプリケーション配信」530 ページ
「（設定－iOS）設定の割り当て」83 ページ
「［「App とブック」設定］タブ」262 ページ
「［その他▼］タブ／「App とブック」」289 ページ

「App とブック」設定テンプレートは、最大 50 件まで作成できます。

◆画面（［アプリケーション］選択時）

表示操作［設定］→［iOS］→［アプリケーション］→［「App とブック」設定テンプレート］→ ✚

項番	項目	説明
1	テンプレート名	設定セットの名称を 30 文字以内で指定します。設定内で重複はできません。
2	「App とブック」管理配布登録	●「App とブック」ライセンス 「「App とブック」ライセンス」で作成したアカウント名を指定します。 ☞「「App とブック」ライセンス」514 ページ
3	［アプリケーション］	App ライセンスを設定する場合に、クリックします。
4	［書籍］	ブックライセンスを設定する場合に、クリックします。
5	App ライセンス付与	●アプリケーション名 アプリをリストボックスから選択します。 ✚ をクリックすると、入力欄が追加されます。 ✖ をクリックすると、入力欄が削除されます。 「App とブック」ライセンスに登録しているアプリが設定できます。画面に表示される件数は、「App とブック」ライセンスに登録しているアプリの数です。 ABM で購入したアプリの件数が表示されます。アプリは最大 300 件まで購入できます。

◆画面（［書籍］選択時）

表示操作　［設定］→［iOS］→［アプリケーション］→［「App とブック」設定テンプレート］→ ＋ →［書籍］

項番	項目	説明
1	テンプレート名	設定セットの名称を 30 文字以内で指定します。設定内で重複はできません。
2	「App とブック」管理配布登録	●「App とブック」ライセンス 「「App とブック」ライセンス」で作成したアカウント名を指定します。 ☞「「App とブック」ライセンス」514 ページ
3	［アプリケーション］	App ライセンスを設定する場合に、クリックします。
4	［書籍］	ブックライセンスを設定する場合に、クリックします。
5	ブックライセンス付与	●書籍名 書籍をリストボックスから選択します。 ＋ をクリックすると、入力欄が追加されます。 × をクリックすると、入力欄が削除されます。 「App とブック」ライセンスに登録している書籍が設定できます。画面に表示される件数は、「App とブック」ライセンスに登録している書籍の数です。 ABM で購入した書籍の件数が表示されます。書籍は最大 300 件まで購入できます。

8.6.3 管理対象アプリポリシー

管理対象アプリに対して、目的に応じたより詳細な設定を行い、管理対象ポリシー設定として保存します。管理対象ポリシー設定は、以下のアプリケーション配信に利用できます。

●「App とブック」ライセンスを付与したアプリ

●自動的にアプリのバージョンアップを行いたいアプリ

iOS 端末で管理対象アプリポリシーの内容を確認することはできません。

「App とブック」の利用に関連したその他の設定については、以下を参照してください。

「「App とブック」設定テンプレート」520 ページ

「管理対象アプリポリシー」523 ページ

「アプリケーション配信」530 ページ

「(設定－iOS)「App とブック」設定」100 ページ

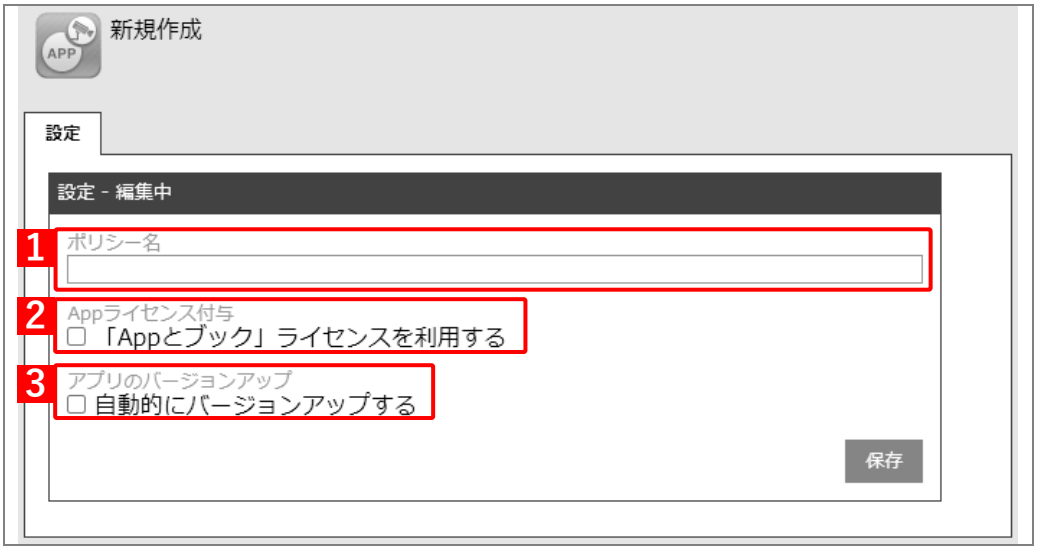
「[「App とブック」設定］タブ」262 ページ

「[その他▼］タブ／「App とブック」」289 ページ

管理対象アプリポリシー設定は、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［iOS］→［アプリケーション］→［管理対象アプリポリシー］→ ✚



項番	項目	説明
1	ポリシー名	ポリシーの名称を 30 文字以内で指定します。設定内で重複はできません。
2	App ライセンス付与	●App ライセンスを利用する 付与する場合は、チェックボックスにチェックを入れてください。
3	アプリのバージョンアップ	App Store アプリを自動的にバージョンアップする場合は、チェックボックスにチェックを入れてください。 「App とブック」ライセンスを付与したアプリは、手動でバージョンアップができません。 省データモードが有効になっている場合は、サイレントインストールでのバージョンアップができません。 iOS 端末のバージョンによりアプリのバージョンアップには、iOS 端末でロック解除をする必要がある場合があります。

8.6.4 オリジナルアプリ登録

オリジナルで制作したアプリを端末に配信するための設定を行い、オリジナルアプリ登録設定として保存します。

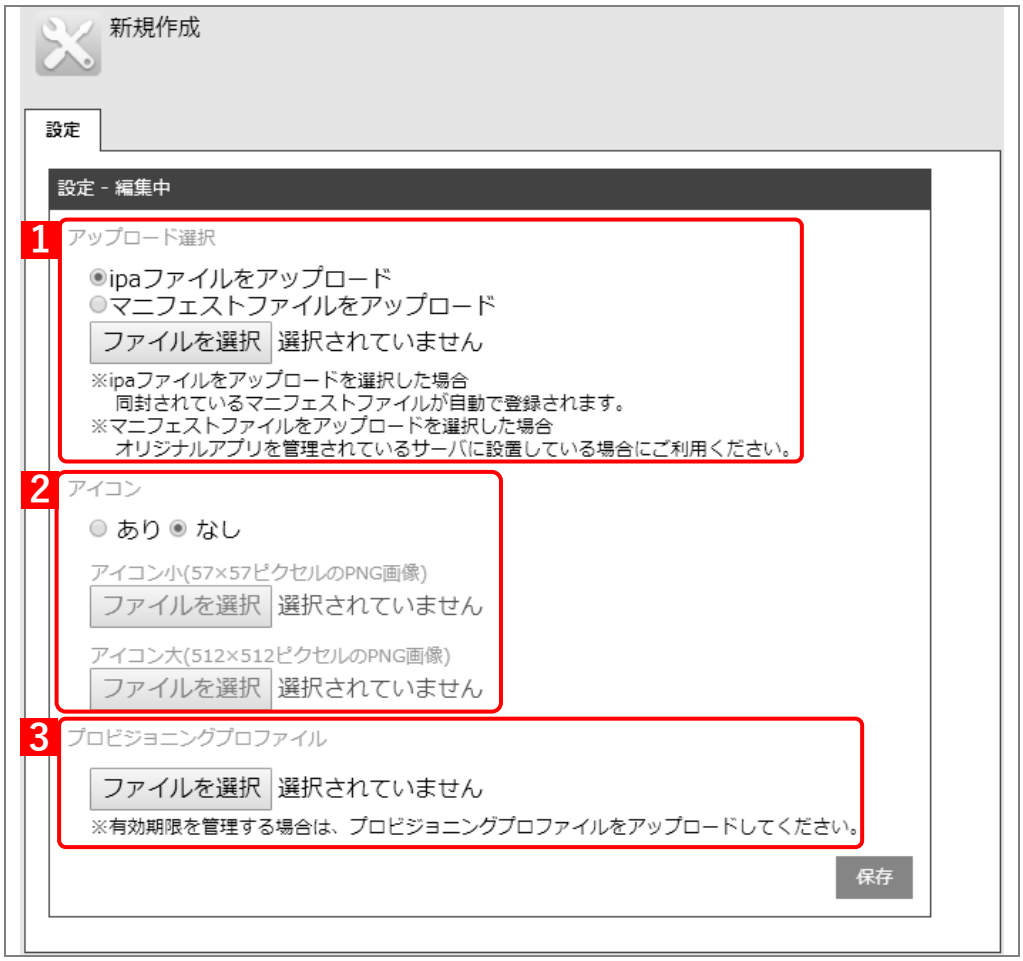
本設定で作成したオリジナルアプリ登録設定は、「アプリケーション配信」でオリジナルアプリを配信する場合に使用します。

- アプリを登録するには、ipa ファイル（*.ipa）、またはマニフェストファイル（*.plist）が必要です。アップロード方法に応じてファイルを準備してください。
- 同じアプリを複数件登録することはできません。
- アプリケーション ID が同一のオリジナルアプリは、ビルド番号が異なる場合のみ最大 3 件まで登録できます。
- InHouse 版（組織内配布）、Ad Hoc 版（評価用配布）に対応しています。Ad Hoc 版（評価用配布）は、配信数に制限があります。
- アップデートするには、新しいオリジナルアプリ登録設定から、アプリケーション ID が同一でバージョンが異なるオリジナルアプリを登録してください。そのあと、該当のアプリケーション配信設定を新しいオリジナルアプリ登録設定に差し替えて同期すると、端末のオリジナルアプリがアップデートされます。
- オリジナルアプリ登録設定は、最大 600 件まで作成できます。

8.6.4.1 ［設定］タブ

◆画面

表示操作　［設定］→［iOS］→［アプリケーション］→［オリジナルアプリ登録］→ ＋



項番	項目	説明
1	アップロード選択	アップロードするファイルの種類を選択します。 ●ipa ファイルをアップロード ipa ファイルにマニフェストファイルが同封されている場合に選択します。 ●マニフェストファイルをアップロード オリジナルアプリを管理されているサーバーに設置している場合に選択します。登録対象アプリとペアとなるマニフェストファイルをアップロードします。
2	アイコン	アプリのアイコンを設定します。「あり」を選択した場合は、アイコンとして設定する画像ファイルを指定します。 ●あり 「アイコン小(57×57 ピクセルの PNG 画像)」または「アイコン大(512×512 ピクセルの PNG 画像)」の［ファイルを選択］をクリックして、画像ファイルを指定します。 ●なし アイコンがない場合に選択します。 本設定で表示されるアイコンは、オリジナルアプリを非管理対象としてアプリケーション配信した場合、ポータルで表示されるアイコンになります。 端末のホーム画面に表示するアイコンを指定することはできません。配信するアプリのアイコンが表示されます。 配信するアプリのアイコンを編集することはできません。
3	プロビジョニングプロファイル	［ファイルを選択］をクリックして、プロビジョニングプロファイルを指定します。 有効期限を管理する場合は、プロビジョニングプロファイルを指定します。

◆エラー一覧

文言	発生契機	対処方法
⚠ ipa ファイルを指定してください。	ipa ファイルにチェックが入っている状態で、何もファイルを指定せずアップロードしている。	「ファイルを選択」から ipa ファイルを選択して、アップロードしてください。
⚠ipa ファイルは不正な形式です。	ipa ファイルにチェックが入っている状態で、ipa 以外の形式のファイルを指定してアップロードしている。	「ファイルを選択」から ipa ファイルを選択して、アップロードしてください
⚠ipa ファイルのファイル名を短くしてください。	ipa ファイルのファイル名が、管理サイトで保存できる文字数の上限を超えている。	ipa ファイルのファイル名を短くして、アップロードしてください。
⚠マニフェストファイル内の URL は 200 文字以内にしてください。	指定したマニフェストファイルの URL が、200 文字を超えて記載されている。	URL を 200 文字以内で書き換えてください。
⚠マニフェストファイル内の URL は半角英数字と記号で入力してください。	指定したマニフェストファイルの URL に、半角英数字と記号以外が記載されている。	URL を半角英数字と記号以外を含まない値に書き換えてください。

文言	発生契機	対処方法
⚠マニフェストファイル内の URL は http://または https://で始めてください。	指定したマニフェストファイルの URL の先頭が、「http://」または「https://」以外で記載されている。	URL の先頭を「http://」または「https://」に書き換えてください。
⚠マニフェストファイル内の URL を入力してください。	指定したマニフェストファイルの URL が記載されていない。	URL を記載してください。
⚠ipa ファイルに Info.plist が存在しません。	指定した ipa ファイルの中身に info.plist の情報が存在していない。	info.plist を含んだ ipa ファイルを指定してアップロードしてください。
⚠Info.plist に Bundle Identifier が存在しません。	指定した ipa ファイルの info.plist に Bundle Identifier の情報が存在していない。	Bundle Identifier の情報を含んだ ipa ファイルを指定してアップロードしてください。
⚠Info.plist の Bundle Identifier は半角英数字とピリオド「.」、ハイフン「-」で入力してください。	指定した ipa ファイルの info.plist に、不正な値を含んだ Bundle Identifier が記載されている。	Bundle Identifier は半角英数字とピリオド「.」、ハイフン「-」のみ使用した値に書き換えてください。
⚠Info.plist に Bundle Version が存在しません。	指定した ipa ファイルの info.plist に Bundle Version の情報が存在していない。	Bundle Version の情報を含んだ ipa ファイルを指定してアップロードしてください。
⚠Info.plist の Bundle Version に特殊文字が含まれています。	指定した ipa ファイルの info.plist に、特殊文字を含んだ Bundle Version が記載されている。	Bundle Version は特殊文字を含まない値に書き換えてください。
⚠Info.plist に Bundle Display Name または Bundle Name が存在しません。	指定した ipa ファイルの info.plist に Bundle Display Name または Bundle Name が存在していない。	Bundle Display Name または Bundle Name を含んだ ipa ファイルを指定してアップロードしてください。
⚠Info.plist の Bundle Display Name に特殊文字が含まれています。	指定した ipa ファイルの info.plist に、特殊文字を含んだ Bundle Display Name が記載されている。	Bundle Display Name は特殊文字を含まない値に書き換えてください。

文言	発生契機	対処方法
⚠Info.plist の Bundle Name に特殊文字が含まれています。	指定した ipa ファイルの info.plist に、特殊文字を含んだ Bundle Name が記載されている。	Bundle Name は特殊文字を含まない値に書き換えてください。
⚠既に同一のアプリケーション ID(Bundle Identifier)とビルド番号のアプリが登録されています。	Bundle Identifier とビルド番号が全く同じアプリがすでに登録されている。	古いアプリを削除するか、登録しようとしているオリジナルアプリの BundleID かビルド番号を書き換えてください。
⚠同一のアプリケーション ID(Bundle Identifier)のアプリは最大数(3)までしか登録できません。	同一の Bundle Identifier のアプリがすでに 3 つ登録されている。	古いアプリを削除するか、登録しようとしているオリジナルアプリの BundleID を書き換えてください。

8.6.5 App Configuration

App Configuration（アプリに対して特定の設定値を受け渡す仕組）で受け渡すアプリ名や設定値などを、App Configuration 設定として保存します。

保存した App Configuration 設定をアプリケーション配信の「App Configuration」項目で設定できます。設定すると、App Configuration に対応した対象のアプリに設定値を受け渡すことができます。

- 設定値を受け渡した結果、実現できることはアプリによって異なります。
- 対応している設定値の形式は、String、Integer、および Boolean です。
- アプリの App Configuration の対応有無、および設定値の仕様については、アプリの開発元へ問い合わせてください。
- エージェントを自動認証するように App Configuration を設定することができます。詳細については、以下を参照してください。

  『iOS キッティングマニュアル』の「エージェントを認証する」―「エージェントをインストール／認証する」―「アプリケーション配信を利用してインストール／自動認証する」―「エージェントを自動認証する」

- App Configuration 設定は、最大 50 件まで作成できます。

8.6.5.1 ［設定］タブ

◆画面

表示操作　［設定］→［iOS］→［アプリケーション］→［App Configuration］→ ✚

項番	項目	説明
1	設定名	App Configuration の設定の名称を 1 文字から 30 文字以内で指定します。
2	アプリケーションタイプ	対象のアプリの種類に応じて、「オリジナルアプリ」または「App Store アプリ」のいずれかを選択します。
3	アプリケーション名	対象のアプリをリストボックスから選択します。 あらかじめ対象のアプリをアプリケーション配信の「オリジナルアプリ一覧」、または「App Store アプリ一覧」に追加しておく必要があります。詳細については、以下を参照してください。 「アプリケーション配信」530 ページ

項番	項目	説明
4	設定値	設定値を登録します。1 つの設定セットにつき、100 件まで登録できます。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。 ●Key Configuration Key を入力します。 ●Type Value Type を以下から選択します。 ・String、Integer、Boolean ●Value 「Type」で選択した Value Type に応じて、以下の操作を行います。 ・「String」または「Integer」を選択した場合は、Key Value を入力します。 「String」を選択した場合は、Value に以下の変数が利用できます。 ・%MDM_ACTIVATION_CODE% iOS 端末固有のアクティベーションコードに変換されます。 ・%COMPANY_CODE% アプリを配信する端末に紐づく企業コードに変換されます。 ・%SERVER_URL% 管理サイトの URL に変換されます。 上記の 3 つの変数は、エージェント、未使用の自動認証機能を利用する場合などに利用します。詳細については、以下を参照してください。 『iOS キッティングマニュアル』の「エージェントを認証する」―「エージェントをインストール／認証する」―「アプリケーション配信を利用してインストール／自動認証する」―「エージェントを自動認証する」 『iOS クライアント リファレンスマニュアル』の「関連アプリの使用方法」―「未使用」―「未使用をインストールする」―「アプリケーション配信を利用してインストール／自動認証する」 ・%USER_NAME% アプリを配信する端末に紐づくユーザーの ID に変換されます。 ・%USER_EMAIL% アプリを配信する端末に紐づくユーザーのメールアドレスに変換されます。 ・%SERIAL_NUMBER% アプリを配信する端末のシリアル番号に変換されます。 ・%USER_FIRST_NAME% アプリを配信する端末に紐づくユーザーの姓に変換されます。 ・%USER_LAST_NAME% アプリを配信する端末に紐づくユーザーの名に変換されます。 ・%DEVICE_GUID% アプリを配信する端末の GUID に変換されます。 ・%DEVICE_NAME% アプリを配信する端末の機器名に変換されます。 ・「Boolean」を選択した場合は、「false」または「true」を選択します。 変数を使用する場合は、テスト端末で変数が正しく置換されていることを確認してください。テスト端末で問題がなければ、すべての端末に設定してください。

8.6.6 アプリケーション配信

指定したアプリを配信します。

本画面では、アプリを配信するための設定を行い、アプリケーション配信の設定セットを作成します。

配信するアプリによって、事前に以下の準備をしてください。

●オリジナルアプリを配信する場合［オリジナルアプリ登録］でオリジナルアプリを登録してください。

「オリジナルアプリ登録」524 ページ

●App Store のアプリを配信する場合
Store ID を確認してください。

「アプリケーション ID の調べかた」544 ページ

以下のとおり設定された構成プロファイルが、iOS 10.0 以上の端末に適用されている場合は、Apple の仕様によりポータルからオリジナルアプリをインストールできません。そのため、オリジナルアプリをインストールする場合は、管理対象アプリとして配信してください。

- ［iOS 制限設定］タブの「App Store からの App のインストールを許可（監視対象のみ）」にチェックを入れていない。（iOS 10.0.0 以上の端末が対象）
- ［iOS 制限設定］タブの「App のインストールを許可」にチェックを入れていない。（iOS 10.0.1 以上の端末が対象）

本機能は、配信したアプリ内のフォルダ削除やアプリを初期化することはありません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 300 件まで作成できます。

以下のアプリ配布はオプション機能を使用するものであり、アプリケーション配信の「アプリケーション管理」を利用している企業のみ利用することができます。詳細については、管理者に問い合わせてください。

●管理対象アプリとしてアプリを配布する場合、本画面でアプリを指定するときに「管理」の［有効］にチェックを入れます。

監視対象端末で省データモードが無効になっている場合は、アプリがサイレントインストールされます。

監視対象端末を対象に非管理対象アプリを管理対象アプリとして再配布した場合、監視対象端末ではユーザーの許可を求めるポップアップメッセージは表示されません。

管理対象アプリの詳細については、「管理」を参照してください。

「アプリケーション配信」530 ページ

●App ライセンスを付与したアプリを配布する場合
詳細については、以下のマニュアルを参照してください。

『iOS アプリケーション配信　手順書』

アプリケーション配信を行うと、対象の iOS 端末に「App とブック」アプリによる割り当て許可を求める確認画面が表示されます（「App とブック」アプリの初回配布のみ）。端末ユーザーの同意後の同期が開始されると、「App とブック」アプリの配布が開始されます。また、ユーザーが同意を拒否した場合は、8 時間が経過したあとの同期時に再度確認画面が表示されます。この確認画面の詳細については、以下を参照してください。

「「App とブック」ライセンス」514 ページ

●カスタム B2B アプリを配布する場合
カスタム B2B アプリとは、取引先や社内だけに限定公開できる iOS のアプリです。カスタム B2B アプリの配布をするには、App ライセンスが必要です。詳細については、以下を参照してください。

「「App とブック」ライセンス」514 ページ

カスタム B2B アプリは、iOS 9.3.2 以上の端末に配信できます。

カスタム B2B アプリの配布手順は、App ライセンスを付与したアプリの配布手順と同じです。
詳細については、以下のマニュアルを参照してください。

『iOS アプリケーション配信　手順書』

●App Store のアプリ配信で、アプリ配信後自動的にアプリのバージョンアップを行いたい場合
［管理対象アプリポリシー］で［アプリのバージョンアップ］にチェックを入れ、管理対象アプリポリシー設定を作成します。本画面でアプリを指定するときに、「管理」の［有効］にチェックを入れ、［管理対象アプリポリシー］で作成した管理対象アプリポリシー設定を選択します。

「管理対象アプリポリシー」523 ページ

◆画面

表示操作［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］→ ✚

項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	オリジナルアプリ一覧	端末へ配信するオリジナルアプリを登録します。1 つの設定セットにつき、600 件まで登録できます。 ✚ をクリックすると、入力欄が追加されます。 ✖ をクリックすると、入力欄が削除されます。 ●アプリケーション名 アプリ名とビルド番号が表示されます。該当のアプリを指定します。「オリジナルアプリ登録」で登録したアプリを指定できます。設定保存後は、アプリケーション ID およびビルド番号が自動表示されます。設定内で重複はできません。 ●管理 管理対象アプリとして配信する場合は、［管理］にチェックを入れます。管理対象アプリは監視対象端末の場合、サイレントインストールされます。また［管理］のチェックを外して同期すると、端末にインストールしたアプリはアンインストールされます。 ［管理］にチェックを入れると、以下の設定ができます。 ・アプリのデータのバックアップを制御 後述の「バックアップ」を参照してください。 ・アプリおよびアプリに関連付けられたデータの削除 ☞「［その他▼］タブ／iOS リモート操作」210 ページ

項番	項目	説明
		・App ライセンスを割り当てたアプリの配信 「管理対象アプリポリシー」523 ページ ・App Configuration の設定 後述の「App Configuration」を参照してください。 対象のアプリが端末に非管理対象アプリとしてインストールされていた場合、［管理］にチェックを入れて同期すると、管理対象アプリに変更されます。 ●バックアップ アプリのデータを iTunes または iCloud にバックアップすることを許可する場合は、チェックを入れます。 アプリをインストールしたあと、本設定の内容を変更することはできません。変更する場合は、アプリのアンインストールを行い、再インストールしてください。 本項目は、「管理」にチェックが入っているときに設定できます。 ●削除防止 アプリの削除を防止する場合は、［有効］にチェックを入れます。［有効］にチェックを入れて同期すると、削除防止が適用された状態でアプリがインストールされます。削除防止が適用されたアプリは端末から削除できません。 本項目は、「管理」にチェックが入っているときに設定できます。 すでに配信しているアプリの削除を防止したい場合は、本項目を設定して端末と同期してください。 ●ポリシー 「管理対象アプリポリシー」で作成したポリシーを指定すると、App ライセンスを適用できます。 「管理対象アプリポリシー」523 ページ ●App Configuration 対象のアプリに App Configuration の設定を適用する場合は、リストボックスから選択します。［新規追加］をクリックすると、App Configuration の設定画面が表示されます。 「App Configuration」528 ページ
3	App Store アプリ一覧	端末へ配信する App Store アプリを登録します。1 つの設定セットにつき、300 件まで登録できます。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。 ●Store ID Store ID を 0 以上 9223372036854775807 以下の半角数字で指定します。入力したあとに［更新］、または［保存］をクリックすると以降の情報を自動取得して表示します。設定内で重複はできません。 ●アプリケーション名 Store ID を入力したあとに［更新］、または［保存］をクリックして、自動取得してください。 ●管理 管理対象アプリとして配信する場合は、［管理］にチェックを入れます。管理対象アプリは監視対象端末の場合、サイレントインストールされます。また［管理］のチェックを外して同期すると、端末にインストールしたアプリはアンインストールされます。 ［管理］にチェックを入れると、以下の設定ができます。 ・アプリのデータのバックアップを制御 後述の「バックアップ」を参照してください。 ・アプリおよびアプリに関連付けられたデータの削除 「［その他▼］タブ／iOS リモート操作」210 ページ ・App ライセンスを割り当てたアプリの配信 「管理対象アプリポリシー」523 ページ

項番	項目	説明
		・App Configuration の設定 後述の「App Configuration」を参照してください。 対象のアプリが端末に非管理対象アプリとしてインストールされていた場合、［管理］にチェックを入れて同期すると、管理対象アプリに変更されます。 ●バックアップ アプリのデータを iTunes または iCloud にバックアップすることを許可する場合は、チェックを入れます。 アプリをインストールしたあと、本設定の内容を変更することはできません。変更する場合は、アプリのアンインストールを行い、再インストールしてください。 本項目は、「管理」にチェックが入っているときに設定できます。 ●削除防止 アプリの削除を防止する場合は、［有効］にチェックを入れます。［有効］にチェックを入れて同期すると、削除防止が適用された状態でアプリがインストールされます。削除防止が適用されたアプリは端末から削除できません。 本項目は、「管理」にチェックが入っているときに設定できます。 すでに配信しているアプリの削除を防止したい場合は、本項目を設定して端末と同期してください。 ●ポリシー 「管理対象アプリポリシー」で作成したポリシーを指定すると、App ライセンスを適用できます。 ☞「管理対象アプリポリシー」523 ページ ●App Configuration 対象のアプリに App Configuration の設定を適用する場合は、リストボックスから選択します。［新規追加］をクリックすると、App Configuration の設定画面が表示されます。 ☞「App Configuration」528 ページ

8.6.7 シングル APP モード（監視対象のみ）

iOS 端末や iPadOS 端末をシングル APP モードにするための設定を行い、設定セットを作成します。

「画面（新規作成）」
「画面（編集）」
「画面（登録後）」

シングル APP モードとは、iOS 端末や iPadOS 端末で起動できるアプリを 1 つのみに制限する機能です。注文、会計、POS アプリおよびデモアプリなどのみを起動させて、他のアプリの操作や設定の変更などをできなくします。

本機能を使用する場合は、以下の注意事項を必ず確認してください。誤った操作を行うと、端末が操作不能になったり、設定を解除できなくなったりするので、注意してください。

注意

- ●シングル APP モードは、iOS 6.0 以上の監視対象端末で使用できます。
- ●シングル APP モードの対象アプリを端末にインストールし、アプリが使用できることを確認してから、本設定を行ってください。
- ●シングル APP モードの反映時、および端末に反映している状態で、［アプリケーション配信］設定の割り当て解除や［アプリケーション配信］の「管理」から［有効］のチェックを外すと、端末にメッセージが表示され、操作ができなくなります。特に注意してください。
- ●シングル APP モード中の端末は、アプリケーション ID で指定したアプリのみ動作します。
  - ・エージェントが必要な機能（メッセージ通知、位置情報取得（紛失モード時を除く））は動作しません。
  - ・対象アプリ以外からの通知は表示されません。
  - ・端末の設定アプリが使用できなくなるため、端末の設定変更はできません。
- ●アプリケーション ID で指定したアプリが、端末にインストールされていない場合、シングル APP モードの適用は延期されます。
- ●対象アプリがプリインストールアプリではない場合、一定回数は、同期を行うたびに対象アプリが端末にインストールされているかを確認します。対象アプリが端末にインストールされていない場合は、シングル APP モードの適用を延期します。延期できる回数と延期している回数は、機器ログに出力されます。また、延期が一定の回数になると、シングル APP モードの端末への適用を中止します。対象アプリをアプリケーション配信で端末にインストールしてから、設定の割り当てを解除して同期し、再度、設定を割り当てて同期してください。
- ●シングル APP モード設定中の端末に、アプリケーション配信設定を外すなどの操作を行い、アプリがアンインストールされた場合、端末が操作不能になる恐れがあります。シングル APP モード設定中の端末からアプリをアンインストールする操作は、絶対に行わないでください。
- ●シングル APP モード設定中の端末を管理サイトから削除した場合、設定の解除や MDM 構成プロファイルのアンインストールが、Apple Configurator 2 以外では行えなくなります。
  必ずシングル APP モードの割り当てを解除して同期を行い、シングル APP モードが端末から解除されたことを確認してから、管理サイトの端末を削除してください。
- ●以下のいずれかを設定していてシングル APP モード設定中の端末と通信ができなくなった場合は、設定の変更や MDM プロファイルのアンインストールは行えなくなります。注意してください。
  - ・［設定］→［iOS］→［構成プロファイルアップロード］→［Configurator 以外のホストとのペアリングを許可］のチェックを外している

    「画面（機能の制限）」400 ページ
  - ・［設定］→［iOS］→［ADE 定義プロファイル］の［Mac とのペアリングを許可する］のチェックを外している

    「ADE 定義プロファイル」505 ページ
- ●iOS 14 以上では、シングル APP モード設定中の端末でも、管理サイトから OS アップデートを行えますが、iOS 14 未満では、シングル APP モード設定中に［OS アップデート］を行うと、端末が操作不能になる事象が Apple に報告されています。

  「（操作－iOS）OS アップデート」126 ページ
- ●シングル APP モードを適用中の iPad では、物理ボタンを使用したシャットダウンや再起動は行うことができません。シャットダウンや再起動は管理サイトから行ってください。

  「（操作－iOS）リモート再起動」127 ページ
  「（操作－iOS）リモートシャットダウン」128 ページ

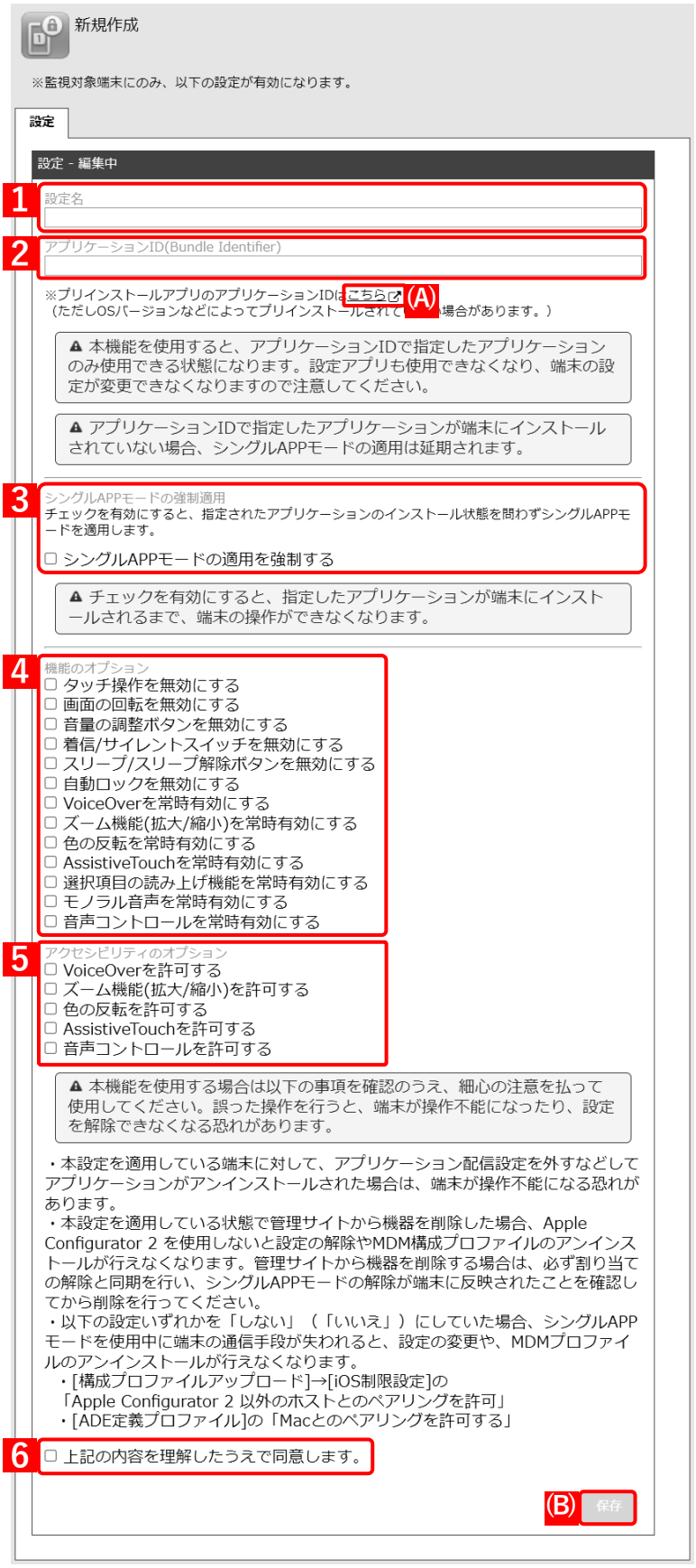
参考

●シングル APP モードで使用するアプリは、［アプリケーション配信］で「管理対象アプリ」として配信し、端末にインストールすることをおすすめします。

「アプリケーション配信」530 ページ

◆画面（新規作成）

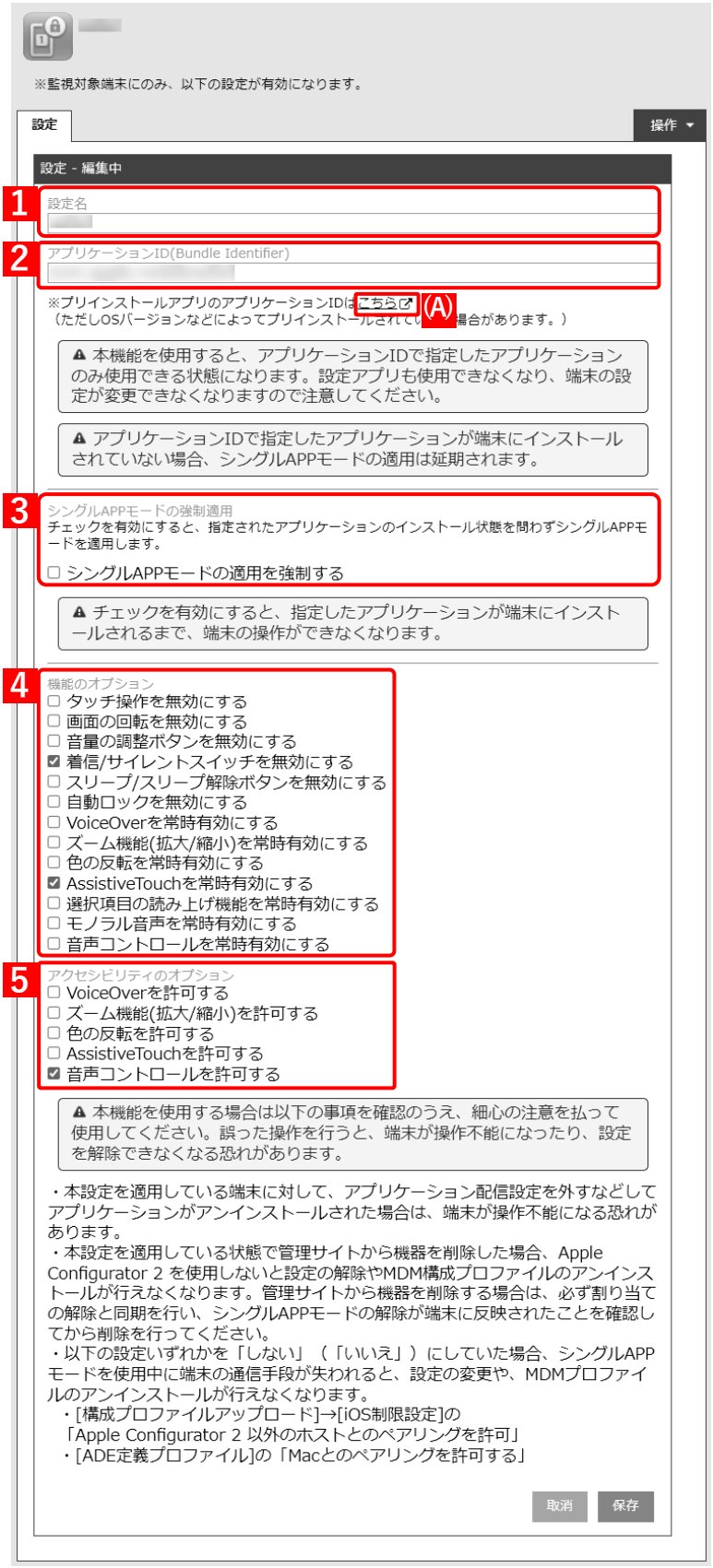
表示操作　［設定］→［iOS］→［アプリケーション］→［シングル APP モード（監視対象のみ）］→ ✚



項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	アプリケーション ID (Bundle Identifier)	シングル APP モードの対象アプリのアプリケーション ID を指定します。 アプリケーション ID の確認方法は、以下を参照してください。 「アプリケーション ID の調べかた」544 ページ (A)［こちら］をクリックすると、プリインストールアプリのアプリケーション ID の一覧が表示されます。
3	シングル APP モードの強制適用	対象アプリがプリインストールアプリで、(A)［こちら］をクリックして、表示される一覧に存在しない場合は、［シングル APP モードの適用を強制する］にチェックを入れます。
4	機能のオプション	シングル APP モード中に無効／有効にしたい項目にチェックを入れます。
5	アクセシビリティのオプション	シングル APP モード中に許可したい項目にチェックを入れます。
6	［上記の内容を理解した上で同意します］	項番 1～5 までの指定や設定した内容を確認し、［上記の内容を理解した上で同意します］にチェックを入れます。 ［上記の内容を理解した上で同意します］にチェックを入れると、(B)［保存］をクリックすることができます。

◆画面（編集）

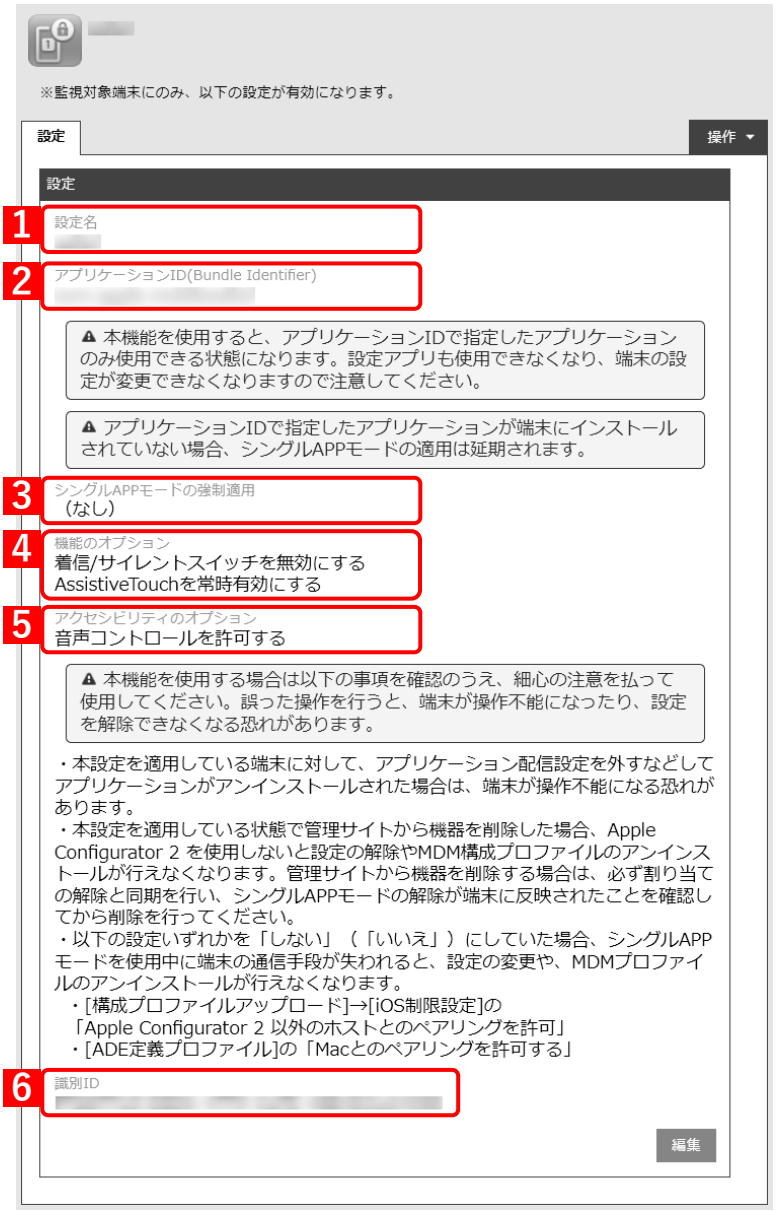
表示操作　［設定］→［iOS］→［アプリケーション］→［シングル APP モード（監視対象のみ）］→一覧から対象を選択→［編集］



項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	アプリケーション ID (Bundle Identifier)	シングル APP モードの対象アプリのアプリケーション ID を指定します。 アプリケーション ID の確認方法は、以下を参照してください。 「アプリケーション ID の調べかた」544 ページ （A）［こちら］をクリックすると、プリインストールアプリのアプリケーション ID の一覧が表示されます。
3	シングル APP モードの強制適用	対象アプリがプリインストールアプリで、（A）［こちら］をクリックして、表示される一覧に存在しない場合は、［シングル APP モードの適用を強制する］にチェックを入れます。
4	機能のオプション	シングル APP モード中に無効／有効にしたい項目にチェックを入れます。
5	アクセシビリティのオプション	シングル APP モード中に許可したい項目にチェックを入れます。

◆画面（登録後）

表示操作［設定］→［iOS］→［アプリケーション］→［シングル APP モード（監視対象のみ）］→一覧から対象を選択



項番	項目	説明
1	設定名	指定した設定名が表示されます。
2	アプリケーション ID (Bundle Identifier)	指定したアプリケーション ID が表示されます。
3	シングル APP モードの強制適用	チェックを入れると「シングル APP モードの適用を強制する」と表示されます。
4	機能のオプション	チェックを入れた項目が表示されます。
5	アクセシビリティのオプション	チェックを入れた項目が表示されます。
6	識別 ID	識別 ID が表示されます。 機器一覧のシングル APP モードのプロファイルに表示される識別 ID と一致したとき、シングル APP モードが端末に適用されていることになります。 「(情報－iOS) プロファイル」162 ページ 識別 ID は、本設定の新規作成や編集をしたときに出力される管理ログでも確認できます。 『ログ一覧』の「ログ一覧」

8.6.8 アプリケーション検知

端末からアプリ一覧を取得し、指定した条件と一致するアプリを検知して、ログを表示します。

「インストール推奨アプリケーション」では、指定するアプリが、端末にインストールされていないことを確認できます。また、「インストール非推奨アプリケーション」では、指定するアプリケーションが端末にインストールされていることを確認することができます。

アプリの検知は端末ごとに、1 日 1 回ランダムなタイミングで実行されます。

本画面では、アプリを検知するための設定を行い、アプリケーション検知の設定セットを作成します。

プリインストールされている内蔵アプリは、検知対象外です。内蔵アプリについては、Apple のサイトで対象の iOS 端末の情報から確認してください。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

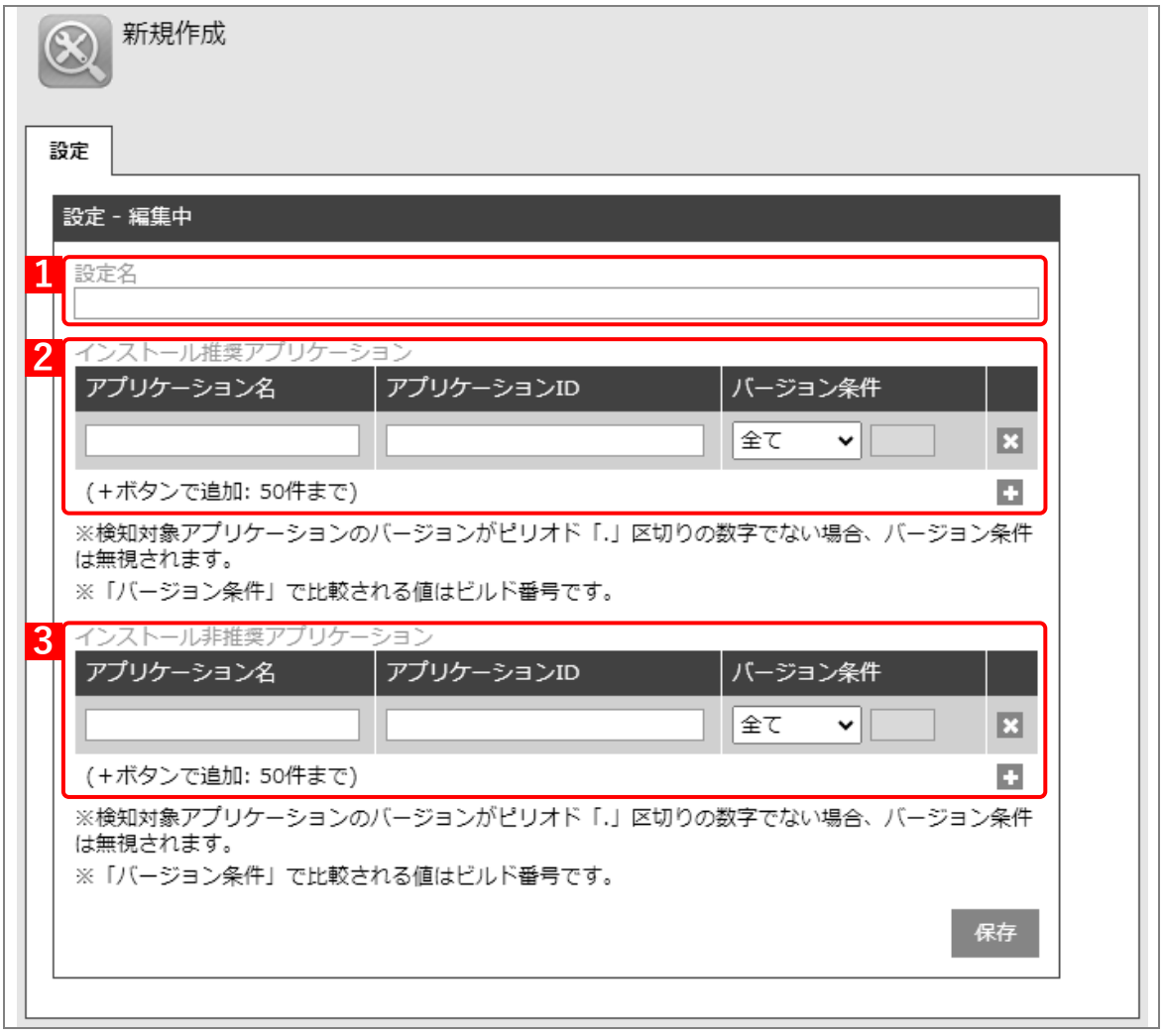
「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［iOS］→［アプリケーション］→［アプリケーション検知］→ ＋



項番	項目	説明
1	設定名	設定セットの名称を指定します。1 文字から 30 文字で入力してください。
2	インストール推奨アプリケーション	インストールを推奨するアプリを登録します。1 つの設定セットにつき、50 件まで登録できます。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。 ●アプリケーション名 アプリ名を 60 文字以内で入力します。 ●アプリケーション ID アプリケーション ID を 255 文字以内で入力します。使用できる文字は、半角英数字と記号（「.」、「-」）です。アプリケーション ID は、対象端末にインストールされているアプリの一覧から確認できます。詳細については、以下を参照してください。 ☞「（情報－iOS）アプリケーション」157 ページ ●バージョン条件 バージョン条件を 255 文字以内で設定します。 入力例 ABC アプリのバージョン 2.0 以上を推奨アプリにする場合 アプリケーション名：ABC アプリ パッケージ名：abcxxxxxxx バージョン条件：≧2.0
3	インストール非推奨アプリケーション	インストールを推奨しないアプリを登録します。1 つの設定セットにつき、50 件まで登録できます。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。 ●アプリケーション名 アプリ名を 60 文字以内で入力します。 ●アプリケーション ID アプリケーション ID を 255 文字以内の半角英数字と記号（「.」、「-」）で入力します。アプリケーション ID の詳細については、以下を参照してください。 ☞「アプリケーション ID の調べかた」544 ページ ●バージョン条件 バージョン条件を 255 文字以内で設定します。 入力例 ABC アプリのバージョン 2.0 未満を非推奨アプリにする場合 アプリケーション名：ABC アプリ プリケーション ID：abcxxxxxxx バージョン条件：＜2.0

◆アプリケーション ID の調べかた

【1】ブラウザーで「https://tools.applemediaservices.com/app-store」にアクセスします。

【2】検索窓に対象アプリ名を入力して検索し、検索結果から対象アプリをクリックします。

⇒対象アプリの説明画面が表示されます。

【3】説明画面の URL からアプリの Store ID を確認します。

⇒Store ID は、URL 末尾の「?country=us」を除く数字です。

以下 Apple Books の URL を例にとると、下線で示した「364709193」が Store ID に該当します。
https://tools.applemediaservices.com/app/364709193?country=us

【4】ブラウザーで「http://itunes.apple.com/lookup?country=JP&id=XXXXXXXXX」にアクセスします。

⇒テキストファイルがダウンロードされます。

上記 URL をブラウザーにコピー＆ペーストし、末尾の「XXXXXXXXX」にあたる部分には、手順【3】で確認した対象アプリの Store ID を入力してください。

【5】ダウンロードされたテキストファイルを開き、「bundleId」という文字列を検索します。

⇒アプリケーション ID は、テキストファイル内で「"bundleId":」に続くダブルクオーテーションで括られた文字列（Apple Books の場合は「com.apple.iBooks」）として示されています。

8.7 便利機能

音声ローミングやデータローミングの設定、iOS 端末のホーム画面のレイアウトを設定します。

8.7.1 ローミング設定

音声ローミングやデータローミングを有効または無効に設定します。

本画面では、ローミングの有効／無効を設定し、ローミング設定の設定セットを作成します。

本設定は、端末で設定の変更を禁止する機能ではありません。「無効にする」を設定しても、端末からデータローミング設定を手動で行えます。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［iOS］→［便利機能］→［ローミング設定］→ ＋（一覧から対象を選択→［編集］）

項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	音声ローミング設定	音声ローミングの有効または無効を指定します。 ●有効にする ●無効にする
3	データローミング設定	データローミングの有効または無効を指定します。 ●有効にする ●無効にする

8.7.2 ホーム画面レイアウト（監視対象のみ）

iOS 端末のホーム画面レイアウトを、管理者が指定および固定することで、キッティング作業や運用の手間を削減することができます。

本画面では、ホーム画面の Dock やページの設定を行い、ホーム画面レイアウトの設定セットを作成します。

画面（新規作成）
画面（編集）
画面（Dock の編集）
画面（Page 1 の編集）
画面（Page の新規作成）

iOS 9.3 以上の監視対象端末のみで利用できます。

本機能でレイアウト指定したアプリ以外は、配置できる箇所に順次配置されます。iOS 端末でのアプリの並び替えや、フォルダーに入れるなどの操作はできません。

本機能で Web クリップのレイアウトを指定することはできません。

使用できるアプリを制限せずに本機能を利用すると、iOS 端末利用者の利便性を損なう恐れがあります。構成プロファイルアップロードで「App の使用を制限（監視対象のみ）」とあわせてご利用になることをお勧めします。詳細については、以下を参照してください。

「構成プロファイルアップロード」393 ページ

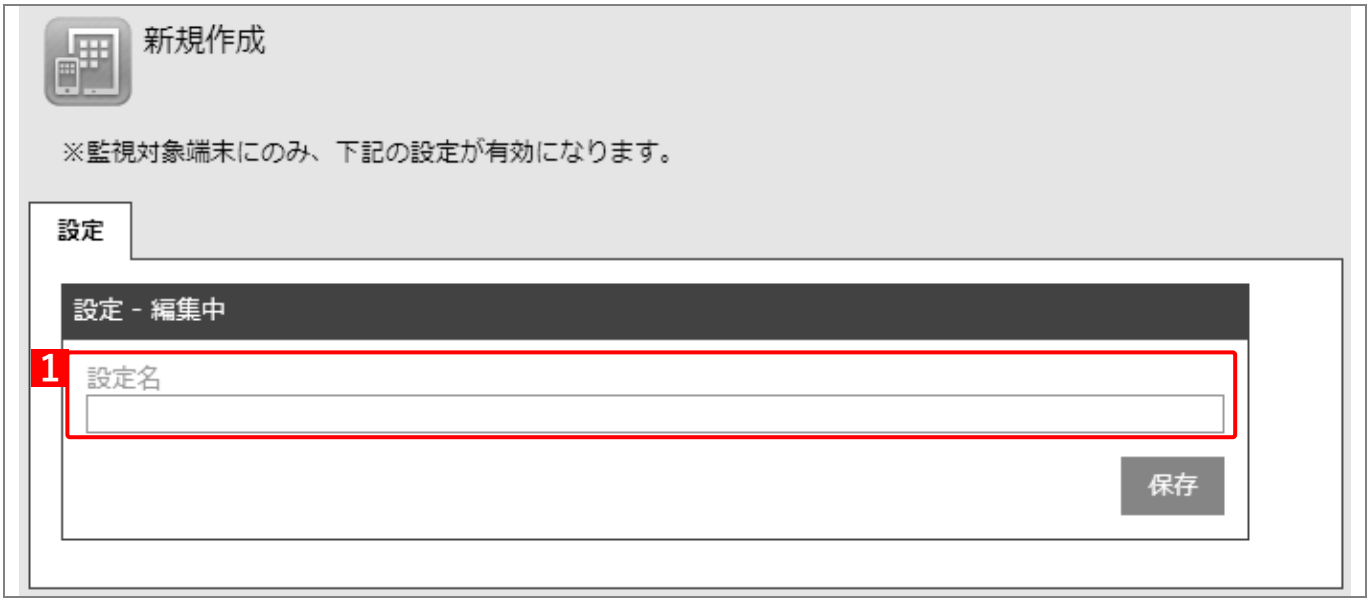
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－iOS）設定の割り当て」83 ページ
「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成）

表示操作　［設定］→［iOS］→［便利機能］→［ホーム画面レイアウト（監視対象のみ）］→ ＋



項番	項目	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で入力してください。

◆画面（編集）

設定セットを新規作成すると、以下のような画面となり、「Dock」「Page 1」「Page 2」を編集する項目が表示されます。詳細については、各項目を参照してください。

表示操作　［設定］→［iOS］→［便利機能］→［ホーム画面レイアウト（監視対象のみ）］→一覧から対象を選択

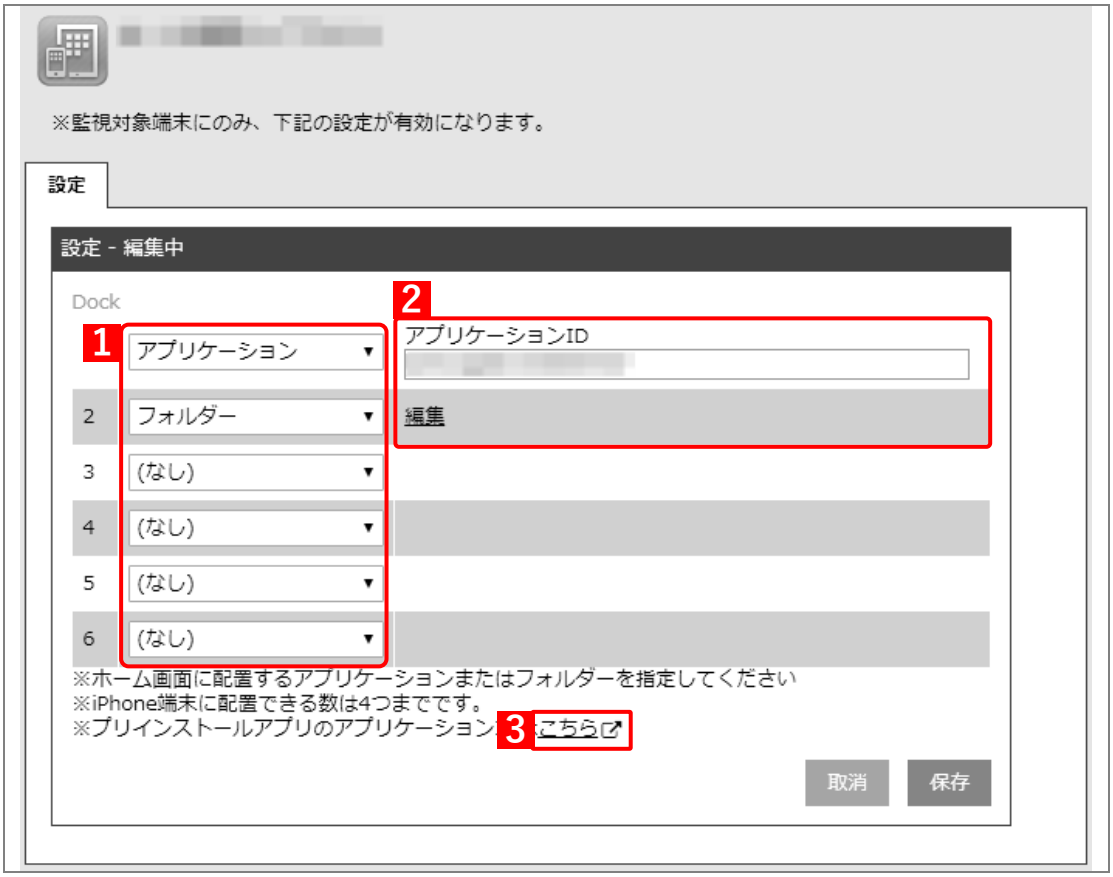
項番	項目	説明
1	設定名	最初に作成した設定名が表示されています。
2	Dock	Dock の設定を行います。詳細については、以下を参照してください。 ☞「画面（Dock の編集）」548 ページ
3	Page 1	ホーム画面 1 ページ目のアプリ配置設定を行います。詳細については、以下を参照してください。 ☞「画面（Page 1 の編集）」550 ページ
4	Page 2	2 ページ目以降の設定を追加します。詳細については、以下を参照してください。 ☞「画面（Page の新規作成）」551 ページ 新規作成するとパネル名が Page3、Page4…という表示になります。

◆画面（Dock の編集）

Dock のレイアウトを編集します。

iPhone 端末に配置できる数は、4 つまでです。

表示操作　**［設定］→［iOS］→［便利機能］→［ホーム画面レイアウト（監視対象のみ）］→一覧から対象を選択→「Dock」の［編集］**



項番	項目	説明
1	種別	●なし 何も設定しない場合に利用します。 ●アプリケーション iOS アプリを設定するときに利用します。 ●フォルダー フォルダーを作成して、フォルダーの中にアプリを設定するときに利用します。

項番	項目	説明
2	内容	項番【1】「種別」で選択した内容に合わせて、以下を設定します。 ●アプリケーション iOS アプリを設定するときに利用します。 ・アプリケーション ID 項番【3】［こちら］をクリックして、プリインストールアプリのアプリケーション ID を調べることができます。 プリインストールアプリ以外のアプリケーション ID の確認については、以下を参照してください。 「(情報－iOS) アプリケーション」157 ページ 「アプリケーションレポート」241 ページ ●フォルダー フォルダーを作成して、フォルダーの中にアプリを設定するときに利用します。 ［編集］をクリックするとフォルダーウインドウが表示されるので、「フォルダー名」を 1 文字から 30 文字以内で作成し、その他必要事項を設定します。
3	［こちら］	プリインストールアプリのアプリケーション ID を調べるときにクリックします。

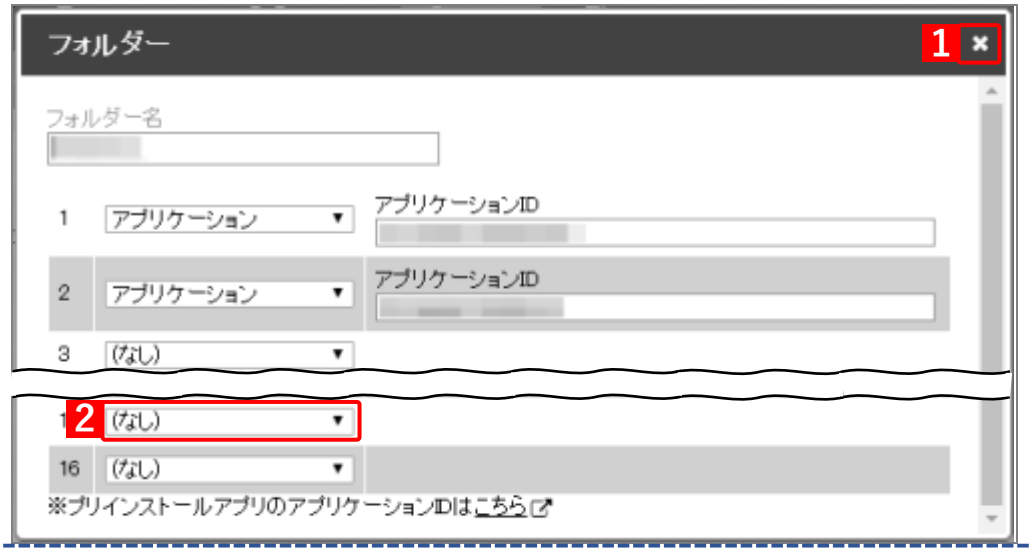
参考

●「フォルダー」を編集する場合

・保存する方法
本画面に保存ボタンはありません。必要事項を入力、設定したあとに【1】［×（Close)］をクリックすると、設定した内容が保存されます。

・登録したアプリやフォルダーを消す方法
リストボックスの「アプリケーション」や「フォルダー」を【2】「なし」に変更してください。

例)

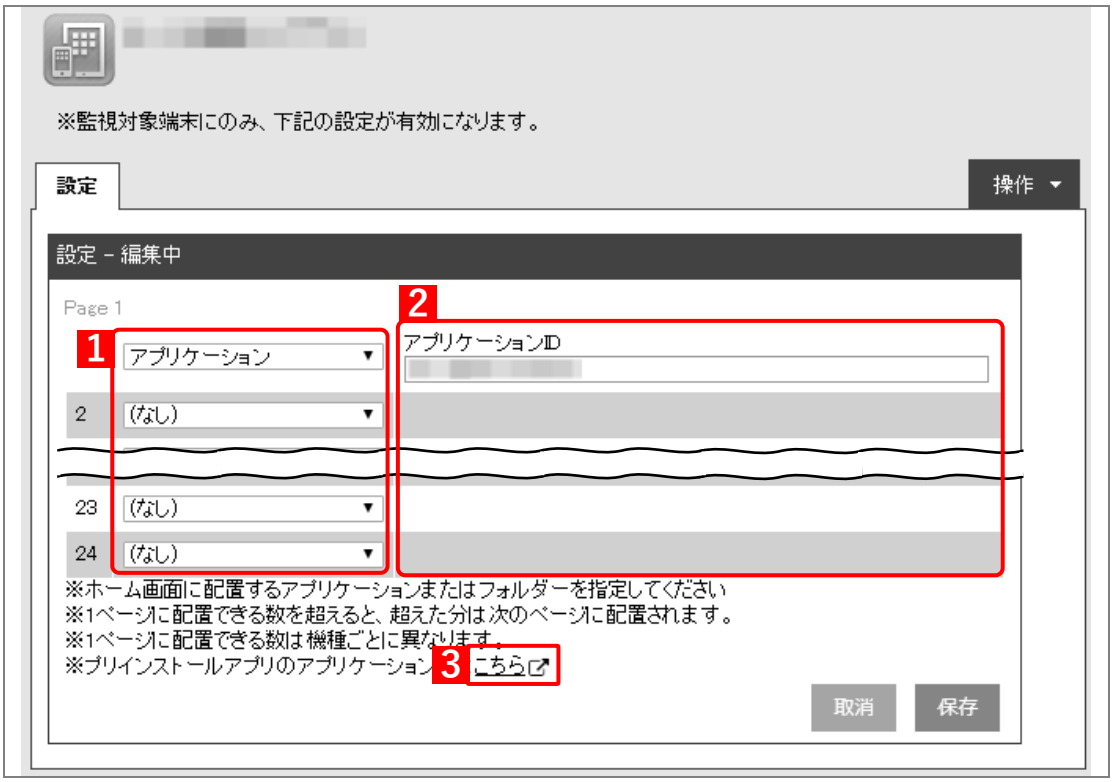


◆画面（Page 1 の編集）

Page のレイアウトを編集します。画面には 1 から 24 までの数字が表示され、それぞれのリストボックスで、［フォルダー］または［アプリケーション］を指定します。iOS 端末では、左上からフォルダーまたはアプリが、数字の順に配置されます。

端末によって 1Page に配置できるアプリ数は異なります。配置可能数を超えて設定をした場合、超過したものは次の Page に配置されます。

表示操作　［設定］→［iOS］→［便利機能］→［ホーム画面レイアウト（監視対象のみ）］→一覧から対象を選択→「Page 1」の［編集］



項番	項目	説明
1	種別	●なし 何も設定しない場合に利用します。 ●アプリケーション iOS アプリを設定するときに利用します。 ●フォルダー フォルダーを作成して、フォルダーの中にアプリを設定するときに利用します。
2	内容	●アプリケーション iOS アプリを設定するときに利用します。 ・アプリケーション ID 項番【3】［こちら］をクリックして、プリインストールアプリのアプリケーション ID を調べることができます。 プリインストールアプリ以外のアプリケーション ID の確認については、以下を参照してください。 ☞「(情報－iOS) アプリケーション」157 ページ ☞「アプリケーションレポート」241 ページ ●フォルダー フォルダーを作成して、フォルダーの中にアプリを設定するときに利用します。 ［編集］をクリックするとフォルダーウインドウが表示されるので、「フォルダー名」を 1 文字から 30 文字以内で作成し、その他必要事項を設定します。

項番	項目	説明
3	［こちら］	プリインストールアプリのアプリケーション ID を調べるときにクリックします。

◆画面（Page の新規作成）

iOS 端末に表示する Page を新規作成します。新規に Page を作成すると、画面上に Page 2、Page 3…と Page のパネルが追加されます。

追加したパネルは、Page 1 と同様に編集してください。

「画面（Page 1 の編集）」550 ページ

端末によって 1Page に配置できるアプリ数は異なります。配置可能数を超えて設定をした場合は、次の Page に配置されます。

表示操作　**［設定］→［iOS］→［便利機能］→［ホーム画面レイアウト（監視対象のみ）］→一覧から対象を選択→「Page 2」の［新規作成］**

項番	項目	説明
1	Page 2―［新規作成］（※1）	［新規作成］をクリックすると、新規に Page が作成されます。必要事項を入力して、［保存］をクリックします。

※1：「Page 2」は、Page を新規作成すると、Page 3、Page 4…と表示されます。

8.7.3 SIM ステータス変更検知

SIM ステータス変更検知の設定セットを作成します。SIM ステータス変更検知は、SIM が抜かれた場合や SIM が挿入された場合に、ログを出力する機能です。

この設定は、Android と iOS で共有することができます。

端末を認証するとき、本設定が端末に割り当てられている場合、初回の同期でログが出力されます。

ネットワークが未接続の状態や同期ができない状態のときは、SIM を変更してもログは出力されません。

SIM のスロットが複数ある端末の場合、1 つめのスロットから SIM を抜いて、2 つめのスロットに SIM の挿入や入れ替えしてもログは出力されません。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

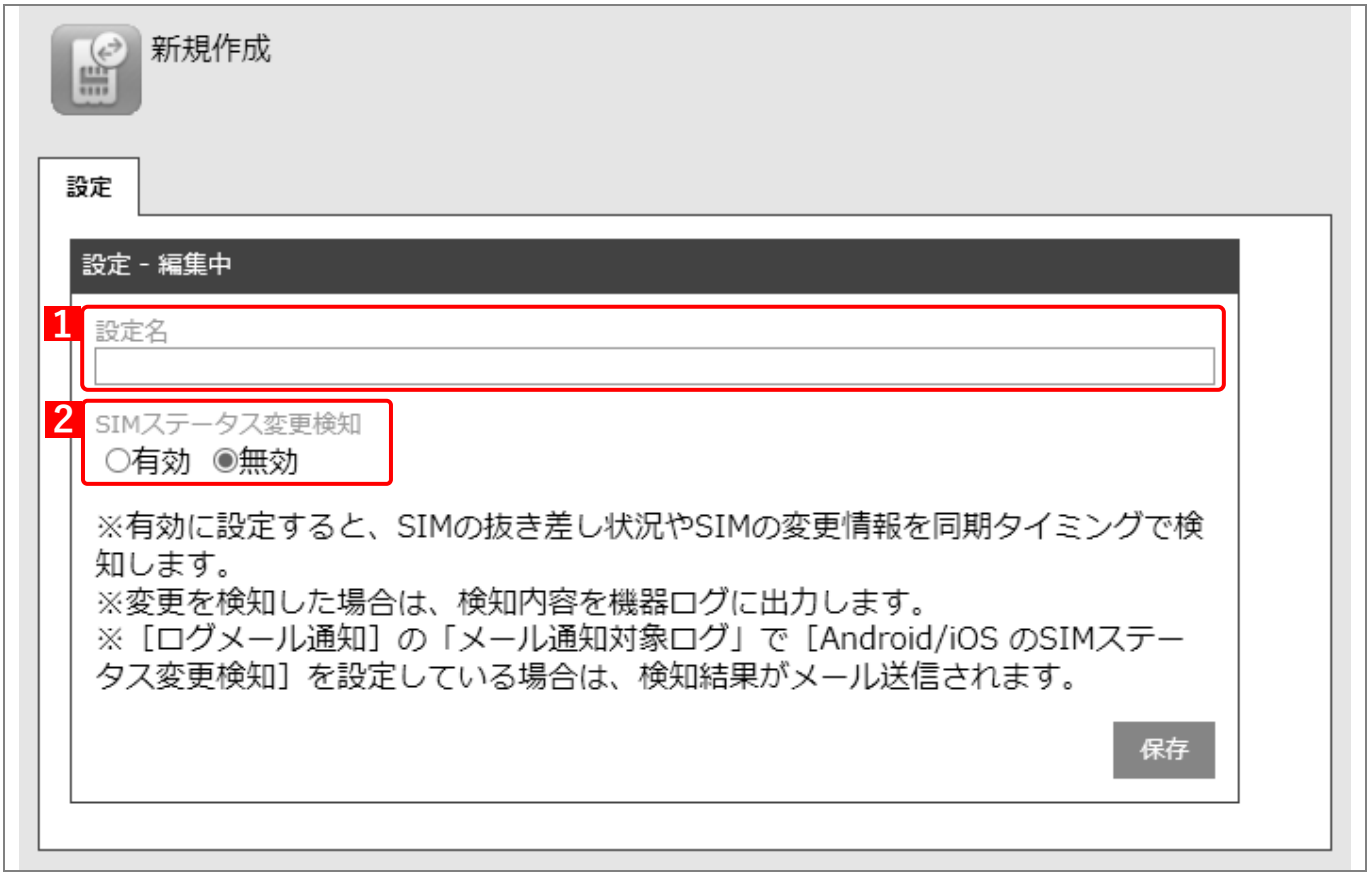
「（設定－iOS）設定の割り当て」83 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［iOS］→［便利機能］→［SIM ステータス変更検知］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	SIM ステータス変更検知	有効に設定すると、SIM の抜き差し状況や SIM の変更情報を同期タイミングで検知します。

8.8 証明書管理

クライアント証明書の管理や一括アップロード、一括削除を行います。

8.8.1 クライアント証明書管理

クライアント証明書を管理サイトに 1 ファイルずつアップロードして保存し、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

画面（新規作成）

画面（管理）

画面（編集）

事前にクライアント証明書を取得してください。

本機能はクライアント証明書の配信までを行います。端末内に保存されるクライアント証明書の場所やインストール方法については、端末メーカーへ問い合わせてください。

アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。

「画面（編集）」556 ページ

クライアント証明書をまとめてアップロードする場合は、以下を参照してください。

「クライアント証明書一括アップロード」557 ページ

管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。

「（設定－Android）クライアント証明書」79 ページ

「（設定－iOS）クライアント証明書」86 ページ

「（設定－iOS）Exchange（ActiveSync）設定」89 ページ

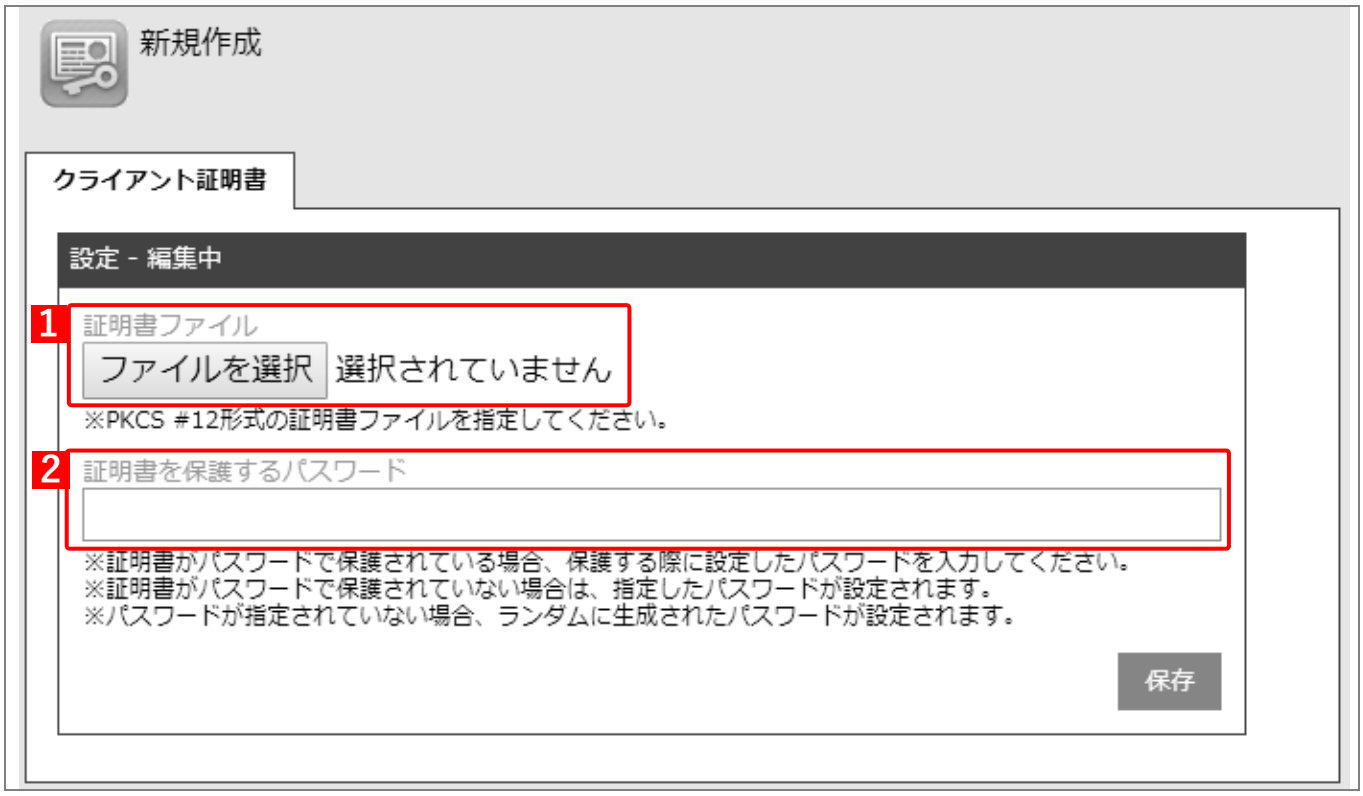
「（設定－iOS）VPN 設定」94 ページ

「（設定－Windows）クライアント証明書」106 ページ

設定セットは、最大で 500,000 件まで作成できます。

◆画面（新規作成）

表示操作［設定］→［iOS］→［証明書管理］→［クライアント証明書管理］→ ✚



項番	項目	説明
1	証明書ファイル	アップロードするクライアント証明書を指定します。［ファイルを選択］をクリックし、クライアント証明書ファイルを選択します。 PKCS #12 形式のクライアント証明書を指定してください。 ファイル名は 30 文字以内で設定してください。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを 255 文字以内の半角英数字で入力します。 パスワード未設定の場合は入力不要です。

◆画面（管理）

表示操作　［設定］→［iOS］→［証明書管理］→［クライアント証明書管理］

項番	項目	説明
1	検索/並び替え	（A）に検索対象項目、（B）に並び替えの対象項目が表示されます。 検索する場合は、検索するキーワードを（C）に入力し、［検索］をクリックします。検索したあとに、すべてのクライアント証明書を再表示するにはブラウザーを再読み込み、または（C）を空欄にし、再度［検索］ をクリックします。
2	✚	クリックするとクライアント証明書情報欄に入力欄が表示されます。 ☞「画面（新規作成）」554 ページ
3	▼	クリックすると以下のメニューが表示されます。 ●全てにチェックを入れる 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスにチェックが入ります。 ●全てのチェックをはずす 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスのチェックが外れます。 ●検索対象 検索対象をファイル名、発行先（証明書情報）のいずれかに変更できます。 ●並べ替え 昇順 ユーザー一覧をファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで昇順に並び替えます。 ●並べ替え 降順 ファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで降順に並び替えます。 ●一括削除 クライアント証明書一覧でチェックの入っている証明書を削除します。
4	クライアント証明書一覧	登録されているクライアント証明書一覧が表示されます。 ●（D） クライアント証明書のファイル名です。 ●（E） 発行先（クライアント証明書情報）です。 ●（F） 有効期間です。
5	クライアント証明書情報	クライアント証明書一覧から選択したクライアント証明書の情報が表示されます。

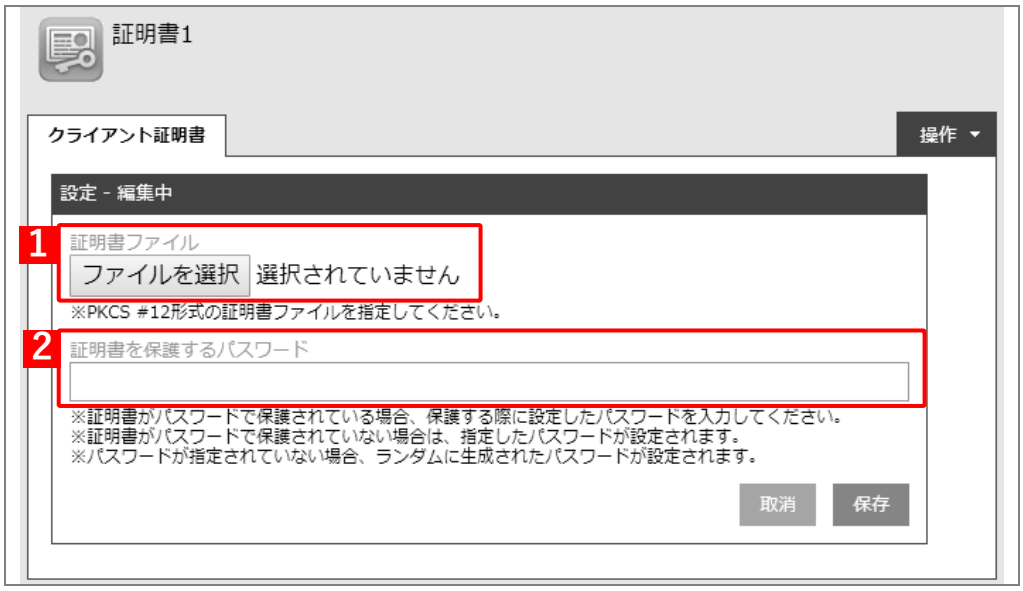
項番	項目	説明
6	［操作］	クリックすると以下のメニューが表示されます。 ●削除 クライアント証明書を削除します。
7	［編集］	クリックすると、登録されているクライアント証明書情報を編集できます。

◆画面（編集）

アップロード済みのクライアント証明書の差し替えやパスワードを変更する場合に内容を修正します。

設定項目は新規作成と同様です。

表示操作　**［設定］→［iOS］→［証明書管理］→［クライアント証明書管理］→一覧から対象を選択→［編集］**



項番	項目	説明
1	証明書ファイル	クライアント証明書一覧から再アップロードする証明書を指定します。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを入力します。パスワード未設定の場合は入力不要です。

8.8.2 クライアント証明書一括アップロード

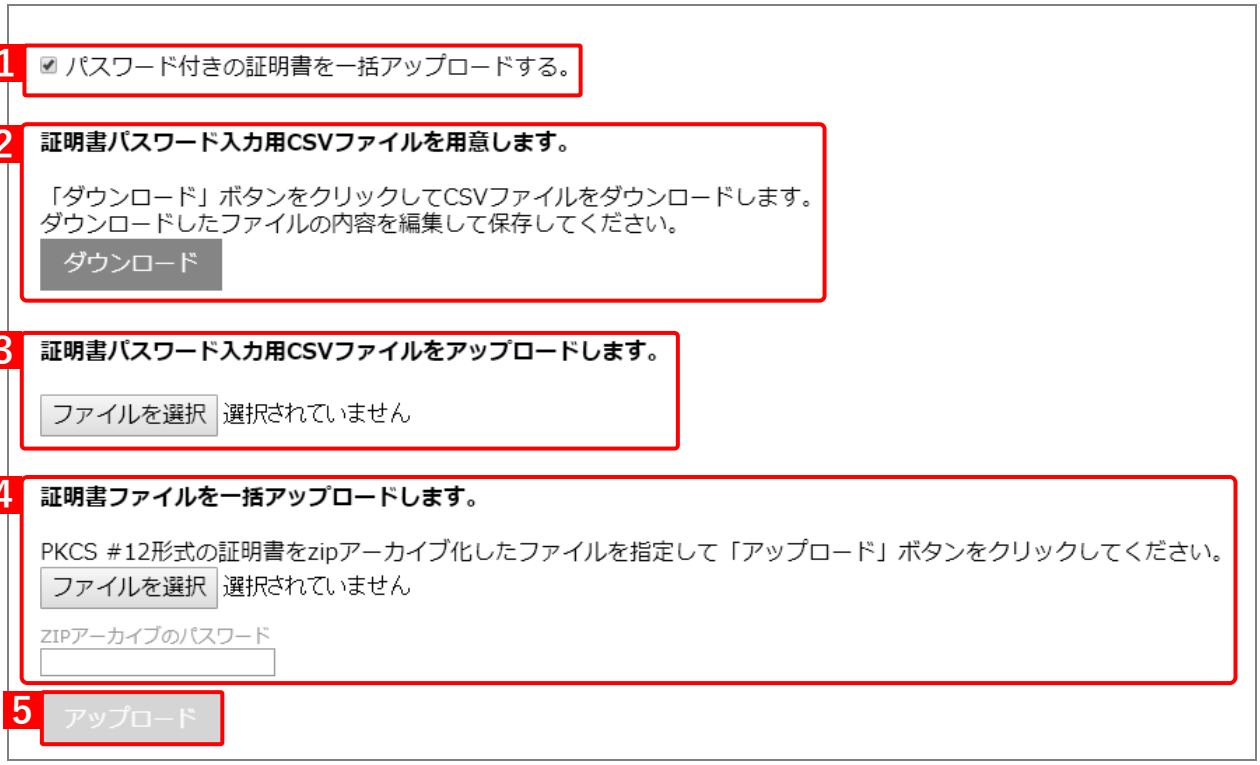
複数のクライアント証明書を ZIP ファイルにまとめて管理サイトにアップロードし、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

- 事前にクライアント証明書を取得してください。
- アップロードする複数のクライアント証明書は、まとめて zip ファイル形式で保存してください。
- アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。
  ☞「画面（編集）」556 ページ
- 管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。
  ☞「（設定－Android）クライアント証明書」79 ページ
  ☞「（設定－iOS）クライアント証明書」86 ページ
  ☞「（設定－iOS）Exchange（ActiveSync）設定」89 ページ
  ☞「（設定－iOS）VPN 設定」94 ページ
  ☞「（設定－Windows）クライアント証明書」106 ページ

◆画面

表示操作［設定］→［iOS］→［証明書管理］→［クライアント証明書一括アップロード］→［パスワード付きの証明書を一括アップロードする］



項番	項目	説明
1	パスワード付きの証明書を一括アップロードする。	チェックを入れると、証明書パスワード入力用 CSV ファイルをアップロードできます。 パスワード付きのクライアント証明書でない場合は、チェックを入れません。

項番	項目	説明
2	証明書パスワード入力用 CSV ファイルを用意します。	証明書パスワード入力用 CSV ファイルをアップロードする場合、［ダウンロード］をクリックし、任意の場所に証明書パスワード入力用 CSV ファイルを保存します。保存したファイルを Excel やメモ帳で開き、クライアント証明書に設定されているパスワードを入力して保存します。 CSV ファイルの「[S]ファイル名」には、拡張子を除いたクライアント証明書のファイル名を入力してください。
3	証明書パスワード入力用 CSV ファイルをアップロードします。	［ファイルを選択］をクリックし、証明書パスワード入力用 CSV ファイルを選択します。
4	証明書ファイルを一括アップロードします。	［ファイルを選択］をクリックし、アップロードする ZIP ファイルを選択します。パスワードで保護された ZIP ファイルを選択した場合は、「ZIP アーカイブのパスワード」に設定されているパスワードを 255 文字以内の半角英数字で入力します。 一括でアップロードする PKCS #12 形式のクライアント証明書のファイルは、あらかじめ ZIP ファイルにまとめておく必要があります。 ファイル名は 30 文字以内で設定してください。
5	［アップロード］	クリックすると、ZIP ファイルに含まれるクライアント証明書の一覧が表示されます。表示内容に問題がないことを確認し、［アップロードを実行］をクリックします。 アップロード済みの同名のクライアント証明書を上書きする場合は「同じファイル名の証明書がすでに存在した場合は上書き保存する」にチェックを入れます。

8.8.3 クライアント証明書一括削除

管理サイトにアップロードされているクライアント証明書を、CSV ファイルを利用して一括で削除します。

操作手順については、以下を参照してください。

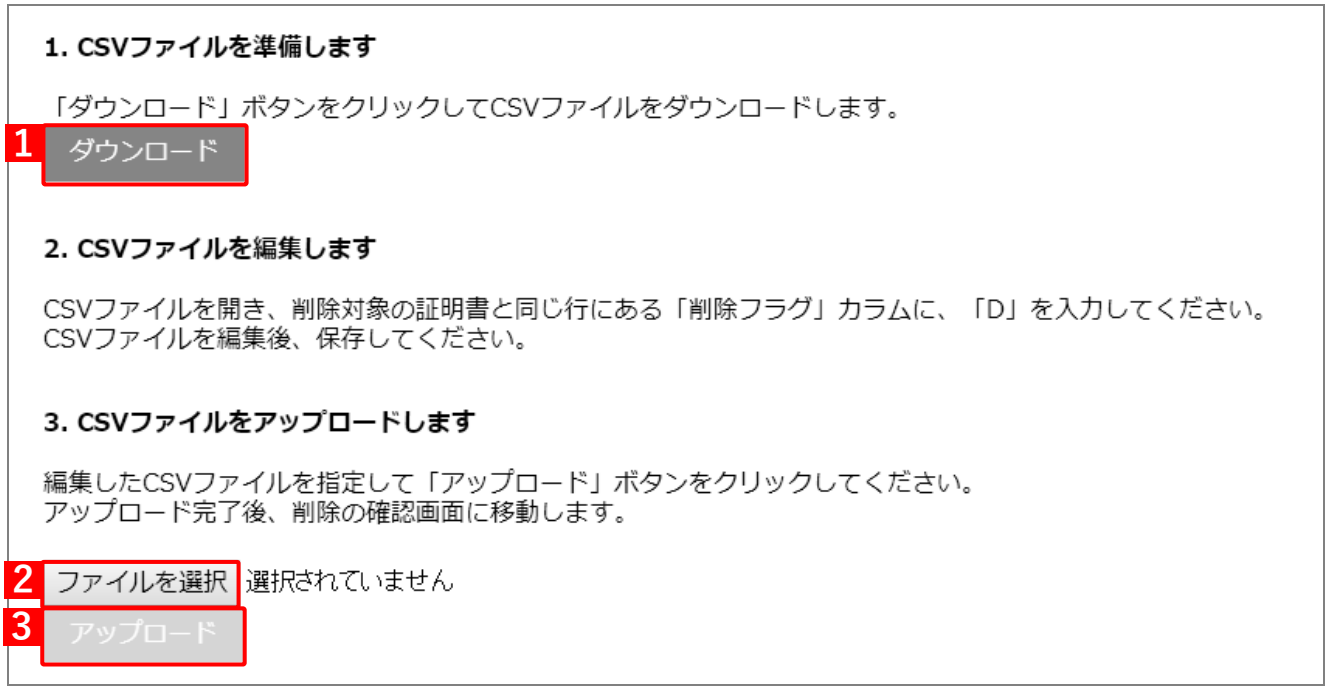
『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

端末に紐づけられているクライアント証明書を削除した場合は、端末に割り当てられている設定が動作しなくなることがあります。

削除対象のクライアント証明書は、管理サイトおよび iOS 端末から削除されます。

◆画面

表示操作　［設定］→［iOS］→［証明書管理］→［クライアント証明書一括削除］



項番	項目	説明
1	［ダウンロード］	任意の場所にクライアント証明書を削除するための CSV ファイルを保存します。保存した CSV ファイルを Excel やメモ帳で開き、削除したいクライアント証明書名の右側にある「[S]削除フラグ」列に「D」と入力して保存します。
2	［ファイルを選択］	項番 1 で保存した CSV ファイルを選択します。
3	［アップロード］	CSV ファイルのアップロードが開始されます。アップロードが完了すると、インポート画面が表示されます。

9 設定－Windows

この章では、サブヘッダーメニューの［Windows］画面に表示される、各種の設定について説明します。

注意

●システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本製品の機能を利用できないことがあります。グループポリシーについては、システム管理者に問い合わせてください。

9.1 管理アプリの通信と動作

管理サイトに登録されているすべての Windows 端末に、共通する以下の操作を適用します。

●管理サーバーとの通信間隔
管理サイトと Windows エージェントアプリが行う定期的な同期の間隔を設定できます。

●ロック
管理サーバーと通信できなかった場合に、端末画面をロックするまでの時間を設定できます。

●ロックメッセージ
ロック画面上にメッセージを表示します。

●端末でのリモートロックの解除方法
管理サイトからのロック解除または、パスワード入力による解除を選択します。

●端末でのエージェント停止・ライセンス解除・アンインストールの制限
エージェントアプリを停止、ライセンス解除を行うときに必要なパスワードを設定できます。

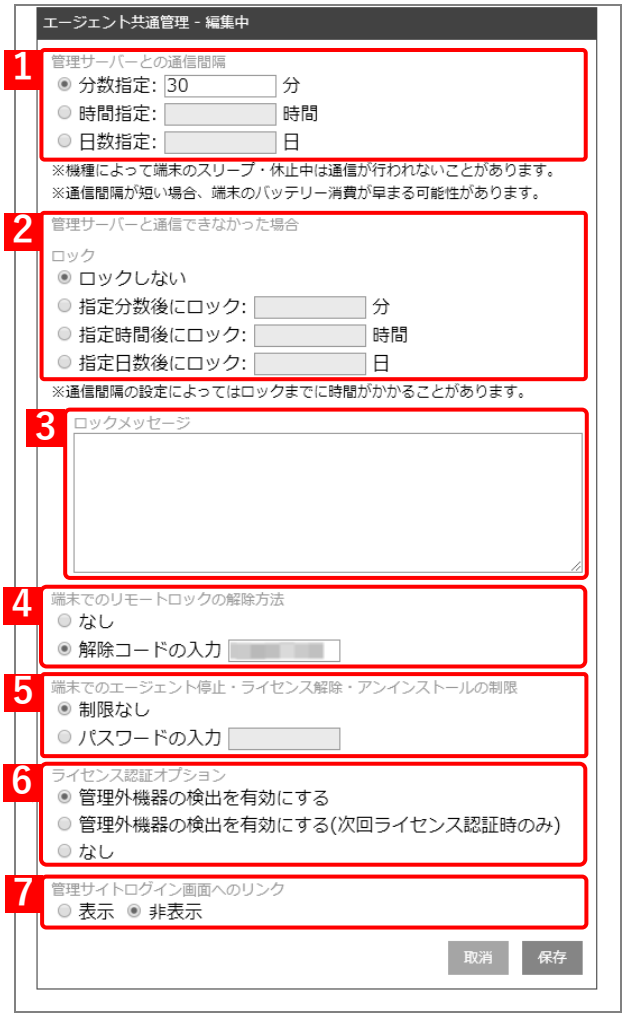
●ライセンス認証オプション
ライセンス認証時に管理外機器の検出を有効にするか設定できます。

●管理サイトログイン画面へのリンク
エージェントアプリから、管理サイトへの URL を表示するか設定できます。

設定を保存した時点ですべての Windows 端末に適用されます。ただし、設定が端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。

◆画面

表示操作［設定］→［Windows］→［管理アプリの通信と動作］→［編集］



項番	項目	説明
1	管理サーバーとの通信間隔	端末が管理サーバーと定期的に同期する間隔を以下から選択して設定します。初期設定では、「分数指定」の「30 分」に設定されています。 ●分数指定 指定した分数間隔で同期を行います。10 から 59 の半角数字を入力します。 ●時間指定 指定した時間間隔で同期を行います。1 から 23 の半角数字を入力します。 ●日数指定 指定した日数間隔で同期を行います。1 から 365 の半角数字を入力します。 機種によって端末のスリープ中は通信が行われないことがあります。 通信間隔が短い場合、端末のバッテリー消費が早まる可能性があります。
2	ロック	管理サーバーと Windows 端末が同期できなくなった場合、Windows 端末をロックするタイミングを以下から選択して設定します。初期設定では「ロックしない」に設定されています。 ●ロックしない リモートロックを行いません。 ●指定分数後にロック 指定した分数経過するとリモートロックを行います。10 から 59 の半角数字を入力します。 ●指定時間後にロック 指定した時間経過するとリモートロックを行います。1 から 23 の半角数字を入力します。 ●指定日数後にロック 指定した日数経過するとリモートロックを行います。1 から 365 の半角数字を入力します。 通信間隔の設定によってはロックまでに時間がかかることがあります。
3	ロックメッセージ	ロック中の Windows 端末の画面にメッセージを表示したい場合に、1 から 200 文字で入力します。 ロック画面上では、入力したメッセージの前後にある空白は削除されます。
4	端末でのリモートロックの解除方法	リモートロックの解除方法を設定できます。 ●なし リモートロックの解除は管理サイトからのみできます。 ●解除コードの入力 リモートロックによるロック画面で使用する解除コードを 4 文字から 20 文字以内の半角英数字で設定します。ロック画面から解除コードを入力すると、ロックを解除できます。 初期設定ではランダムな 8 文字のパスワードが設定されています。
5	端末でのエージェント停止・ライセンス解除・アンインストールの制限	エージェントアプリからライセンスを解除する場合や、アンインストールする場合に、パスワードを要求する設定ができます。 ●制限なし パスワードを入力せずにライセンス解除やアンインストールできます。 ●パスワードの入力 ライセンス解除やアンインストールするときにパスワードの入力が必要です。パスワードは 4 文字から 20 文字以内の半角英数字で入力します。 初期設定では「制限なし」が設定されております。

項番	項目	説明
6	ライセンス認証オプション	ライセンス認証時に、管理外機器の検出を有効にするかどうかを以下から選択します。 ●管理外機器の検出を有効にする ライセンス認証のたびに管理外機器の検出を有効にしたい場合、選択します。ライセンス認証後も「なし」へ変更されることはありません。 ●管理外機器の検出を有効にする（次回ライセンス認証時のみ） 設定後、ライセンス認証が一度終わると、設定は自動的に「なし」へ変更されます。常に管理外機器の検出を有効にしたい場合は、「管理外機器の検出を有効にする」を選択します。 ●なし 管理外機器の検出をしない場合に選択します。 すでにライセンス認証されている機器に適用されません。設定完了後にライセンス認証される機器のみに適用されます。 初期設定では「管理外機器の検出を有効にする（次回ライセンス認証時のみ）」が設定されており、ライセンス認証が一度終わると「なし」へ設定が変更されます。 「なし」に設定している場合でも、管理外機器検出を実施しているネットワークは、継続して管理外機器を検出します。新しく接続したネットワークでは、管理外機器検出は実施されません。
7	管理サイトログイン画面へのリンク	エージェントに管理サイトログイン画面へのリンクを表示するか選択します。 ●表示 エージェントに管理サイトログイン画面へのリンクを表示します。 ●非表示 エージェントに管理サイトログイン画面へのリンクを表示しません。

9.2 設定テンプレート

各機能で設定した設定セットの内容を、設定テンプレートとして保存します。

複数の Windows 端末に同じ設定内容を繰り返し設定したい場合や、用途に応じて設定内容を切り替えたいときにテンプレートを使用すると、簡単に設定内容を適用することができます。

本機能では、設定テンプレートの作成や作成したテンプレートをデフォルトに設定するなどの操作を行うことができます。

画面

画面（設定テンプレートの作成）

設定テンプレートを一括で複数の Windows 端末に適用できません。

テンプレートとして登録したい各機能の設定セットを、あらかじめ作成してください。

作成した設定テンプレートは、Windows 端末ごと、または組織ごとに適用することができます。

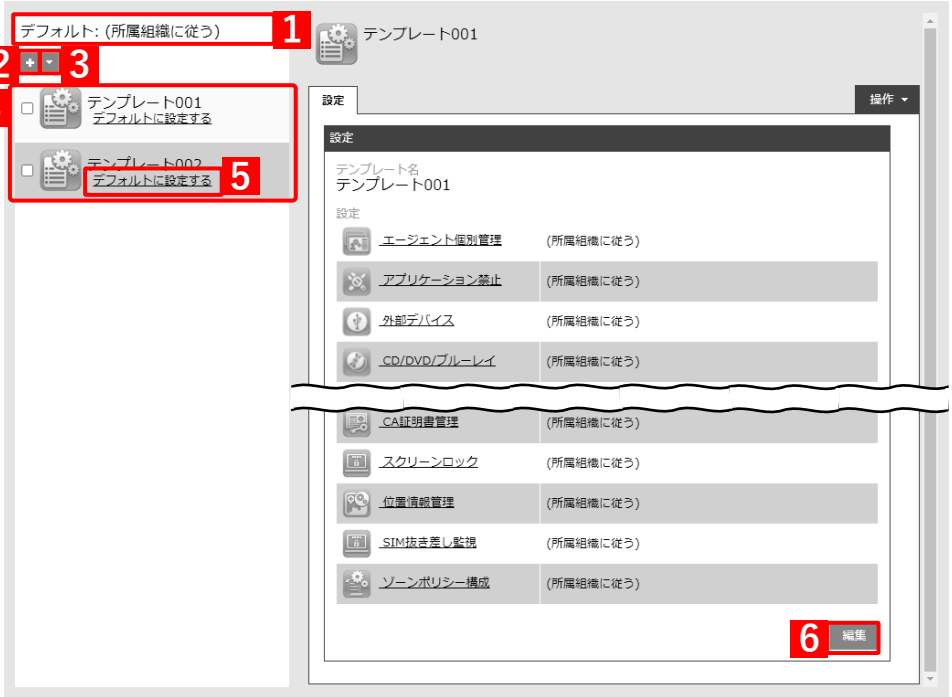
「（設定－Windows）設定テンプレートの割り当て」105 ページ

「［Android 設定］タブ／［iOS 設定］タブ／［Windows 設定］タブ」286 ページ

設定テンプレートは、最大 51 件まで作成できます。

◆画面

表示操作 ［設定］→［Windows］→［設定テンプレート］

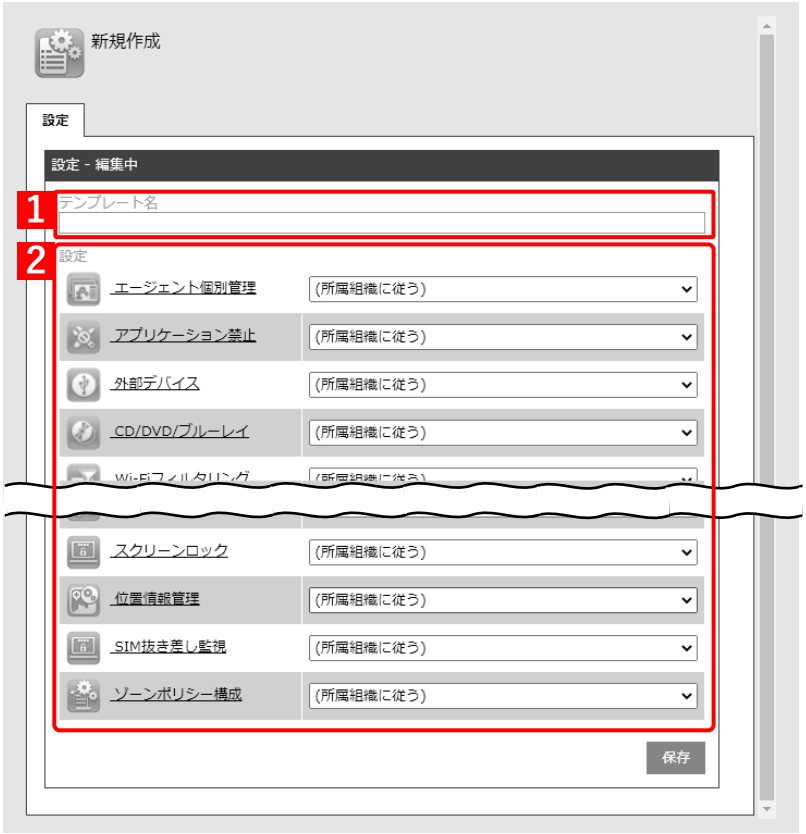


項番	項目	説明
1	デフォルトテンプレート表示	デフォルトに設定したテンプレートの名称が表示されます。 デフォルトに設定したときは、「(所属組織に従う)」が表示されます。 「(所属組織に従う)」は設定テンプレートの初期設定値です。
2	＋	設定テンプレートを新規に作成します。 「画面（設定テンプレートの作成)」565 ページ

項番	項目	説明
3	▼	設定テンプレートのチェックや、チェックした設定テンプレートの一括削除のほか、デフォルトに設定した設定テンプレートを初期値の「(所属組織に従う)」に戻します。 ☞「(所属組織に従う)をデフォルトに設定する」567 ページ
4	設定テンプレート	＋で作成した設定テンプレートが表示されます。
5	［デフォルトに設定する］	作成した設定テンプレートをデフォルトにします。 ☞「設定テンプレートをデフォルトに設定する」566 ページ
6	［編集］	設定テンプレートを編集します。 ☞「画面（設定テンプレートの作成)」565 ページ

◆画面（設定テンプレートの作成）

表示操作［設定］→［Windows］→［設定テンプレート］→ ＋



項番	項目	説明
1	テンプレート名	設定テンプレートの名称を 1 文字から 30 文字で入力します。
2	設定	各機能に設定する内容を以下から選択します。 ●各機能の設定名 各機能で作成した設定名を指定します。指定した設定名に対する編集および削除が行われた場合、設定テンプレートにも反映されます。 ●(所属組織に従う) 機器ごとに所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(変更しない) 機器ごとに適用している設定に変更を行いません。 ●(設定なし) 各機能の設定を外します。 リモートワイプは対象機器をご確認の上、設定してください。

設定テンプレートをデフォルトに設定する

作成した設定テンプレートをデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が設定テンプレートの内容に設定されます。

管理サイトに登録する端末を同じ設定にしたい場合に便利です。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［Windows］→［設定テンプレート］→デフォルトにするテンプレートの「デフォルトに設定する」

項番	項目	説明
1	デフォルト	デフォルトに設定しているテンプレート名が表示されます。また、デフォルトになっているテンプレート名の下に「デフォルト」と表示されます。(A)の箇所に記載されます。
2	［デフォルトに設定する］	クリックすると、そのテンプレート名の設定をデフォルトにできます。
3	メッセージボックス	選択したテンプレートをデフォルトにすることを確認する画面です。 ●OK 選択したテンプレートをデフォルトに設定します。 ●キャンセル 選択したテンプレートをデフォルトに設定することを中断します。

(所属組織に従う)をデフォルトに設定する

「(所属組織に従う)」をデフォルトに設定すると、ライセンス認証して管理サイトに登録された端末は、各設定セットの内容が「(所属組織に従う)」に設定されます。

初期設定では、デフォルトに「(所属組織に従う)」が設定されています。

作成した設定テンプレートが設定されていない場合は、「(所属組織に従う)」がデフォルトに設定されます。

表示操作　［設定］→［Windows］→［設定テンプレート］→ ▼ →［(所属組織に従う)をデフォルトにする］

項番	項目	説明
1	(所属組織に従う)をデフォルトにする	各種設定内容が「(所属組織に従う)」になるテンプレートをデフォルトにします。
2	メッセージボックス	デフォルトに設定することを確認する画面です。 ●OK 「(所属組織に従う)」をデフォルト設定します。 ●キャンセル 設定を行いません。

9.3 セキュリティ

本機能では、スクリーンロックのパスワード設定、暗号化の設定、位置情報の取得、システムセキュリティの設定／診断、外部デバイス接続の制限、CD／DVD／ブルーレイの制限について、設定セットを作成します。

9.3.1 画面ロック

Windows 標準のスクリーンセーバーとログインパスワードについて制限を設けるための設定セットを作成します。

パスワードの文字数や英数字利用の指定、パスワードの有効期限、スクリーンロック解除の失敗に応じてワイプを行う設定などができます。

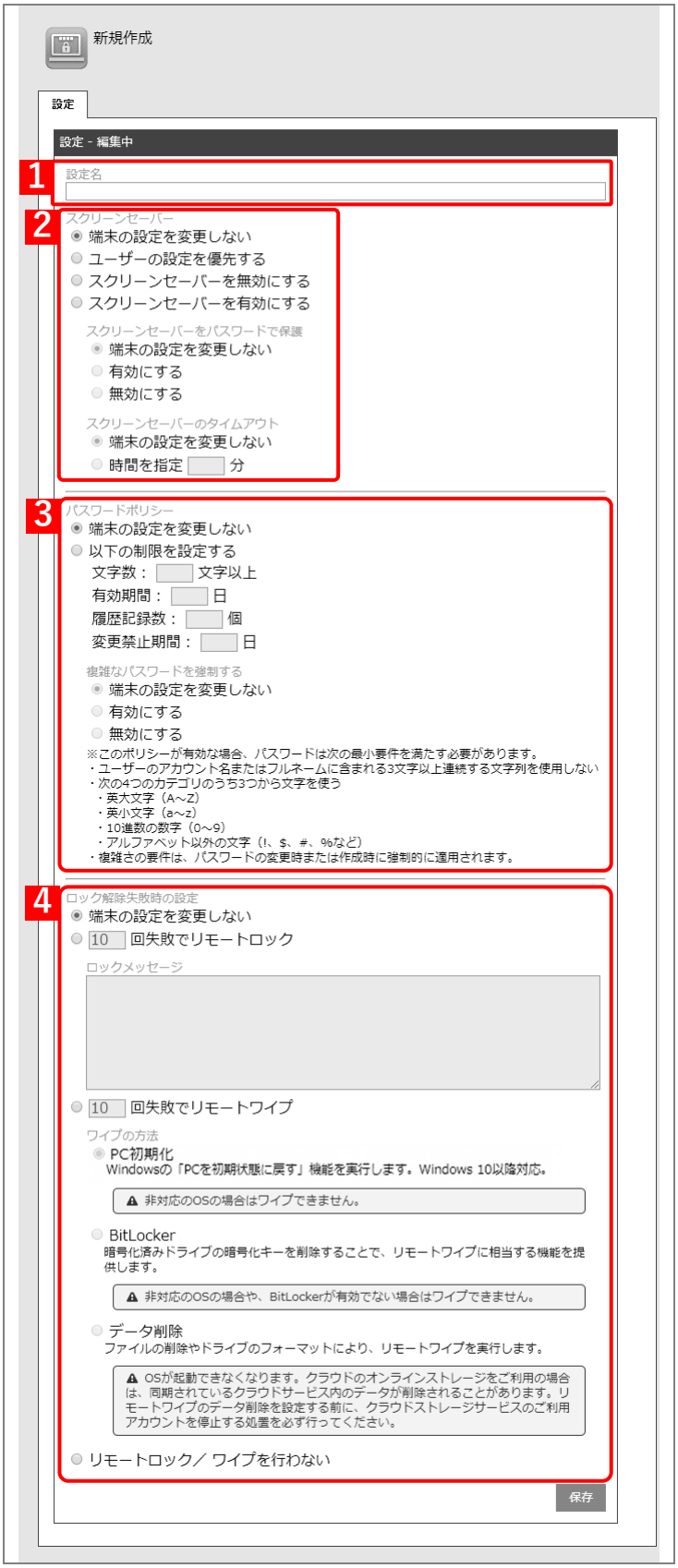
- 本機能はパスワードのポリシーを定めますが、パスワード自体を管理するのは Windows OS です。管理サイトではパスワードの保持を行いませんのでご注意ください。
- Windows 端末にグループポリシーが適用されている場合、グループポリシーのスクリーンセーバー設定が優先されます。また、本機能は Windows 端末のコントロールパネルから設定したスクリーンセーバー設定よりも優先されます。
- 一部の Windows エディション（「Starter」、「Home」、通常版の一部）ではスクリーンセーバーの設定はできません。
- 対象端末が Windows ドメインで管理されている場合、本機能の設定を端末に反映するには、ドメインでのスクリーンセーバーの設定を「未構成」にする必要があります。またパスワードポリシーの設定は、Windows ドメインで管理されている端末に反映できません。
- パスワードポリシーの「有効期間」を「0 日」に設定した場合、パスワードの期限は設定されず、無期限となります。
- パスワードポリシーは、基本的に本機能を端末に適用後、パスワードの変更時または作成時に適用されます。ただし「有効期間」については、本機能を端末に適用時から有効となります。
- 作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

☞「（設定－Windows）設定セットの割り当て」103 ページ
☞「全機器一括設定」200 ページ

- 設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［セキュリティ］→［画面ロック］→ ✚ （一覧から対象を選択→［編集］）



項番	項目		説明
1	設定名		設定の名称を 1 文字から 30 文字で入力します。
2	スクリーンセーバー		Windows スクリーンセーバーの制限を選択します。
		端末の設定を変更しない	現在の設定を変更しません。
		ユーザーの設定を優先する	一度本機能で「スクリーンセーバーを無効にする」または「スクリーンセーバーを有効にする」の設定を適用後、ユーザーが端末上でスクリーンセーバーの設定ができるように戻す場合に選択します。
		スクリーンセーバーを無効にする	スクリーンセーバーの設定を解除し、ユーザーが端末からスクリーンセーバーの設定を変更できないようにします。
		スクリーンセーバーを有効にする	スクリーンセーバーを有効に設定し、パスワードによる保護とタイムアウトの時間を設定します。 ●スクリーンセーバーをパスワードで保護 スクリーンセーバーを解除するときのパスワード入力について設定します。 ・端末の設定を変更しない 一度本機能で「有効にする」または「無効にする」の設定を適用後、ユーザーが端末上でスクリーンセーバーのパスワード保護設定が変更できるように戻す場合に選択します。 ・有効にする スクリーンセーバーを解除するときにパスワード入力を要求します。また、ユーザーがスクリーンセーバーのパスワード保護設定を変更できないようにします。 「有効にする」を選択しても、端末上でパスワードが設定されていない場合は、パスワード保護がかかりませんのでご注意ください。 ・無効にする スクリーンセーバーを解除するときにパスワード入力を要求されません。また、ユーザーがスクリーンセーバーのパスワード保護設定を変更できないようにします。 ●スクリーンセーバーのタイムアウト スクリーンセーバーを起動するまでのタイムアウト時間（待ち時間）を設定します。 ・端末の設定を変更しない 一度本機能で「時間を指定」を適用後、ユーザーが端末上でスクリーンセーバーのタイムアウト設定が変更できるように戻す場合に選択します。 ・時間を指定〇分 スクリーンセーバーを起動するまでのタイムアウト時間（待ち時間）を 1 から 1,440 の分数で設定します。またユーザーがスクリーンセーバーのタイムアウト設定を変更できないようにします。
3	パスワードポリシー		ロック画面で入力するパスワードの制限を選択します。
		端末の設定を変更しない	現在の設定を変更しません。
		以下の制限を設定する	●文字数 パスワードの最小の入力文字数を 1 から 14 の半角数字で入力します。例えば、文字数に「5」を指定した場合は、5 文字以上のパスワードを入力する必要があります。 ●有効期間 パスワードの有効期限を日数指定します。入力数を 0 から 999 の半角数字で入力します。 パスワードポリシーの「有効期間」を「0 日」に設定した場合、パスワードの期限は設定されず、無期限となります。 ●履歴記録数 一度使用したパスワードを再利用できるまでに必要なパスワード変更回数を指定します。指定した回数を超えない限り、使用したことがある

項番	項目		説明
			パスワードの再使用を禁止します。入力数を 0 から 999 の半角数字で入力します。 ●変更禁止期間 パスワードの変更を禁止する日数を指定します。入力数を 0 から 998 の半角数字で入力します。 有効期間が 0 日以外の場合、禁止期間は有効期間日数よりも少ない数値で指定してください（998 まで）。 ●複雑なパスワードを強制する Windows で決められた複雑さの要件を強制します。複雑さの要件についての詳細については、以下の URL を参照してください。 ・端末の設定を変更しない 端末の設定は変更せず、端末で決められた設定にしたがいます。 ・有効にする 複雑なパスワードを強制します。 ・無効にする 複雑なパスワードを強制しません。
4	ロック解除失敗時の設定		ロック解除に失敗した場合の動作を設定します。
		端末の設定を変更しない	現在の設定を変更しません。
		○回失敗でリモートロック	ロックの解除に指定回数失敗した場合は、自動的にリモートロックするように設定 ●ロックメッセージ 200 文字以内で入力してください。
		○回失敗でリモートワイプ	ロックの解除に指定回数失敗した場合は、自動的にワイプするように設定します。回数は 2 から 50 の半角数字で入力します。また、以下からワイプ方法を選択します。 「BitLocker」、「データ削除」の詳細については、以下を参照してください。 ☞「［その他▼］タブ／Windows リモート操作」215 ページ ●PC 初期化 Windows の「PC を初期状態に戻す」機能を実行します。 工場出荷時のリカバリー領域が必要です。リカバリー領域がないと、リモートワイプに失敗します。 ●BitLocker BitLocker で暗号化済みドライブの回復キー以外のキープロテクターを削除します。 BitLocker でのワイプを実行したあとは、端末を起動したときに BitLocker の回復キー入力画面が表示されます。回復キーを入力するまでドライブのデータにアクセスできません。 回復キーのキープロテクターがないドライブは、BitLocker でのワイプができません。 削除した回復キーを新規で作成するには、以下の URL で「構文」と「パラメーター」を参照してください。回復キーの作成方法については、システム管理者に問い合わせてください。 ☞ https://learn.microsoft.com/ja-jp/windows-server/administration/windows-commands/manage-bde-protectors 本製品の暗号化機能を利用している場合は、暗号化機能の設定セットを無効、有効の順で割り当てて同期すると、回復キーを遠隔で新規作成することができます。 BitLocker 以外の暗号化ツールを使用している場合は、本機能は使用できません。 Windows 11 Pro/Enterprise/Education の端末に対応しています。詳細については、以下を参照してください。

項番	項目		説明
			「暗号化」573 ページ BitLocker については、Microsoft の Web サイトを参照してください。 https://learn.microsoft.com/ja-jp/windows/security/operating-system-security/data-protection/bitlocker/ 回復キーとは、48 桁の文字列です。回復パスワードという場合もあります。詳細については、以下を参照してください。 「（情報－Windows）セキュリティ」181 ページ ●データ削除 ファイルの削除やドライブのフォーマットにより、リモートワイプを実行します。 OS が起動できなくなることがあります。クラウドのオンラインストレージをご利用の場合は、同期されているクラウドサービス内のデータが削除されることがあります。リモートワイプのデータ削除を設定する前に、クラウドストレージサービスのご利用アカウントを停止する処置を必ず行ってください。 通信間隔の設定によってはワイプまでに時間がかかることがあります。
		リモートロック／ワイプを行わない	ロックの解除に失敗した場合、リモートロック、ワイプを行いません。

9.3.2 暗号化

Windows 端末に搭載されている BitLocker を使用し、システムドライブおよびデータドライブのデータを暗号化するための設定セットを作成します。

本機能は BitLocker 機能を備える、Windows 11 Pro/Enterprise/Education に対応しています。ただし、以下に該当する端末については対象外です。

●すでに本製品以外の暗号化ツールを導入している端末

●デュアルブート環境およびパーティション変更ツールなどを導入している端末

また、上記の条件を満たす場合でも以下を参照し、必ず事前に Windows 端末が暗号化できるか確認してください。

☞「確認手順」574 ページ

本機能で、暗号化が行えない場合や BitLocker のオプション機能が必要な場合は、手動で暗号化することもご検討ください。

ドライブレターが割り当てられていないドライブは暗号化の対象になりません。ドライブレターを設定してから暗号化を行うか、手動で暗号化を行ってください。

回復キーについては、以下を参照してください。

☞「（情報－Windows）セキュリティ」181 ページ

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

☞「（設定－Windows）設定セットの割り当て」103 ページ
☞「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆確認手順

以下の手順で、Windows 端末が暗号化できるか確認してください。

複数の Windows 端末がある場合は、同様の条件であれば、1 台だけの確認で問題ありません。

【1】暗号化を有効にした設定セットを作成します。

【2】Windows 端末に上記の設定セットを割り当てます。

【3】Windows 端末でタスクトレイの Optimal Biz エージェントのアイコンを右クリックして、［同期］をクリックします。

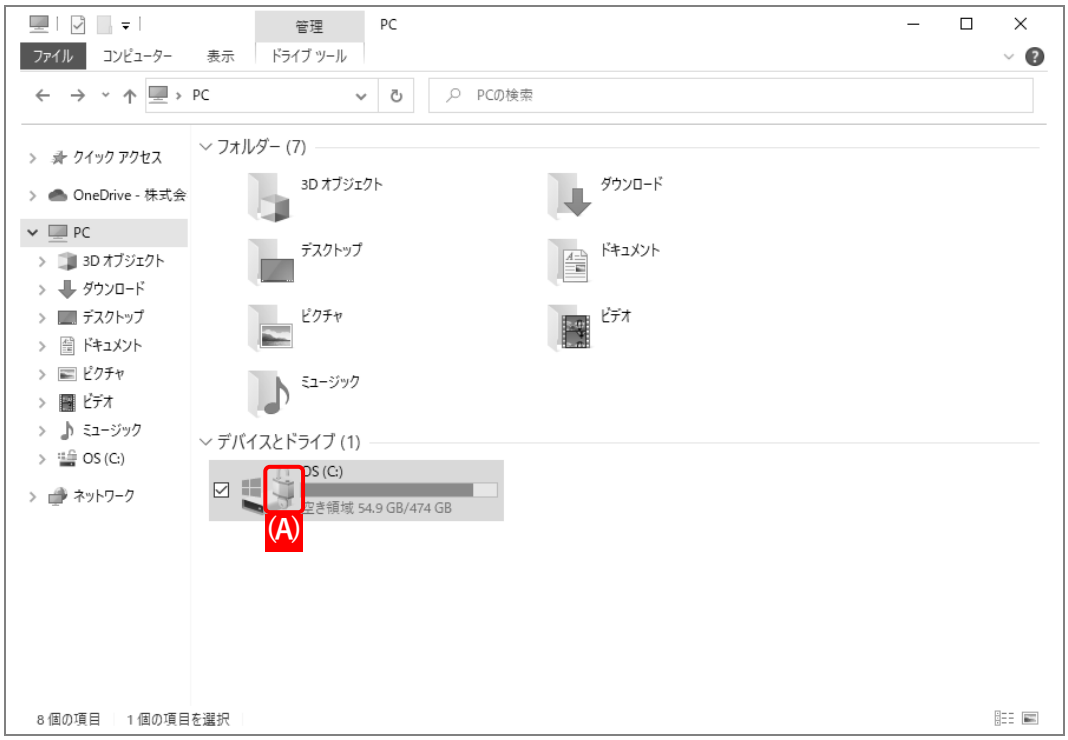
TPM の有効化や再起動を促すダイアログが表示された場合は、［OK］をクリックします。

【4】エクスプローラーを起動します。

【5】ドライブに（A）南京錠が表示されていることを確認します。

⇒正常に暗号化の設定ができます。

南京錠が表示されていない場合は、ドライブの右クリックメニューの［BitLocker を有効にする］から、手動で暗号化ができるか試してください。手動でも暗号化ができない場合は、Windows 端末が BitLocker を有効にする要件を満たしていないため、本機能で暗号化することはできません。

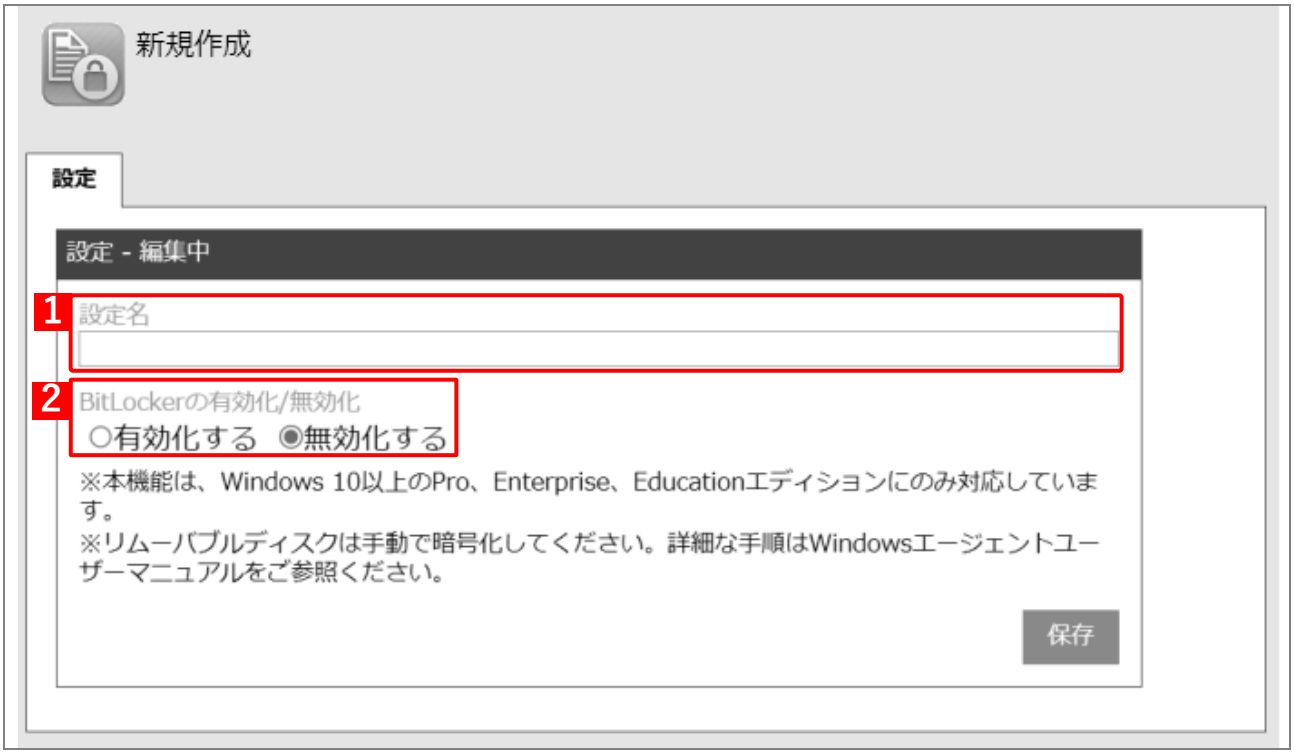


【6】Windows 端末を再起動して、正常に起動できることを確認します。

◆画面

表示操作　［設定］→［Windows］→［セキュリティ］→［暗号化］→ ＋ （一覧から対象を選択→［編集］）

設定セットは、最大 50 件まで作成できます。



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	BitLocker の有効化／無効化	BitLocker の暗号化利用可否を指定します。 ●有効化する ●無効化する リムーバブルディスクは手動で暗号化してください。詳細については、Microsoft の Web サイトを参照してください。 Microsoft - BitLocker ドライブ暗号化

9.3.3 位置情報管理

Windows 端末で位置情報を取得する契機を指定するための設定セットを作成します。取得した位置情報を確認する場合は、以下を参照してください。

「（情報－Windows）位置」183 ページ

使用している Windows 端末の位置情報をオンに設定してください。

位置情報の設定方法については、Windows 端末の取扱説明書、または Microsoft の Web サイトを参照してください。

https://support.microsoft.com/ja-jp/windows/windows-%E3%81%AE%E4%BD%8D%E7%BD%AE%E6%83%85%E5%A0%B1%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%A8%E3%83%97%E3%83%A9%E3%82%A4%E3%83%90%E3%82%B7%E3%83%BC-3a8eee0a-5b0b-dc07-eede-2a5ca1c49088#windowsversion=windows_11

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

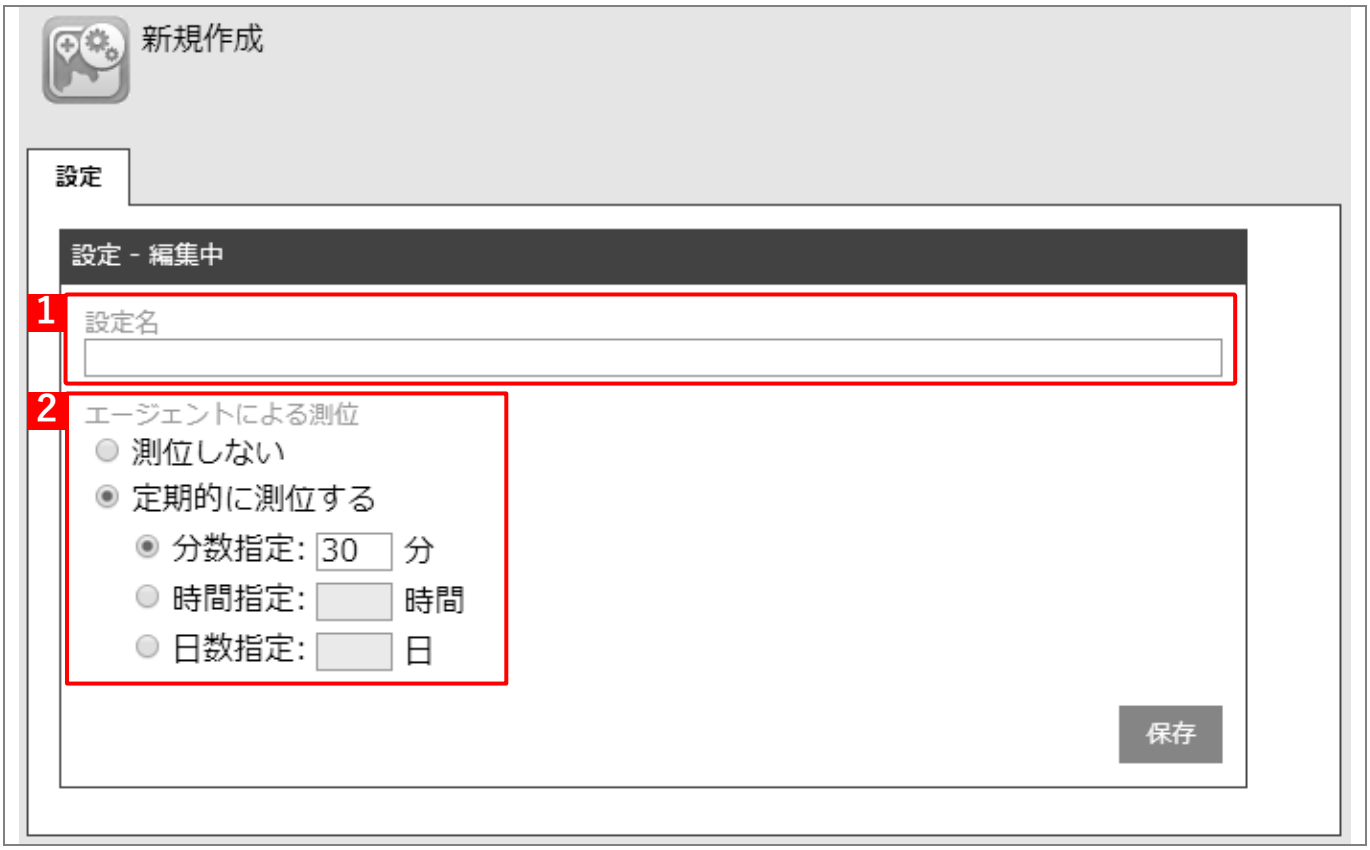
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［セキュリティ］→［位置情報管理］→ ＋ （一覧から対象を選択→［編集］）



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	エージェントによる測位	エージェント側の位置情報の測位の契機を以下から選択します。 ●測位しない エージェント側では、位置情報を測位しません。ただし、管理サイトから「同期」を指示した場合は、端末の位置情報を測位します（契機 1）。 ●定期的に測位する 契機 1 に加え、測位する契機を分数指定、時間指定、日数指定から選択できます。 ・分数指定 指定した分数間隔で測位する場合に選択します。分数は 10 から 59 の半角数字で入力します。 ・時間指定 指定した時間間隔で測位する場合に選択します。時間は 1 から 23 の半角数字で入力します。 ・日数指定 指定した日数間隔で測位する場合に選択します。日数は 1 から 365 の半角数字で入力します。 端末の位置情報の無線ネットワークと GPS が無効の場合、測位を行いません。 この設定値は、機器で位置情報を測位する周期で使用します。 管理サーバーへ位置情報を同期する設定値は、［設定］の［管理アプリの通信と動作］にある「管理サーバーとの通信間隔」で設定できます。 「管理アプリの通信と動作」561 ページ

9.3.4 システムセキュリティ

Windows 端末のシステムセキュリティに設定および診断を行うための設定セットを作成します。

診断結果に問題がある場合はログに出力されます。ログの確認は以下を参照してください。

「ログ」645 ページ

システムでグループポリシーが設定されている場合は、グループポリシーが優先され、本機能を利用できないことがあります。グループポリシーについては、システム管理者に問い合わせてください。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

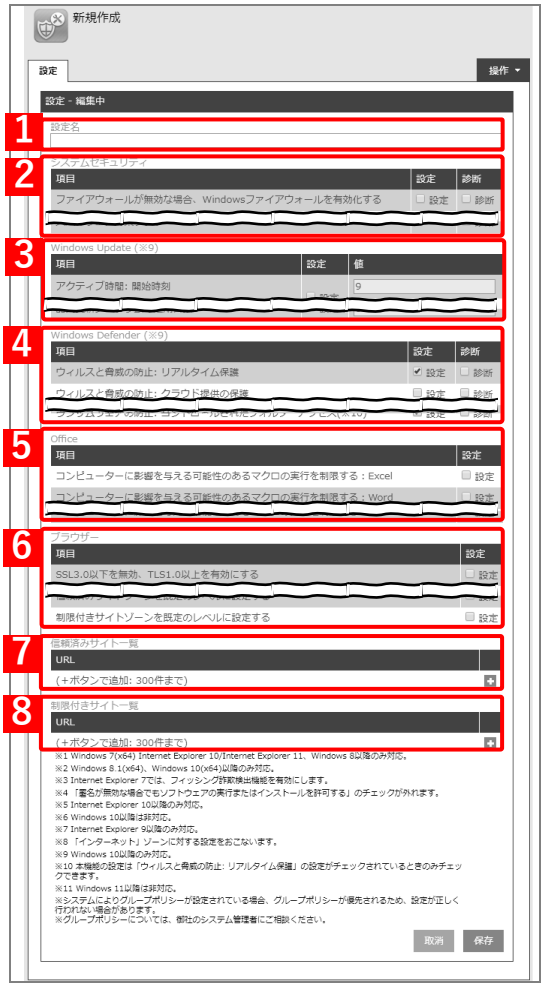
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［セキュリティ］→［システムセキュリティ］→ ＋ （一覧から対象を選択→［編集］）



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	システムセキュリティ	項目ごとに設定／診断を行うか指定します。詳細については、以下を参照してください。 「システムセキュリティ項目」579 ページ

項番	項目	説明
3	Windows Update	項目ごとに設定と値を指定します。詳細については、以下を参照してください。 ☞「Windows Update」580 ページ
4	Windows Defender	項目ごとに設定／診断を行うか指定します。詳細については、以下を参照してください。 ☞「Windows Defender」582 ページ
5	Office	項目ごとに設定を行うか指定します。項目の詳細については、以下を参照してください。 ☞「Office 項目」583 ページ 「Office」の設定対象バージョンは、Office 2007／2010／2013／2016 です。
6	ブラウザー	項目ごとに設定を行うか指定します。項目の詳細については、以下を参照してください。 ☞「ブラウザー項目」583 ページ 本機能はサポートされていません。
7	信頼済みサイト一覧	インターネットオプションの「信頼済みサイト」の URL 登録を行います。登録できる URL は 300 件です。URL は 200 文字以内の半角英数字と記号で入力します。 本機能はサポートされていません。
8	制限付きサイト一覧	インターネットオプションの「条件付きサイト」の URL 登録を行います。登録できる URL は 300 件です。URL は 200 文字以内の半角英数字と記号で入力します。 「*」（アスタリスク）によるワイルドカードが利用できます。 指定した URL の閲覧を制限する機能ではありません。 本機能はサポートされていません。

◆システムセキュリティ項目

診断を有効にすると、各項目の端末の状態を確認します。端末に該当の設定が行われていなかった場合、ログにアラートと診断結果が出力されます。

項目	設定／診断	説明
ファイアウォールが無効な場合、Windows ファイアウォールを有効化する	設定	●チェックを入れると Windows ファイアウォールを有効にします。すでに有効な場合は何も行いません。Windows のグループポリシーが設定済みの場合は何も行いません。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
	診断	●チェックを入れると Windows ファイアウォールの状態を診断します。 ●チェックを外すと何も行いません。
Windows の Guest アカウントを無効化する	設定	●チェックを入れると Windows の Guest アカウントを無効にします。すでに無効な場合は何も行いません。Windows のグループポリシーが設定済みの場合は何も行いません。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
	診断	●チェックを入れると Windows の Guest アカウントの状態を診断します。 ●チェックを外すと何も行いません。
Windows の更新を自動インストールする	設定	●チェックを入れると Windows の自動更新を有効にします。すでに有効な場合は何も行いません。Windows のグループポリシーが設定済みの場合は何も行いません。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 本機能はサポートされていません。

項目	設定／診断	説明
	診断	●チェックを入れると Windows の自動更新の状態を診断します。 ●チェックを外すと何も行いません。 本機能はサポートされていません。
Windows の更新時に他の Microsoft 製品の更新プログラムを入手する	設定	●チェックを入れると Windows の更新時に他の Microsoft 製品の更新プログラムをダウンロードします。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
	診断	●チェックを入れると他の Microsoft 製品の更新プログラムの入手状態を診断します。 ●チェックを外すと何も行いません。
スクリーンセーバーの解除時にようこそ画面に戻る	設定	●チェックを入れるとスクリーンセーバー解除時にようこそ画面を表示する設定に変更します。すでに表示する設定になっている場合は何も行いません。Windows のグループポリシーが設定済みの場合は何も行いません。 端末のスクリーンセーバーの設定にある「再開時にログオン画面に戻る」が有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
	診断	●チェックを入れるとスクリーンセーバー解除時の状態を診断します。 ●チェックを外すと何も行いません。
ウイルス対策ソフト	設定	●設定は指定できません。
	診断	●チェックを入れるとウイルス対策ソフトの状態を診断します。 セキュリティセンターに、「有効」で「最新」のウイルス対策ソフトが 1 つも存在しない場合、ログにアラートと診断結果が出力されます。 ●チェックを外すと何も行いません。
スパイウェア対策ソフト	設定	●設定は指定できません。
	診断	●チェックを入れるとスパイウェア対策ソフトの状態を診断します。 セキュリティセンターに、「有効」で「最新」のスパイウェア対策ソフトが 1 つも存在しない場合、ログにアラートと診断結果が出力されます。 ●チェックを外すと何も行いません。

◆Windows Update

項目	説明
アクティブ時間: 開始時刻 アクティブ時間: 終了時刻	Windows 端末を通常いつ使うかを知らせるアクティブ時間を設定します。アクティブ時間中は自動的に再起動しません。 ●設定 チェックを入れると設定したアクティブ時間が有効になります。 ●値 ・アクティブ時間: 開始時刻：「開始時刻」を設定します。 0 以上 23 以下の半角数字で入力してください。 ・アクティブ時間: 終了時刻：「終了時刻」を設定します。 0 以上 23 以下の半角数字で入力してください。 終了時刻は開始時刻から 18 時間以内に設定してください。
更新プログラムをいつインストールするかを選択	更新プログラムをインストールするタイミングを設定できます。 ●設定 チェックを入れると設定したタイミングで更新プログラムがインストールされます。 ●値

項目	説明
	更新プログラムを配信するチャネルを以下から選択します。 チャネルとは、データの通り道のことです。接続するチャネルによって、配信される更新プログラムが異なります。 ・プレビュー ビルド - ファスト 最新の開発中（Insider Preview 版）の更新プログラムが配信されます。 Windows Insider Program への参加が必要です。参加していない場合は、「半期チャネル」が適用されます。 ・プレビュー ビルド - スロー 近々リリースされる予定の開発中（InsiderPreview 版）の更新プログラムが配信されます。 Windows Insider Program への参加が必要です。参加していない場合は、「半期チャネル」が適用されます。 ・リリース プレビュー 「半期チャネル」に配信される予定の更新プログラム内容が、「半期チャネル」で配信されるよりも少し早く配信されます。 Windows Insider Program への参加が必要です。参加していない場合は、「半期チャネル」が適用されます。 ・半期チャネル（対象指定） 動作が安定しているリリース版の更新プログラムが、半年（半期）ごとに配信されます。配信の時期は「半期チャネル」と同じですが、インストールに猶予期間がありません。 バージョン 1809 以下の端末に対応しています。 バージョン 1903 以上の端末に設定した場合は、「半期チャネル」が適用されます。設定値は、機器のセキュリティ画面から確認できます。 ☞「（情報－Windows）セキュリティ」181 ページ Windows Insider Program への参加は制限されます。Insider Preview 版の更新プログラムは受け取れません。 ・半期チャネル 動作が安定しているリリース版の更新プログラムが、半年（半期）ごとに配信されます。配信されてから 2～3 か月は、インストールするか選択できる猶予期間があります。 バージョン 1903 以上の端末では、デフォルトになります。 Windows Insider Program への参加は制限されます。Insider Preview 版の更新プログラムは受け取れません。 ・1809 またはそれ以前の半期チャネル バージョン 1809 以下の旧半期チャネルから、更新プログラムが配信されます。 バージョン 1903 以上の端末に対応していますが、Microsoft から非推奨とされています。特に理由のない限り使用しないでください。 バージョン 1809 以下の端末に設定した場合は、「半期チャネル」が適用されます。設定値は、機器のセキュリティ画面から確認できます。 ☞「（情報－Windows）セキュリティ」181 ページ Windows Insider Program への参加は制限されます。Insider Preview 版の更新プログラムは受け取れません。 Windows 11 Pro/Enterprise/Education に対応しています。 本設定は、Windows 10 のローカルコンピューターポリシー（ローカルグループポリシー）の「Windows Update for Business」を利用しています。本設定を有効にすると、「Windows Update for Business」の「受信する更新プログラムの Windows 準備レベルを選択してください」と「プレビュービルドを管理にする」の設定内容が変更されます。 「Windows Update for Business」は Windows 11 以上では、「Windows Update から提供される更新プログラムの管理」という名称に変更されました。 動作が安定している更新プログラムのみを受け取りたい場合は、本項目で

項目	説明
	「半期チャネル」を設定してください。 現在、運用しているアプリへの影響が明らかになるまでは、更新プログラムの受け取りを遅らせたいなどの場合は、「機能更新プログラムの延期日数」や「品質更新プログラムの延期日数」で延期日数を指定してください。
機能更新プログラムの延期日数	機能更新プログラムとは、大型アップデート行うプログラムです。大型アップデートを行う延期日数を指定できます。 ●設定 チェックを入れると機能更新プログラムの延期日数が有効になります。 ●値 延期日数を 0 以上 365 以下の半角数字で入力します。 Windows 11 Pro/Enterprise/Education に対応しています。 本設定は、Windows 10 のローカルコンピューターポリシー（ローカルグループポリシー）の「Windows Update for Business」を利用しています。本設定を有効にすると、「Windows Update for Business」の「プレビュービルドまたは機能更新プログラムがリリースされた後、受信を延期する日数」の設定内容が変更されます。 「Windows Update for Business」は Windows 11 以上では、「Windows Update から提供される更新プログラムの管理」という名称に変更されました。
品質更新プログラムの延期日数	品質更新プログラムとは、セキュリティの問題や製品の不具合を修正するため、毎月 1 回以上提供される更新プログラムです。更新を行う延期日数を指定できます。 ●設定 チェックを入れると品質更新プログラムの延期日数が有効になります。 ●値 延期日数を 0 以上 30 以下の半角数字で入力します。 Windows 11 Pro/Enterprise/Education に対応しています。 本設定は、Windows 10 のローカルコンピューターポリシー（ローカルグループポリシー）の「Windows Update for Business」を利用しています。本設定を有効にすると、「Windows Update for Business」の「品質更新プログラムがリリースされた後、受信を延期する日数」の設定内容が変更されます。 「Windows Update for Business」は Windows 11 以上では、「Windows Update から提供される更新プログラムの管理」という名称に変更されました。

◆Windows Defender

項目	設定／診断	説明
ウィルスと脅威の防止: リアルタイム保護	設定	●チェックを入れると「ウィルスと脅威の防止: リアルタイム保護」が有効になります。 ●チェックを外すと何も行いません。
	診断	●チェックを入れると「ウィルスと脅威の防止: リアルタイム保護」の診断を行います。 ●チェックを外すと何も行いません。
ウィルスと脅威の防止: クラウド提供の保護	設定	●チェックを入れると「ウィルスと脅威の防止: クラウド提供の保護」が有効になります。 ●チェックを外すと何も行いません。
	診断	●チェックを入れると「ウィルスと脅威の防止: クラウド提供の保護」の診断を行います。 ●チェックを外すと何も行いません。

項目	設定／診断	説明
ウィルスと脅威の防止: サンプルの自動送信	設定	●チェックを入れると「ウィルスと脅威の防止: サンプルの自動送信」が有効になります。 ●チェックを外すと何も行いません。
	診断	●チェックを入れると「ウィルスと脅威の防止: サンプルの自動送信」の診断を行います。 ●チェックを外すと何も行いません。
ランサムウェアの防止: コントロールされたフォルダーアクセス　（※1）	設定	●チェックを入れると「ランサムウェアの防止: コントロールされたフォルダーアクセス」が有効になります。 ●チェックを外すと何も行いません。
	診断	●チェックを入れると「ランサムウェアの防止: コントロールされたフォルダーアクセス」の診断を行います。 ●チェックを外すと何も行いません。

※1: 本機能の設定は「ウィルスと脅威の防止: リアルタイム保護」の設定がチェックされているときのみチェックできます。

◆Office 項目

Office の仕様により「信頼済みドキュメント」と判断されたドキュメントは、マクロの実行が有効になります。
信頼済みドキュメントについては、以下を参照してください。

https://support.microsoft.com/ja-jp/office/%E4%BF%A1%E9%A0%BC%E6%B8%88%E3%81%BF%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88-cf872bd8-47ec-4c02-baa5-1fdba1a11b53

項目	説明
コンピューターに影響を与える可能性のあるマクロの実行を制限する：Excel	●チェックを入れるとコンピューターに影響を与える可能性のある Excel 内のマクロの実行を制限します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
コンピューターに影響を与える可能性のあるマクロの実行を制限する：Word	●チェックを入れるとコンピューターに影響を与える可能性のある Word 内のマクロの実行を制限します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
コンピューターに影響を与える可能性のあるマクロの実行を制限する：PowerPoint	●チェックを入れるとコンピューターに影響を与える可能性のある PowerPoint 内のマクロの実行を制限します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
コンピューターに影響を与える可能性のあるマクロの実行を制限する：Outlook	●チェックを入れるとコンピューターに影響を与える可能性のある Outlook 内のマクロの実行を制限します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。

◆ブラウザー項目

本機能はサポートされていません。

項目	説明
SSL3.0 以下を無効、TLS1.0 以上を有効にする	●チェックを入れると SSL3.0 以下の SSL を停止し、TLS1.0 以上が有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
拡張保護モードを有効にする	●チェックを入れると拡張保護モードが有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
拡張保護モードで 64 ビットプロセッサを有効にする	●チェックを入れると拡張保護モードで 64 ビットプロセッサを有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。

項目	説明
SmartScreen フィルター機能を有効にする	●チェックを入れると SmartScreen フィルター機能が有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
POST の送信が POST を許可しないゾーンにリダイレクトされた場合に警告する	●チェックを入れると POST の送信が POST を許可しないゾーンにリダイレクトされた場合に警告します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
サーバーの証明書失効を確認する	●チェックを入れるとサーバーの証明書失効時に確認を行います。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
署名が有効な場合のみソフトウェアの実行またはインストールを許可する	●チェックを入れるとソフトウェアの実行またはインストールが許可されるのは署名が有効な場合のみになります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「署名が無効な場合でもソフトウェアの実行またはインストールを許可する」のチェックが外れます。
証明書のアドレスの不一致について警告する	●チェックを入れると証明書のアドレスの不一致について警告します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
発行元証明書の取り消しを確認する	●チェックを入れると発行元証明書の取り消しを確認します。 ●チェックを外すと設定セット適用前の状態に設定を復元します
厳密な P3P 検証を有効にする	●チェックを入れると厳密な P3P（Platform for Privacy Preferences 標準）検証が有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
他の混在したコンテンツを持つセキュリティで保護されていないイメージをブロックする	●チェックを入れると他の混在したコンテンツを持つセキュリティで保護されていないイメージがブロックされます。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
保護つき/保護なしのサイト間を移動する場合に警告する	●チェックを入れると保護つき／保護なしのサイト間を移動する場合に警告します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
安全だとマークされてない ActiveX コントロールの初期化とスクリプトの実行を無効にする	●チェックを入れると安全だとマークされてない ActiveX コントロールの初期化とスクリプトの実行を無効にします。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
署名された ActiveX コントロールのダウンロードをする場合にダイアログを表示する	●チェックを入れると署名された ActiveX コントロールのダウンロードをする場合にダイアログを表示します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
署名されていない ActiveX コントロールのダウンロードを無効にする	●チェックを入れると署名されていない ActiveX コントロールのダウンロードを無効にします。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
アクティブスクリプトを無効にする	●チェックを入れるとアクティブスクリプトを無効にします。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
IFRAME 内からプログラムやファイルを起動する前にダイアログを表示する	●チェックを入れると IFRAME 内からプログラムやファイルを起動する前にダイアログを表示します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。

項目	説明
Web ブラウザー コントロール内でスクリプトの実行を禁止する	●チェックを入れると Web ブラウザー コントロール内でスクリプトの実行を禁止します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
ポップアップブロック機能を有効にする	●チェックを入れるとポップアップブロック機能が有効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
既存のクライアント証明書が 1 つしか存在しない場合の証明書の選択を無効にする	●チェックを入れると既存のクライアント証明書が 1 つしか存在しない場合のクライアント証明書の選択が無効になります。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
SSL/TLS で暗号化された部分とされていない部分が混在するときにダイアログを表示する	●チェックを入れると SSL／TLS で暗号化された部分とされていない部分が混在するときにダイアログを表示します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
イントラネットゾーンでのみユーザー認証が必要なページに自動的にログオンする	●チェックを入れるとユーザー認証が必要なページに自動的にログオンするのはイントラネットゾーンに限られます。 ●チェックを外すと設定セット適用前の状態に設定を復元します。 「インターネット」ゾーンに対する設定を行います。
プライバシーが「中」未満の場合に「中」に設定する	●チェックを入れるとプライバシー設定が「中」未満の場合に設定を「中」に設定します。 ●チェックを外すと設定セット適用前の状態に設定を復元します。
ローカルイントラネットゾーンを既定のレベルに設定する	●チェックを入れるとローカルイントラネットゾーンが既定のレベルになります。 ●チェックを外すと何も行いません。 既定以上のセキュリティレベルの場合は変更されません。
信頼済みサイトゾーンを既定のレベルに設定する	●チェックを入れると信頼済みサイトゾーンが既定のレベルになります。 ●チェックを外すと何も行いません。 既定以上のセキュリティレベルの場合は変更されません。
制限付きサイトゾーンを既定のレベルに設定する	●チェックを入れると制限付きサイトゾーンが既定のレベルになります。 ●チェックを外すと何も行いません。 既定以上のセキュリティレベルの場合は変更されません。

9.3.5 SIM 抜き差し監視

SIM 抜き差し監視は、正規の SIM（本機能を有効にした状態で同期したときに最初に検知される SIM）が抜かれた場合や、正規の SIM 以外の SIM が挿入された場合に、ロック画面を表示して、Windows 端末を操作できない状態にします。

本画面では、正規の SIM が挿入された状態でのみ、Windows 端末を使用できる設定セットを作成します。

- 本機能では、非正規の SIM は使用できません。
- 本機能は、SIM が使用できる Windows 端末が対象です。
- Windows 端末の「WWAN AutoConfig」サービスが起動していることを確認してください。
- 本機能では、外部 SIM（USB 接続の SIM などの外付けで接続している SIM）の抜き取り検知ができないため、外部 SIM の使用は推奨できません。
- eSIM と外部 SIM が存在する Windows 端末では、端末上で外部 SIM の使用を選択している場合、正規の SIM として外部 SIM が登録されます。しかし、外部 SIM を抜いたタイミングで端末が eSIM の使用へと自動的に切り替えるため、eSIM を非正規 SIM として認識し、ロック画面が表示される場合があります。ロック画面が表示された場合はロック画面を解除し、SIM の再登録を行ってください。
  ☞「（設定－Windows）設定セットの割り当て」103 ページ
  ☞「（操作－Windows）ロック解除」131 ページ
- 正規の SIM として登録するために、SIM ごとに固有の認識番号として「ICCID」を使用しています。SIM 紛失時などに再発行を行うと ICCID が変更されるため、正規の SIM として検出されなくなるため、あらためて再登録を行ってください。
- 作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。
  ☞「（設定－Windows）設定セットの割り当て」103 ページ
  ☞「全機器一括設定」200 ページ
- 設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［セキュリティ］→［SIM 抜き差し監視］→ ✚

項番	項目	説明
1	設定名	設定テンプレートの名称を 1 文字から 30 文字で入力します。 設定は最大 50 個まで作成できます。
2	SIM 登録	SIM 抜き差し監視を行うか、以下の選択肢から選択します。 ●有効 SIM 抜き差し監視の対象とする場合は、「有効」を選択します。 ●無効 SIM 抜き差し監視の対象としない場合は、「無効」を選択します。 「有効」から「無効」に切り替え、同期を行うと登録されている正規の SIM は解除されます。
3	ロックメッセージ	項番 2 の「SIM 登録」が「有効」の場合、ロック画面に表示するメッセージを入力できます。 ロックメッセージは 200 文字以内で入力してください。

◆ロック画面が表示される条件

Windows 端末で以下の操作が行われた場合は、端末にロック画面が表示します。

●正規の SIM を抜去した場合

●正規の SIM が抜去されている場合

●正規の SIM 以外の SIM を挿入した場合

●正規の SIM 以外の SIM が挿入されている場合

●SIM が挿入されていない場合

●SIM が認識されていない場合

◆別の SIM を正規の SIM として登録

登録されている正規の SIM を解除し、別の SIM を正規の SIM として登録する場合は、以下の操作を行います。

この操作を行うには、「SIM 抜き差し監視」で設定セットを作成し、「設定セットの割り当て」で［有効］を割り当ててください。

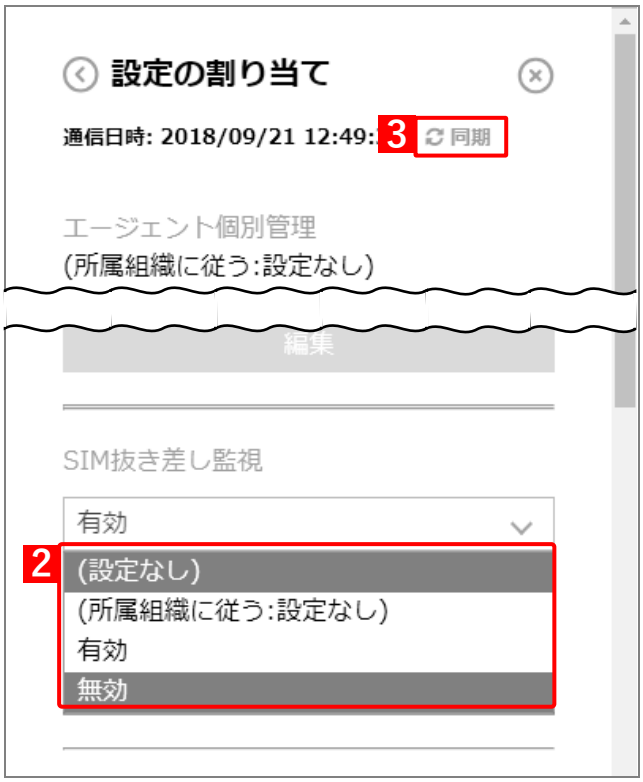
【1】機器一覧から該当の Windows 端末を選択して、機器の詳細画面を表示します。

「機器の詳細画面」59 ページ

【2】「設定セットの割り当て」の「SIM 抜き差し監視」を「有効」から「無効」または「(設定なし)」に変更します。

【3】同期 をクリックして同期を実行します。

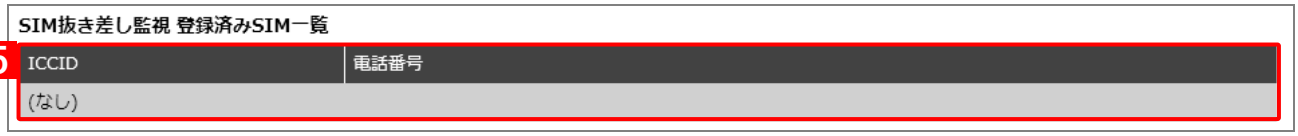
「(設定－Windows) 設定セットの割り当て」103 ページ



【4】該当の Windows 端末で自動同期が反映されるのを待つか、手動で同期を実行します。

【5】「セキュリティ」の「SIM 抜き差し監視 登録済み SIM 一覧」に登録がないことを確認します。

「(情報－Windows) セキュリティ」181 ページ

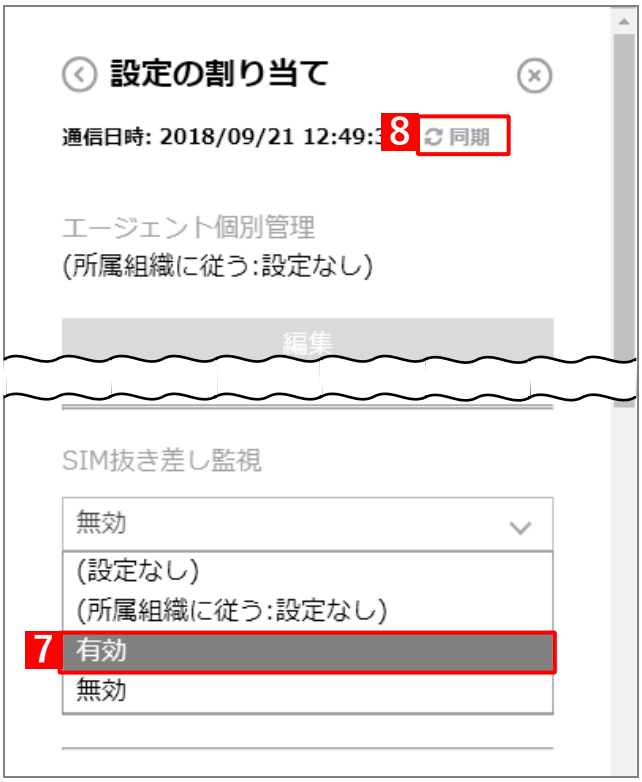


【6】該当の Windows 端末に新規に登録したい SIM を挿入します。

【7】「設定セットの割り当て」の「SIM 抜き差し監視」を「無効」または「(設定なし)」から「有効」に変更します。

【8】 同期 をクリックして同期を実行します。

「(設定－Windows) 設定セットの割り当て」103 ページ



【9】該当の Windows 端末で自動同期が反映されるのを待つか、手動で同期を実行します。

【10】「セキュリティ」の「SIM 抜き差し監視 登録済み SIM 一覧」に登録があることを確認します。

「(情報－Windows) セキュリティ」181 ページ

9.3.6 機能制限

外部デバイス、CD、DVD、ブルーレイおよびフロッピーディスク（FD）の使用を禁止することができます。

本機能では、外部デバイスや外部メディアの使用を制限する設定セットを作成することができます。

9.3.7 機能制限／外部デバイス

USB デバイス、SD デバイス、IEEE1394 デバイスの使用を禁止することができます。また、［禁止(ストレージへの書き込み)］以外の禁止項目を選択し、「ハードウェア ID」、「インスタンスパスまたはシリアル ID」を指定すると、特定デバイスを許可（ホワイトリストに登録）することができます。

本画面では、外部デバイスの使用を禁止するための設定セットを作成します。

外部デバイスの「ハードウェア ID」や「インスタンスパスまたはシリアル ID」は、以下のように使い分けてください。

●ハードウェア ID
同種または同系統の機器すべてを許可したい場合に指定します。

●インスタンスパスまたはシリアル ID
特定の機器 1 台のみを許可したい場合に指定します。

スマートフォンなど一部のデバイスでは、ストレージやポータブルデバイス以外の接続機能、アプリを使用したファイル転送などの機能を提供しています。このようなデバイスの場合、［禁止(ストレージおよびポータブルデバイス)］を選択しても USB 機器との接続を禁止できないため、「USB デバイス」で［禁止］を選択して USB 接続を禁止し、該当するアプリを個別に起動禁止にしてください。

USB デバイスの禁止設定を解除またはホワイトリストに登録した場合、USB デバイスを挿入し直してください。

禁止設定を解除後に USB デバイスを認識しない場合は、USB デバイスのドライバーを再インストールしてください。

USB、SD、IEEE1394 デバイスの使用を禁止した場合、お使いの機器によってはキーボード、マウスなどによる入力ができなくなることがあります。必要に応じてホワイトリスト（「許可デバイス（ハードウェア ID)」「許可デバイス（インスタンスパスまたはシリアル ID)」）に入力機器を登録してください。端末により禁止できないものがあります。

同一の外部デバイスを複数の Windows 端末で許可したい場合、取得できるインスタンスパスまたはシリアル ID の値は、Windows 端末ごとに異なります。Windows 端末ごとに取得したインスタンスパスまたはシリアル ID を管理サイトに登録してください。

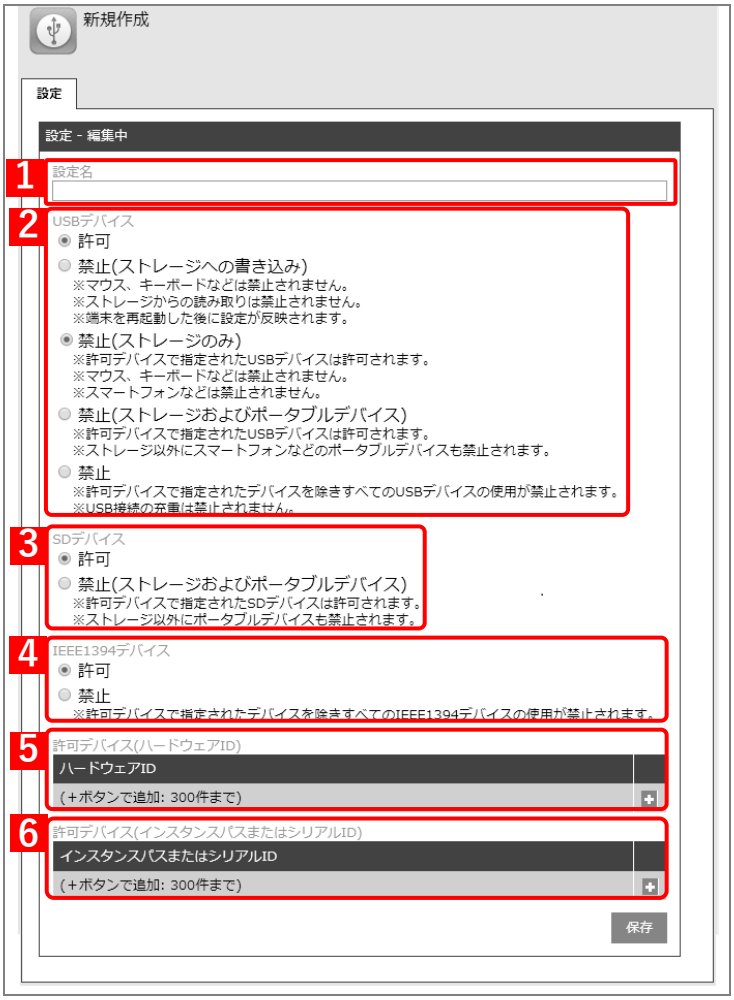
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「(設定－Windows）設定セットの割り当て」103 ページ
「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［セキュリティ］→［機能制限］→［外部デバイス］→ ＋（一覧から対象を選択→［編集］）



項番	項目		説明
1	設定名		設定の名称を 1 文字から 30 文字以内で入力します。
2	USB デバイス		USB デバイスについて制限を選択します。
		許可（※1）	USB デバイスの利用を許可します。
		禁止(ストレージへの書き込み)（※1）	USB デバイスへの書き込みを禁止します。 マウス、キーボードなどは禁止されません。 ストレージからの読み取りは禁止されません。 端末を再起動した後に設定が反映されます。
		禁止(ストレージのみ)（※1）	USB デバイスの使用を禁止します。 許可デバイスで指定された USB デバイスは許可されます。 マウス、キーボードなどは禁止されません。 スマートフォンなどは禁止されません。 禁止できる外部デバイスは以下を参照してください。 「禁止できる外部デバイスのパターン一覧」－「USB デバイス（「禁止（ストレージのみ）」の場合）」598 ページ

項番	項目		説明
		禁止(ストレージおよびポータブルデバイス)（※1）	USB デバイスに加えて、ポータブルデバイス（※2）を禁止します。ポータブル デバイス（※2）として PC に認識されている USB 機器の使用を禁止できます。 許可デバイスで指定された USB デバイスは許可されます。 ストレージ以外にスマートフォンなどのポータブルデバイスも禁止されます。 禁止できる外部デバイスは以下を参照してください。 「禁止できる外部デバイスのパターン一覧」－「USB デバイス（「禁止（ストレージおよびポータブルデバイス）」の場合）」598 ページ
		禁止（※1）	すべての USB デバイスが利用できなくなります。 許可デバイスで指定されたデバイスを除きすべての USB デバイスの使用が禁止されます。 USB 接続の充電は禁止されません。
3	SD デバイス		SD デバイスについて制限を選択します。
		許可	SD デバイスの利用を許可します。
		禁止(ストレージおよびポータブルデバイス)	SD デバイスの使用を禁止します。ただし、SD として認識されるマウスやキーボードなどへの接続は禁止されません。 許可デバイスで指定された SD デバイスは許可されます。 ストレージ以外にポータブルデバイスも禁止されます。 禁止できる外部デバイスは以下を参照してください。 「禁止できる外部デバイスのパターン一覧」－「SD デバイス」598 ページ
4	IEEE1394 デバイス		IEEE1394 デバイスについて制限を選択します。
		許可	IEEE1394 デバイスの利用を許可します。
		禁止	許可デバイスで指定されたデバイスを除きすべての IEEE1394 デバイスの使用が禁止されます。 許可デバイスで指定されたデバイスを除きすべての IEEE1394 デバイスの使用が禁止されます。 禁止できる外部デバイスは以下を参照してください。 「禁止できる外部デバイスのパターン一覧」－「IEEE1394 デバイス」598 ページ
5	許可デバイス(ハードウェア ID)		をクリックして、許可する外部デバイスのハードウェア ID を半角英数字と記号で登録します。最大 300 件登録できます。 「許可デバイスを調べる」593 ページ 表示されたハードウェア ID の値の変更はできません。
6	許可デバイス(インスタンスパスまたはシリアル ID)		をクリックして、許可する外部デバイスの「インスタンスパス」または「シリアル ID」を半角英数字と記号で登録します。最大 300 件登録できます。 「許可デバイスを調べる」593 ページ 表示されているインスタンスパスまたはシリアル ID の値の変更はできません。

※1：詳細については、「選択肢の詳細」を参照してください。

※2：ポータブルデバイスは携帯電話、スマートフォン、デジタルカメラ、ポータブルメディアプレイヤーなどの多くの携帯機器で利用される接続機器です。

◆選択肢の詳細

項目	ストレージ		ポータブルデバイス(※1)	マウス・キーボードの操作	USB 充電
	読込	書込			
許可	○	○	○	○	○
禁止(ストレージへの書き込み)	○	×	○	○	○
禁止(ストレージのみ)	×	×	○	○	○
禁止(ストレージおよびポータブルデバイス)	×	×	×	○	○
禁止	×	×	×	×	○

○：デバイスを使用できる（禁止されない）
×：デバイスを使用できない（禁止される）
※1：ポータブルデバイスは携帯電話、スマートフォン、デジタルカメラ、ポータブルメディアプレイヤーなどの多くの携帯機器で利用される接続機器です。

◆許可デバイスを調べる

許可デバイスを調べるためにプロパティ画面を表示します。

プロパティ画面を表示後は、以下の確認を行ってください。

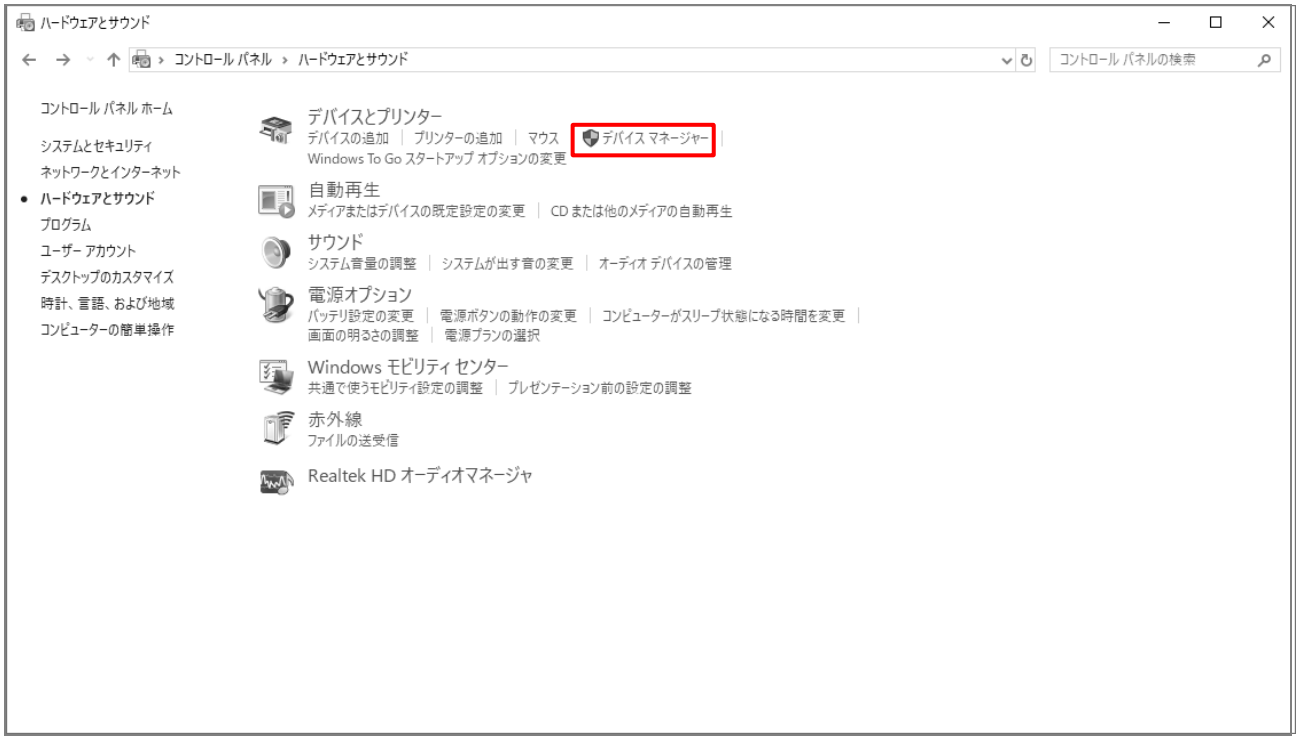
☞「ハードウェア ID を確認する」595 ページ
☞「インスタンスパスまたはシリアル ID を確認する」596 ページ
☞「禁止できる外部デバイスか確認する」597 ページ
☞「禁止できる外部デバイスのパターン一覧」598 ページ
☞「取り外し可能なデバイスの確認方法」599 ページ

Windows 10 での操作を例に説明します。詳細については、OS の開発元へ問い合わせてください。

手順【1】から【4】までは、同じ手順です。

【1】⊞ →「Windows システムツール」→［コントロールパネル］をクリックします。

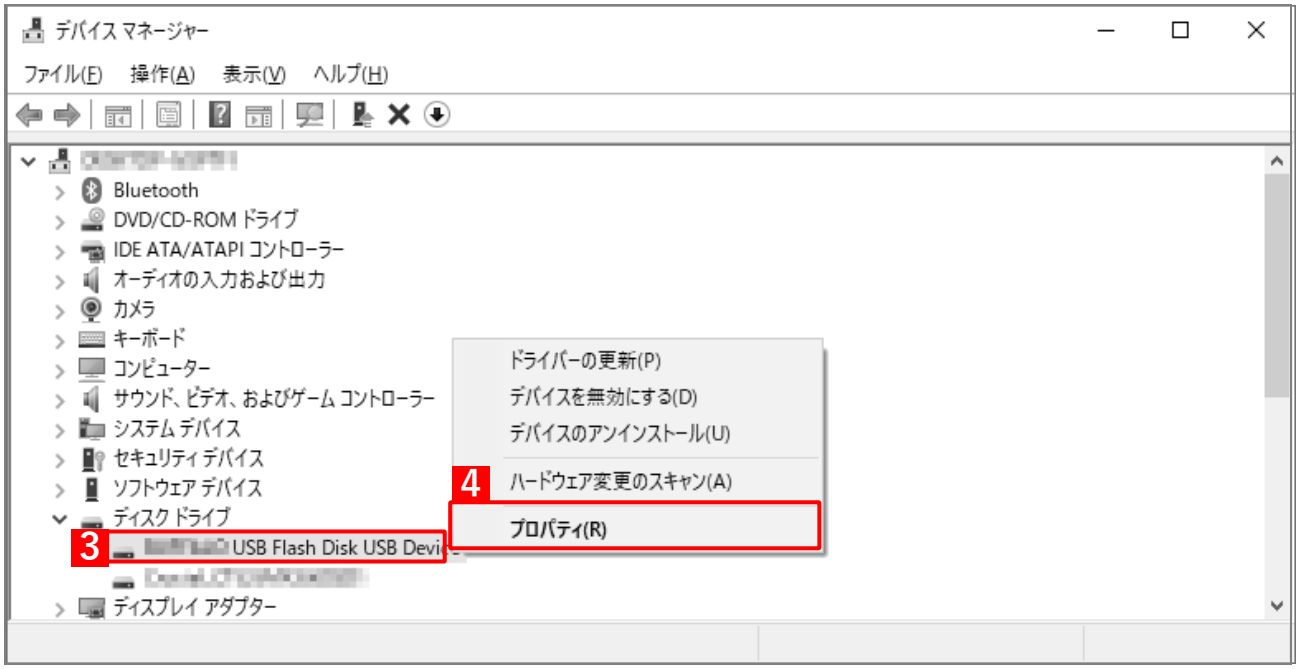
【2】「ハードウェアとサウンド」→「デバイス マネージャー」をクリックします。



【3】デバイス一覧から該当機器を選択します。

【4】選択した機器の上で右クリック→［プロパティ(R)］をクリックします。

⇒デバイスのプロパティ画面が表示されます。



◆ハードウェア ID を確認する

【1】「許可デバイスを調べる」の操作で表示されるプロパティ画面で、［詳細］タブをクリックします。

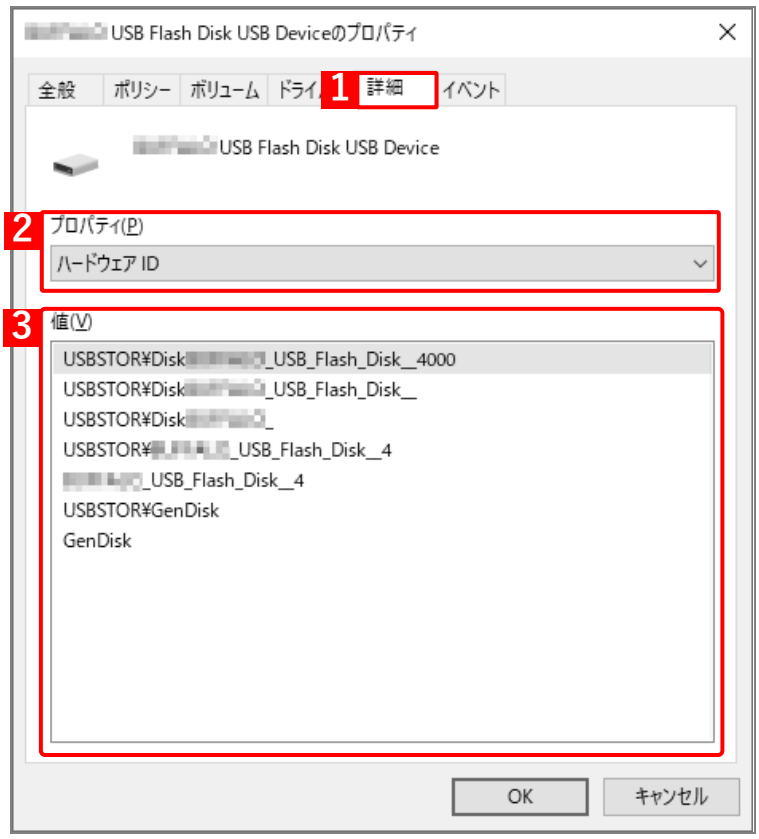
【2】「プロパティ」のリストメニューから「ハードウェア ID」を選択します。

⇒「値」にハードウェア ID の一覧が表示されます。

【3】「値」に表示されたハードウェア ID を 1 つ設定します。

⇒ハードウェア ID が有効に機能します。

ハードウェア ID は、設定したすべてのデバイスで有効になります。



◆インスタンスパスまたはシリアル ID を確認する

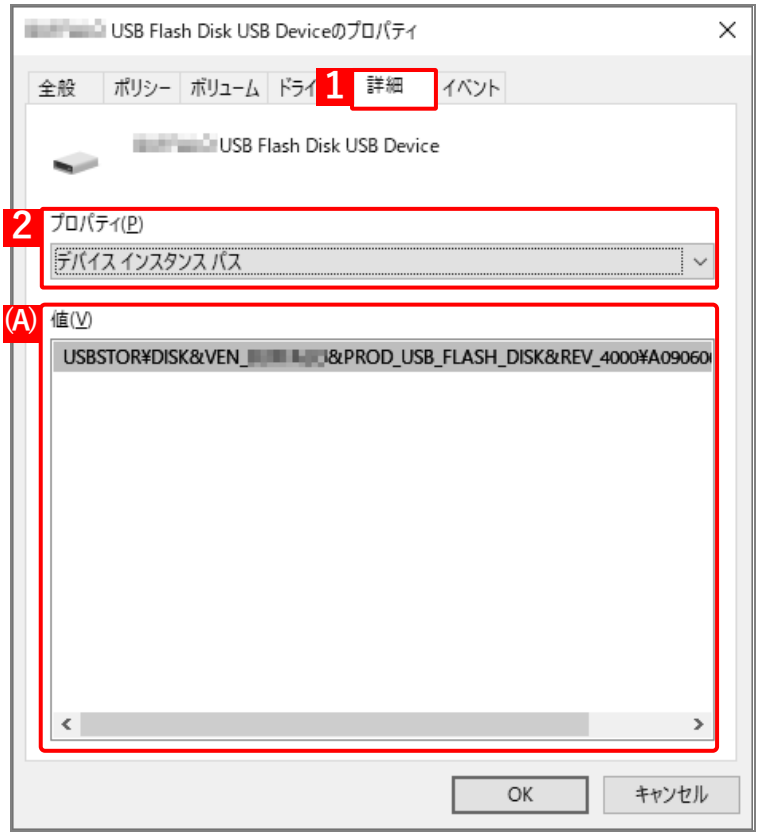
【1】「許可デバイスを調べる」の操作で表示されるプロパティ画面で、［詳細］タブをクリックします。

【2】「プロパティ」のリストメニューから［デバイス インスタンス パス］を選択します。

⇒（A）「値」にインスタンスパスが表示されます。

インスタンス パスからシリアル ID を確認します。インスタンスパスは 2 つの`¥`により 3 分割されますが、本製品では最後の部位の識別子をシリアル ID と呼称しています。

例として、デバイスインスタンスパスが「USB¥VID_099C&PID_9998&MI_00¥7&9999C191&0&0000」の場合、「7&9999C191&0&0000」がシリアル ID となります。



◆禁止できる外部デバイスか確認する

列挙子、サービス、クラス GUID の値を確認します。外部デバイスの列挙子、サービス、クラス GUID の組み合わせが特定のパターンに該当する場合のみ、［禁止］の設定が有効になります。

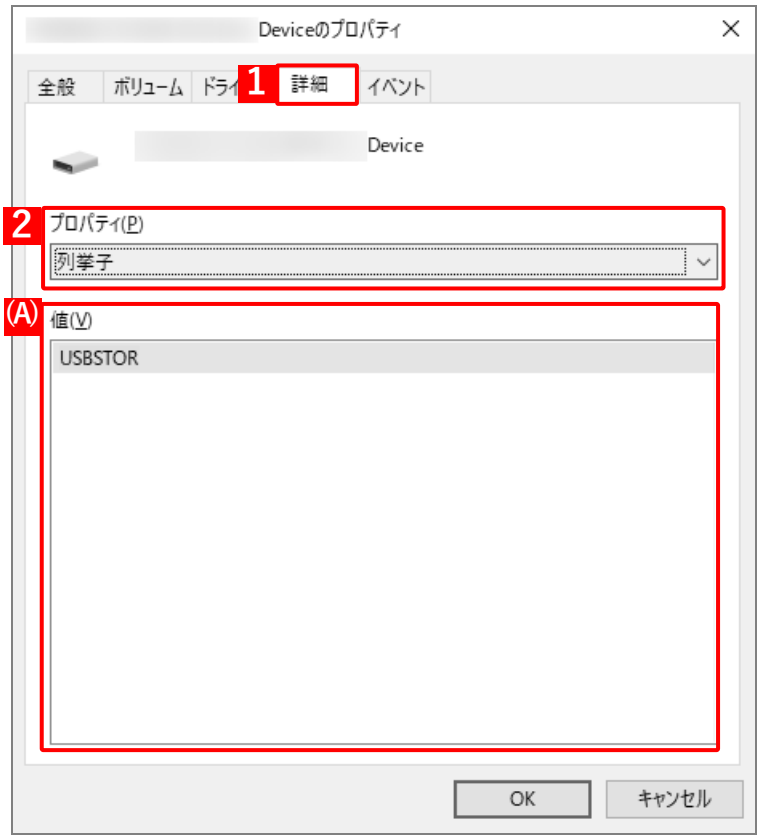
パターンの詳細については、以下を参照してください。

「禁止できる外部デバイスのパターン一覧」598 ページ

【1】「許可デバイスを調べる」の操作で表示される外部デバイスのプロパティ画面で、［詳細］タブをクリックします。

【2】「プロパティ」のリストメニューから［列挙子］、「サービス」または「クラス GUID」を選択します。

⇒（A）選択したプロパティの値が表示されます。



◆禁止できる外部デバイスのパターン一覧

以下のパターン一覧にない値は、本製品では非対応です。

取り外し可能なデバイスのみ対応しています。取り外し可能なデバイスの確認方法は、以下を参照してください。

「取り外し可能なデバイスの確認方法」599 ページ

特定のデバイスを許可している（ホワイトリスト）場合は、禁止されません。以下を参照してください。

「機能制限／外部デバイス」590 ページ

確認方法は、以下を参照してください。

「禁止できる外部デバイスか確認する」597 ページ

「－」は、すべての値が許容します。

●USB デバイス（「禁止（ストレージのみ）」の場合）

パターン	列挙子	サービス	クラス GUID
1	USB	USBSTOR	—
2	USB	—	{4d36e967-e325-11ce-bfc1-08002be10318}
3	USBSTOR	USBSTOR	—
4	USBSTOR	—	{4d36e967-e325-11ce-bfc1-08002be10318}

●USB デバイス（「禁止（ストレージおよびポータブルデバイス）」の場合）

パターン	列挙子	サービス	クラス GUID
1	USB	USBSTOR	—
2	USB	—	{4d36e967-e325-11ce-bfc1-08002be10318}
3	USB	—	{eec5ad98-8080-425f-922a-dabf3de3f69a}
4	USBSTOR	USBSTOR	—
5	USBSTOR	—	{4d36e967-e325-11ce-bfc1-08002be10318}
6	USBSTOR	—	{eec5ad98-8080-425f-922a-dabf3de3f69a}

●SD デバイス

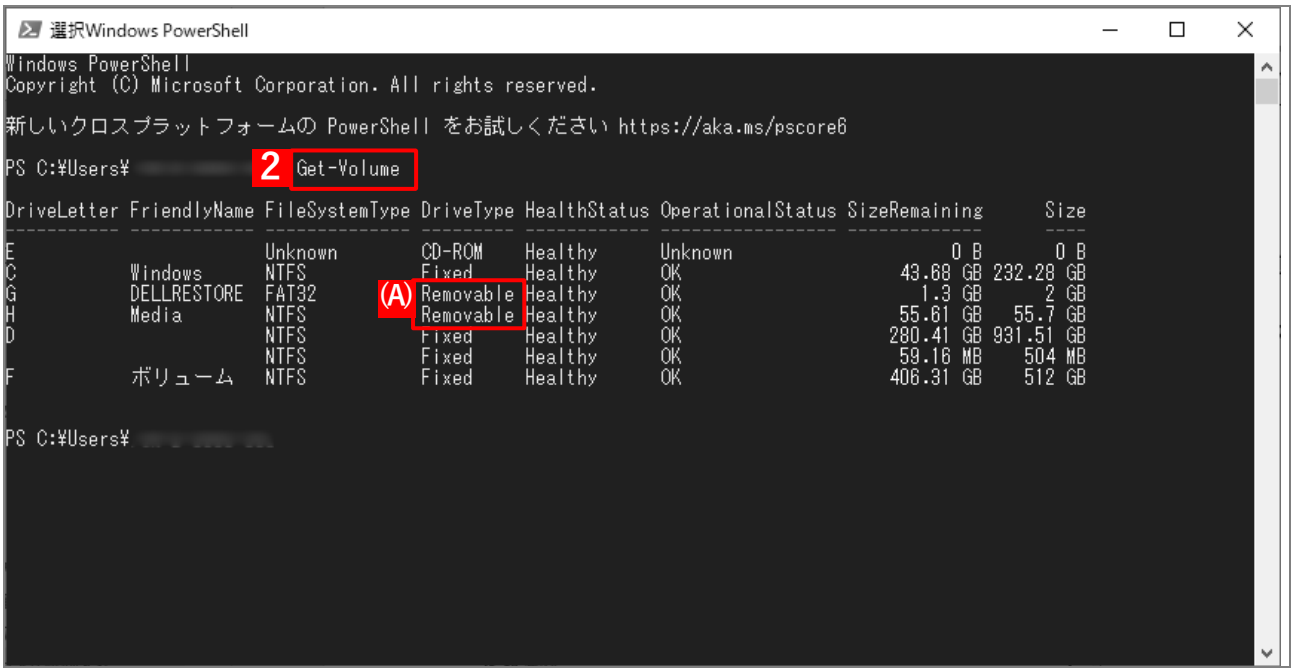
パターン	列挙子	サービス	クラス GUID
1	SD	SDSTOR	—
2	SD	—	{4d36e967-e325-11ce-bfc1-08002be10318}
3	SWD	SDSTOR	—
4	SWD	—	{eec5ad98-8080-425f-922a-dabf3de3f69a}
5	USBSTOR	USBSTOR¥SD	—

●IEEE1394 デバイス

パターン	列挙子	サービス	クラス GUID
1	IEEE1394	—	—
2	SBP2	—	—

◆取り外し可能なデバイスの確認方法

【1】スタートメニューから、Powershell を起動します。
【2】コマンド「Get-Volume」を実行します。
【3】DriveType が（A）Removable になっているデバイスが取り外し可能です



9.3.8 機能制限／CD/DVD/ブルーレイ

CD、DVD、ブルーレイおよびフロッピーディスク（FD）の使用を禁止するための設定セットを作成します。

利用を禁止した場合、アプリから CD、DVD、ブルーレイおよびフロッピーディスクが利用できなくなります。

アプリによっては、アプリが起動できなくなる場合もあります。

設定セットが機器に適用されたあとに、端末を再起動すると設定が反映されます。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［**設定**］→［**Windows**］→［**セキュリティ**］→［**機能制限**］→［**CD/DVD/ブルーレイ**］→ ＋（**一覧から対象を選択**→［**編集**］）

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	CD/DVD/ブルーレイ	CD、DVD、ブルーレイの使用について以下から選択します。 ●許可 ●書き込み禁止 ●禁止 本設定では、Windows 標準機能による読み書きが制御できます。サードパーティー製ライティングソフトによる書き込みも禁止する場合は、アプリケーション禁止で対象ソフトを指定してください。 「アプリケーション禁止」602 ページ
3	FD	フロッピーディスクの使用について以下から選択します。 ●許可 ●禁止

9.4 アプリケーション

Windows 端末のアプリに関連する設定、および設定セットを作成します。

本機能では、特定のアプリの使用禁止を行うことができます。

9.4.1 アプリケーション禁止

アプリの使用を禁止するための設定セットを作成します。

画面

画面（編集）

画面（許可するアプリケーションを指定する）

画面（禁止するアプリケーションを指定する）

本画面では、以下の禁止ルールを設定することができます。

●許可するアプリケーションを指定してルールを作成（ホワイトリスト形式）

・アプリのパス名を指定して、アプリの利用を許可する。

・アプリのパッケージ名を指定して、アプリの利用を許可する。

●禁止するアプリケーションを指定してルールを作成（ブラックリスト形式）

・実行ファイル名またはパッケージファミリー名を指定して、アプリの利用を禁止する。

・アプリのウインドウ名を指定して、アプリの利用を禁止する。

禁止対象のアプリは起動できません。

本設定で外部デバイス、CD、DVD、ブルーレイ機能を含むアプリを禁止にしなくても、機能制限で、外部デバイス、CD、DVD、ブルーレイの使用が禁止されている場合は、CD、DVD、ブルーレイ機能を含むアプリの機能が制限されます。

「機能制限」590 ページ

ウインドウ名指定でアプリケーション禁止が動作しない場合は、実行ファイル名指定で設定してください。

本機能について重要な注意事項がありますので、ご利用のときは以下の内容を必ずご覧ください。

「ホワイトリスト形式の利用に関する重要な注意事項」607 ページ

本製品のエージェントアプリを禁止することはできません。

ホワイトリスト形式の対応 OS は、Windows 11 Enterprise/Education/Pro のみです。また、ブラックリスト形式の対応 OS は、以下を参照してください。

『Windows クライアント リファレンスマニュアル』の「Windows クライアントについて」－「エージェントの動作環境」

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

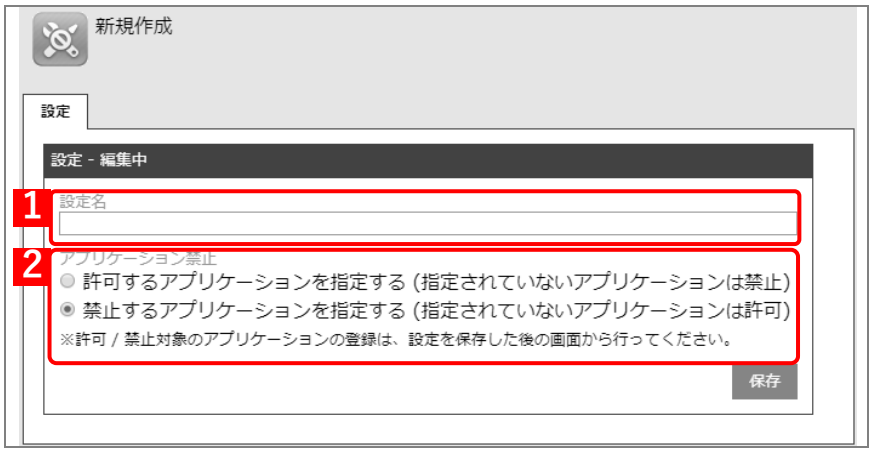
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［アプリケーション］→［アプリケーション禁止］→ ✚



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	アプリケーション禁止	アプリの禁止種別を以下から選択します。 ●許可するアプリケーションを指定する(指定されていないアプリケーションは禁止) ●禁止するアプリケーションを指定する(指定されていないアプリケーションは許可) 1 度選択したアプリの禁止種別は変更できません。複製のときにも変更できません。

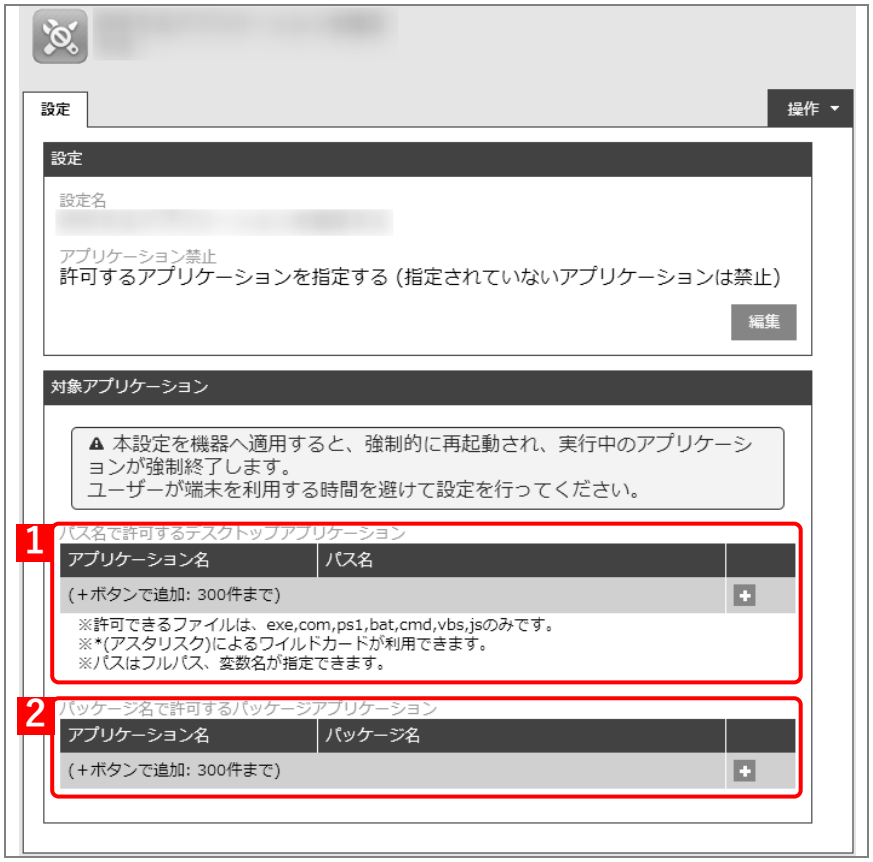
◆画面（編集）

表示操作［設定］→［Windows］→［アプリケーション］→［アプリケーション禁止］→**一覧から対象を選択**→［編集］

項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	アプリケーション禁止	1 度選択したアプリの禁止種別は変更できません。また、複製のときにも変更できません。変更したい場合は、新規に作成してください。 ●許可するアプリケーションを指定する（指定されていないアプリケーションは禁止） ●禁止するアプリケーションを指定する（指定されていないアプリケーションは許可）

◆画面（許可するアプリケーションを指定する）

表示操作　［設定］→［Windows］→［アプリケーション］→［アプリケーション禁止］→一覧から対象（「許可するアプリケーションを指定する」の設定）を選択



項番	項目		説明
1	パス名で許可するデスクトップアプリケーション		パス名で許可するアプリを指定します。＋をクリックし、300 件まで登録できます。 動作するために必要なアプリをすべて「対象アプリケーション」として指定する必要があります。
		アプリケーション名	アプリ名を 60 文字以内で入力します。
		パス名	パス名を 260 文字以内で入力します。 パスはフルパス、変数名が指定できます。利用可能な変数名は以下を参照してください。 ☞「利用可能な変数名」605 ページ 指定できるファイルは exe、com、ps1、bat、cmd、vbs、js ファイルのみです。 「*」（アスタリスク）によるワイルドカードが利用できます。

項番	項目		説明
2	パッケージ名で許可するパッケージアプリケーション		パッケージ名で許可するアプリを指定します。＋ をクリックし、300 件まで登録できます。 動作するために必要なアプリをすべて「対象アプリケーション」として指定する必要があります。
		アプリケーション名	アプリ名を 60 文字以内で入力します。
		パッケージ名	パッケージ名を 3 文字から 50 文字以内で入力します。 半角英数字と「.」（ピリオド）、「-」（ハイフン）で入力してください。 パッケージ名については、以下を参照してください。 「パッケージファミリー名およびパッケージ名の探しかた」608 ページ

◆利用可能な変数名

項番	Windows のディレクトリーまたはドライブ	変数名
1	Windows フォルダー	%WINDIR%
2	System32 フォルダー	%SYSTEM32%
3	Windows インストールドライブ	%OSDRIVE%
4	Program Files フォルダー（x86 も含む）	%PROGRAMFILES%
5	リムーバブルメディア（例: CD、DVD）	%REMOVABLE%
6	リムーバブル記憶装置（例: USB フラッシュ ドライブ）	%HOT%

◆画面（禁止するアプリケーションを指定する）

表示操作　［設定］→［Windows］→［アプリケーション］→［アプリケーション禁止］→一覧から対象（「禁止するアプリケーションを指定する」の設定）を選択

項番	項目		説明
1	実行ファイル名またはパッケージファミリー名で禁止するアプリケーション		実行ファイル名で禁止対象となるアプリを指定します。 ＋ をクリックし、300 件まで登録できます。
		アプリケーション名	アプリ名を 60 文字以内で入力します。
		実行ファイル名またはパッケージファミリー名	実行ファイル名またはパッケージファミリー名を 255 文字以内で入力します。「¥」、「/」、「<」、「>」、「*」、「?」、「"」、「|」、「:」は入力できません。 指定できるファイルは exe ファイルのみです。拡張子は入力しないでください。 パッケージファミリー名については、以下を参照してください。 ☞「パッケージファミリー名およびパッケージ名の探しかた」608 ページ 禁止できるファイルは exe ファイルのみです。 実行ファイル名またはパッケージファミリー名には拡張子（.exe）を含めないでください。例えば、ペイント（実行ファイル名が mspaint.exe）を禁止する場合は、「mspaint」と入力します。
2	ウインドウ名で禁止するアプリケーション		ウインドウ名で禁止対象となるアプリを指定します。＋ をクリックし、300 件まで登録できます。
		アプリケーション名	アプリ名を 60 文字以内で入力します。
		ウィンドウ名	ウインドウ名を 255 文字以内で入力します。アプリを起動したときにタイトルバーに表示される文字列から指定してください。
		条件	指定するウインドウ名のマッチング条件を以下から選択します。 ●と一致する 指定したウインドウ名と完全に一致する場合に、禁止対象にします。 例えば、ウインドウ名に「abc.png － ペイント」を指定して、条件で「と一致する」を選択すると、名称が「abc.png － ペイント」のウインドウだけが禁止対象になります。 ●を含む 指定したウインドウ名が含まれているに、禁止対象にします。 例えば、ウインドウ名に「ペイント」を指定して、条件で「を含む」を選択すると、名称に「ペイント」が含まれるウインドウすべてが禁止対象になります。

◆ホワイトリスト形式の利用に関する重要な注意事項

「新規作成」画面の「アプリケーション禁止」で［許可するアプリケーションを指定する(指定されていないアプリケーションは禁止)］を選択し、ホワイトリスト形式を利用して設定を行う場合は、必ず以下の注意事項をお読みください。

●ホワイトリストへの設定を切り替えるとき、必ず再起動が必要です。

・設定なし→ホワイトリスト設定あり

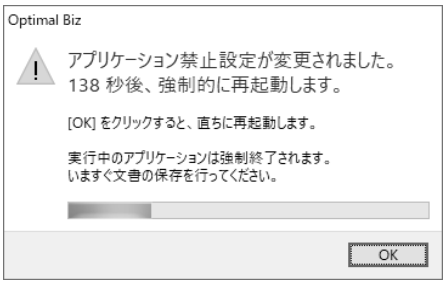
・ホワイトリスト設定あり（例：設定 A）→ホワイトリスト設定あり（例：設定 B）

・ホワイトリスト設定あり→設定なし

以下のケースでは、再起動は求められません

・ホワイトリスト設定あり（例：設定 A）→ホワイトリスト設定あり（例：設定 A）

設定切替のタイミングで以下の通知メッセージが表示され、3 分後に強制的に再起動が行われ、実行中のアプリは強制終了します。再起動はキャンセルできませんので、通知メッセージが表示されましたら必要な作業およびファイルについては必ず保存を行うように、事前に利用者へのご連絡をお願いいたします。



通知メッセージの表示中にアプリを強制終了させるなどして、意図的に再起動の回避を試みた場合は、即時強制的に再起動が行われることがあります。

●企業であれば就業時間中に、学校であれば授業時間中に、再起動の設定内容の変更、割り当てる設定セットの変更（Zone Management による自動切替含む）を行いますと、強制的に再起動されます。

就業時間外や授業時間外に設定変更や同期を行ってください。

●端末が最低限動作するために必要な Windows システムアプリ（Microsoft の証明書が付与されたアプリ）や、本製品が動作するために必要な本製品のエージェントなどは、管理者がホワイトリストに設定せずとも、許可されている状態になっています。それ以外のウイルス対策ソフト（Windows Defender 含む）など必要なアプリは、管理者が設定してください。

●ホワイトリスト形式のアプリケーション禁止のご利用時は、テスト機 1 台にまずは設定を割り当て、端末利用者の運用に沿った動作確認を行い問題ないことを確認してから、対象端末全台への割り当てを行ってください。

●ホワイトリスト形式のアプリケーション禁止では、Windows OS に搭載されている App Locker 機能を使用しています。ホワイトリスト形式の設定を端末に適用した時点で、管理者が本製品を使用しないで設定した AppLocker 設定は、削除されます。元に戻すことはできません。

●管理サイトの「アプリケーション禁止ログ」の表示では設定が正しく行われたことになっていても、ドメイン側で異なるアプリケーション禁止設定が反映されている場合は、以下の問題が発生する可能性があります。

・利用を許可しているアプリが利用できない。

上記の問題が発生した場合は、ドメイン側の設定を確認してください。

パッケージファミリー名およびパッケージ名の探しかた

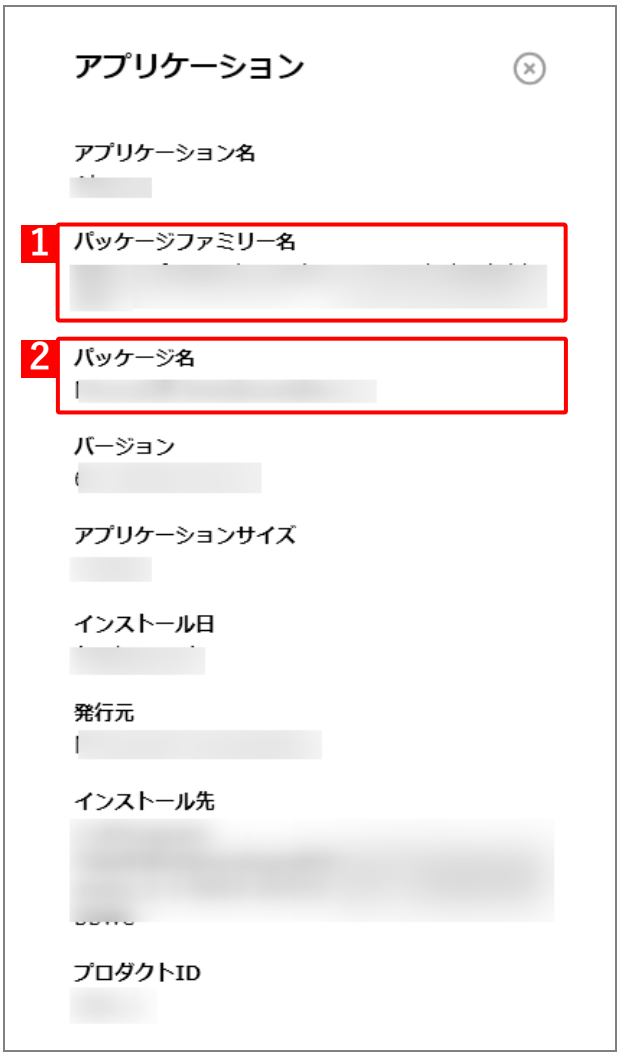
パッケージファミリー名、およびパッケージ名は、Windows 端末にすでに登録されているアプリ一覧で確認できます。

端末の詳細画面のアプリ一覧の詳細については、以下を参照してください。

「（情報－Windows）アプリケーション」178 ページ

◆画面

表示操作　**［機器］→［一覧］→Windows 端末の「詳細」の ＞ →詳細画面の「情報」の［アプリケーション］→一覧から対象のアプリケーションの ＞**



項番	項目	説明
1	パッケージファミリー名	設定に必要となるパッケージファミリー名が表示されています。
2	パッケージ名	設定に必要となるパッケージ名が表示されています。

9.5 インターネット

インターネットに関連する設定を行います。

Wi-Fi の設定、Wi-Fi フィルタリング、プロキシ設定、端末のブラウザーへのお気に入り追加を設定することができます。

9.5.1 Wi-Fi

Wi-Fi の接続先ネットワークの設定を、管理サイトから制御するための設定セットを作成します。

端末を機内モードに設定していると、本機能は端末に反映されません。

本製品を解約しても端末に反映した設定は保持されます。事前に各種設定セットに［(設定なし)］を適用し、同期を行ってから本製品を解約してください。

誤ってプロファイルを削除してしまった場合は、以下のいずれかの対応を行ってください。Wi-Fi の設定があらためて配信されます。

- 本製品のエージェントを停止し、再度起動してから同期する
- OS の再起動を行ったあとに同期する
- 管理サイトから前回と異なる設定セット、または［設定なし］を適用し同期し、あらためて元の設定セットを適用して同期する

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「(設定－Windows) 設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　**［設定］→［Windows］→［インターネット］→［Wi-Fi］→ ＋ （一覧から対象を選択→［編集］）**

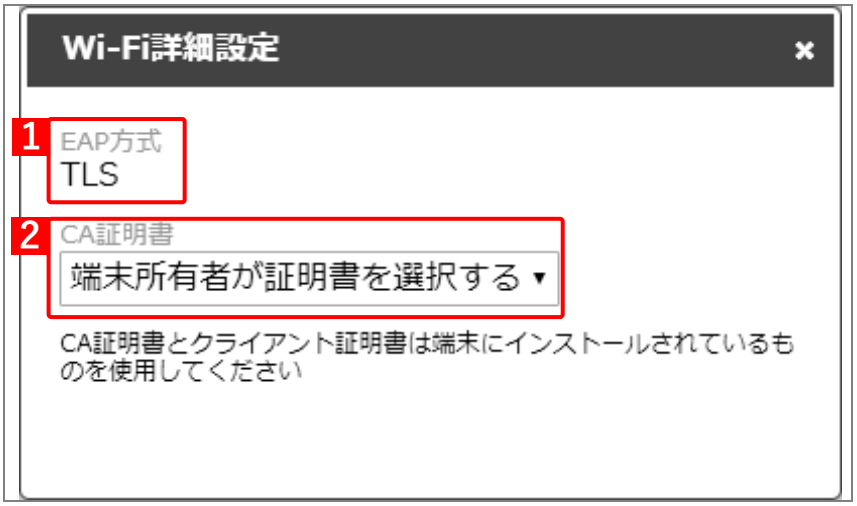
項番	項目		説明
1	設定名		設定の名称を 1 文字から 30 文字以内で入力します。
2	ネットワーク一覧		端末へ設定する Wi-Fi 情報の設定を行います。1 つの設定セットにつき、5 件まで登録できます。
		SSID	端末へ配布する Wi-Fi 設定の SSID の名称を 32 文字以内の半角英数記号で入力します。
		セキュリティ	端末へ配布する Wi-Fi 設定のセキュリティ方式を以下から選択します。 ●なし ●WPA/WPA2-PSK ●802.1x EAP
		パスワード / 詳細設定	端末へ配布する Wi-Fi 設定のセキュリティパスワードを登録します。セキュリティの設定によって入力文字数が変わります。 ●「なし」の場合 パスワードは設定しません。 ●「WPA/WPA2-PSK」の場合 文字の種類によって、以下のように入力文字数が異なります。 ・ASCII 文字のときは、8 文字以上 63 文字以下で入力します。 ・16 進数のときは、64 文字で入力します。 ●「802.1x EAP」の場合 ［Wi-Fi 詳細設定］をクリックして、Wi-Fi 詳細設定画面で詳細を設定します。 ☞「Wi-Fi 詳細設定（セキュリティが「802.1x EAP」の場合)」611 ページ
		Hidden	Hidden SSID の場合に、チェックを入れます。

Wi-Fi 詳細設定（セキュリティが「802.1x EAP」の場合）

「ネットワーク一覧」の「セキュリティ」で［802.1x EAP］を選択した場合に、「パスワード／詳細設定」設定に表示される［Wi-Fi 詳細設定］をクリックすると表示されます。

EAP 方式での設定の場合は、アクセスポイント切り替えに伴う OS の挙動により、アクセスポイントの設定時に瞬断（端末により瞬断ではない時間）が発生します。

◆画面



項番	項目	説明
1	EAP 方式	「TLS」と表示されます。 変更はできません。
2	CA 証明書	ご自身で CA 証明書を端末にインストールする場合は、「端末所有者が証明書を選択する」を選択します。 本製品に事前に登録している CA 証明書を使用する場合は、プルダウンに表示されますので、該当の CA 証明書を選択します。CA 証明書のアップロードについては、以下を参照してください。 ☞「CA 証明書管理」623 ページ CA 証明書をあとから配信する場合は、同期に失敗して CA 証明書の配信ができない可能性があります。 CA 証明書だけでなくクライアント証明書も端末にインストールされている必要がございます。ご自身でインストールするか、もしくは本製品のクライアント証明書管理機能をご利用ください。 ☞「クライアント証明書管理」616 ページ

9.5.2 Wi-Fi フィルタリング

特定の無線 LAN アクセスポイントのみに端末の接続を許可する設定セットを作成します。他の SSID、または MAC アドレス以外への Wi-Fi 接続はできなくなります。

誤った設定を行うと Wi-Fi モデルでは一切ネットワークに接続できなくなりますのでご注意ください。

本製品を解約しても端末に反映した設定は保持されます。事前に各種設定セットに［(設定なし)］を適用し、同期を行ってから本製品を解約してください。

Windows 端末からエージェントの停止や削除した場合、本機能で制限していた Wi-Fi に接続したい場合は、端末で別途設定してください。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

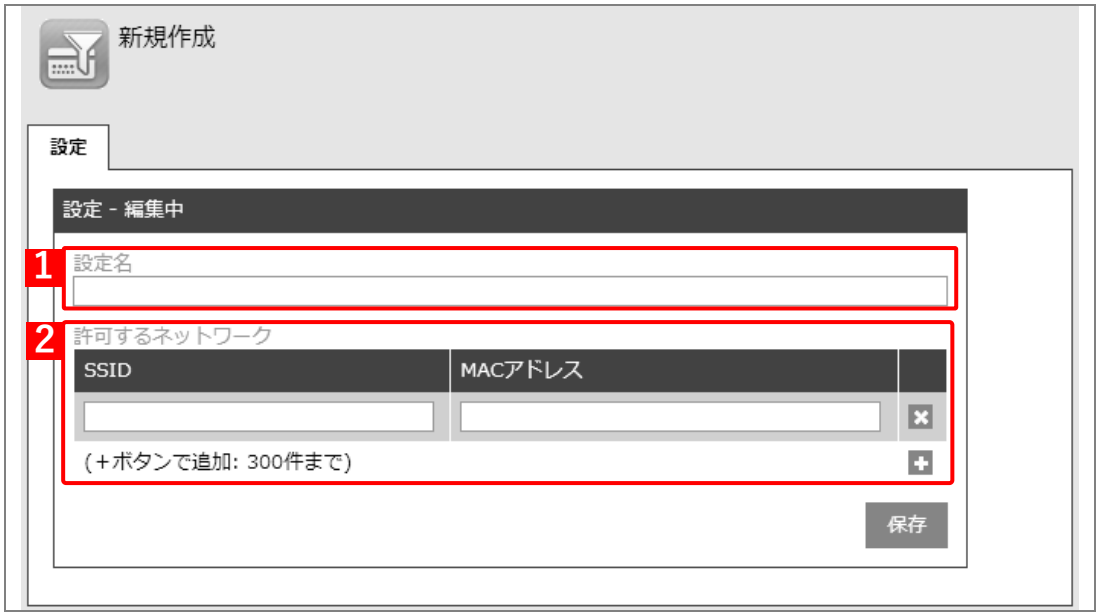
「(設定－Windows) 設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［設定］→［Windows］→［インターネット］→［Wi-Fi フィルタリング］→ ＋ （一覧から対象を選択→［編集］）



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	許可するネットワーク	端末に接続を許可するネットワークの情報を登録します。＋ をクリックして、最大 300 件まで登録できます。 ●SSID 端末で接続を許可する Wi-Fi の SSID を 32 文字以内の半角英数字、記号（「-」、「_」、「@」）で入力します。 ホワイトリストにない SSID は切断されます。切断した SSID は自動的に接続されないので、手動で接続してください。 ●MAC アドレス 必要に応じてアクセスポイントの MAC アドレスを入力します。「XX:XX:XX:XX:XX:XX」（X は大文字の 16 進数）という形式で入力してください。 MAC アドレスは、アクセスポイントの BSSID を意味します。 同一の SSID に複数の MAC アドレスを指定できます。

9.5.3 プロキシ

インターネット接続に利用するプロキシサーバーの設定を行うための設定セットを作成します。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

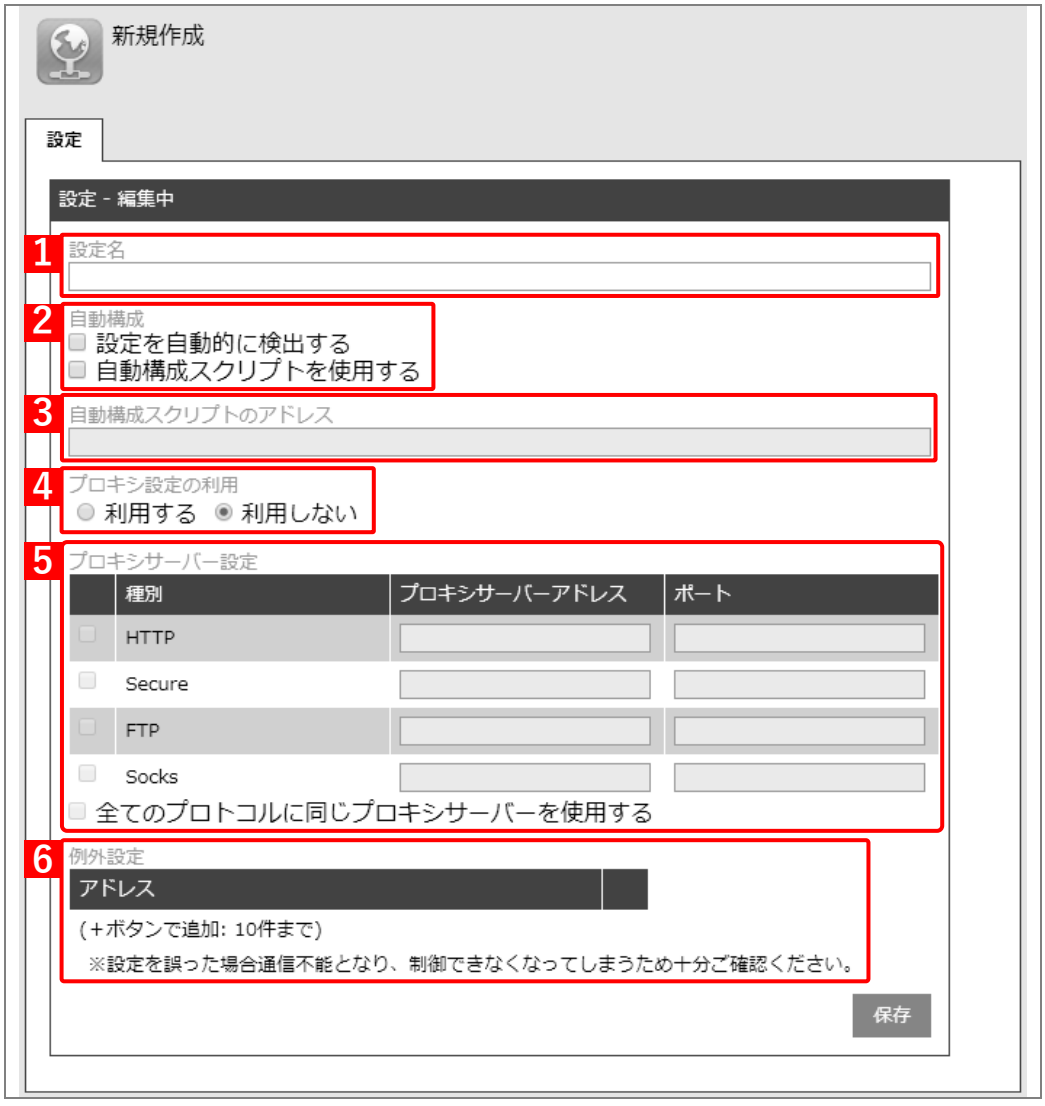
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Windows］→［インターネット］→［プロキシ］→ ✚ （一覧から対象を選択→［編集］）



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	自動構成	プロキシサーバーの自動構成を利用する場合に、利用方法に応じてチェックを入れます。 ●設定を自動的に検出する 利用するプロキシ設定を自動的に検出します。 ●自動構成スクリプトを利用する 自動構成スクリプトを利用してプロキシ設定を行います。
3	自動構成スクリプトのアドレス	「自動構成」で「自動構成スクリプトを利用する」にチェックを入れた場合は、自動構成ファイル（PAC ファイル）の URL を入力します。
4	プロキシ設定の利用	プロキシ設定の利用を以下から選択します。 ●利用する プロキシを利用し、接続先のプロキシサーバーを指定します。 選択すると、「プロキシサーバー設定」と「例外設定」が設定できます。 ●利用しない プロキシを利用しません。
5	プロキシサーバー設定	プロキシサーバーの以下の項目について設定します。 ●種別 プロトコル種別ごとにプロキシサーバーを指定します。 HTTP、Secure、FTP、Socks プロトコルでの指定ができます。各種別のチェックボックスにチェックを入れると「プロキシサーバーアドレス」と「ポート」が入力できるようになります。 ●プロキシサーバーアドレス プロキシサーバーのアドレスを 200 文字以内の半角英数字、記号で入力します。先頭には「http://」または「https://」を入力します。 誤ったプロキシ設定を行った場合は、インターネット接続や自動での Windows Update が接続不可となる可能性があります。 ●ポート 各プロトコルで利用するポート番号を 0 から 65,535 の半角数字で入力します。 ●全てのプロトコルに同じプロキシサーバーを使用する チェックを入れると、すべてのプロトコル種別に「HTTP」に指定した「プロキシサーバーアドレス」と「ポート」と同じ設定が適用されます。
6	例外設定	例外として許可するプロキシサーバーアドレスを指定します。 をクリックして、最大 10 件まで登録できます。

9.5.4 お気に入り

端末のブラウザーに、お気に入りの追加やホームページ設定を行うための設定セットを作成します。

本機能は、Internet Explorer 11 のみ有効です。

Windows 10、Windows 11 の Internet Explorer 11 は、サポートを終了しました。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

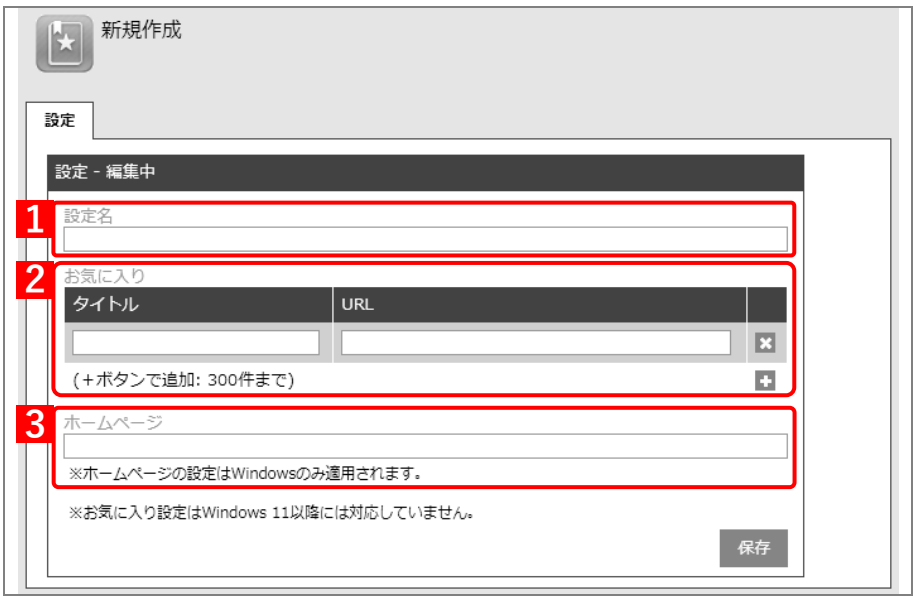
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Windows］→［インターネット］→［お気に入り］→ ＋ （一覧から対象を選択→［編集］）



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字以内で入力します。
2	お気に入り	お気に入りとして、以下の項目を入力します。＋ をクリックして、最大 300 件まで登録できます。 ●タイトル お気に入りのタイトル名を 100 文字以内の半角英数字と記号（「-」、「_」、「@」）で入力します。 ●URL URL 情報を 200 文字以内の半角英数字、記号で入力します。先頭には「http://」または「https://」を入力します。 「お気に入り」の設定は行わず、「ホームページ」の設定のみ行う設定セットを作成する場合は、お気に入りの入力欄は ✖ をクリックして削除したあとに、［保存］をクリックしてください。
3	ホームページ	ブラウザーのホームページに設定するサイトの URL を 200 文字以内の半角英数字、記号で入力します。先頭は「http://」または「https://」にしてください。 ホームページの設定は Windows 端末にだけ有効です。

9.6 証明書管理

クライアント証明書の管理や一括アップロード、一括削除のほか、CA 証明書の管理を行います。

9.6.1 クライアント証明書管理

クライアント証明書を管理サイトに 1 ファイルずつアップロードして保存し、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

画面（新規作成）

画面（管理）

画面（編集）

事前にクライアント証明書を取得してください。

本機能はクライアント証明書の配信までを行います。端末内に保存されるクライアント証明書の場所やインストール方法については、端末メーカーへ問い合わせてください。

アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。

「画面（編集）」619 ページ

クライアント証明書をまとめてアップロードする場合は、以下を参照してください。

「クライアント証明書一括アップロード」620 ページ

管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。

「（設定－Android）クライアント証明書」79 ページ

「（設定－iOS）クライアント証明書」86 ページ

「（設定－iOS）Exchange（ActiveSync）設定」89 ページ

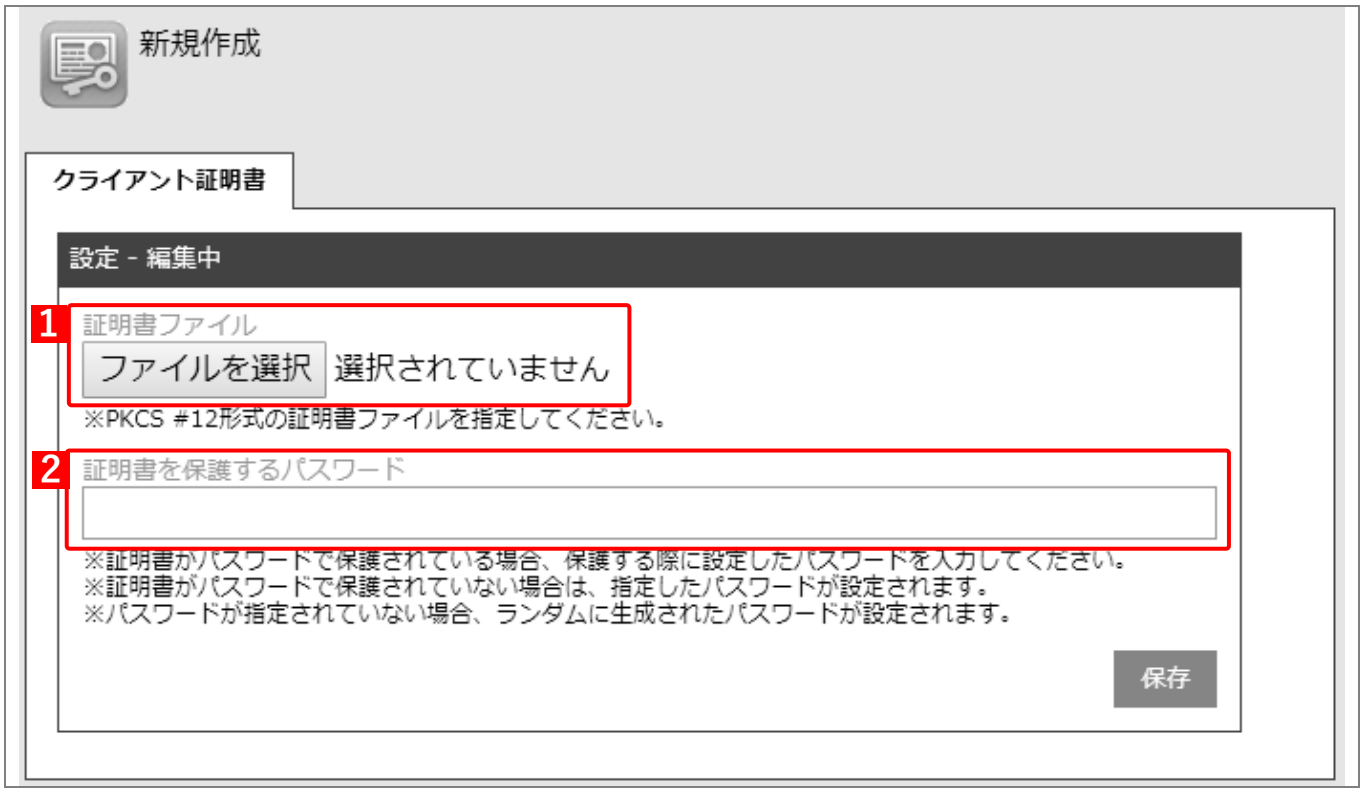
「（設定－iOS）VPN 設定」94 ページ

「（設定－Windows）クライアント証明書」106 ページ

設定セットは、最大で 500,000 件まで作成できます。

◆画面（新規作成）

表示操作　［設定］→［Windows］→［証明書管理］→［クライアント証明書管理］→ ✚



項番	項目	説明
1	証明書ファイル	アップロードするクライアント証明書を指定します。［ファイルを選択］をクリックし、クライアント証明書ファイルを選択します。 PKCS #12 形式のクライアント証明書を指定してください。 ファイル名は 30 文字以内で設定してください。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを 255 文字以内の半角英数字で入力します。 パスワード未設定の場合は入力不要です。

◆画面（管理）

表示操作　［設定］→［Windows］→［証明書管理］→［クライアント証明書管理］

項番	項目	説明
1	検索/並び替え	（A）に検索対象項目、（B）に並び替えの対象項目が表示されます。 検索する場合は、検索するキーワードを（C）に入力し、［検索］をクリックします。検索したあとに、すべてのクライアント証明書を再表示するにはブラウザーを再読み込み、または（C）を空欄にし、再度［検索］ をクリックします。
2	✚	クリックするとクライアント証明書情報欄に入力欄が表示されます。 「画面（新規作成）」617 ページ
3	▼	クリックすると以下のメニューが表示されます。 ●全てにチェックを入れる 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスにチェックが入ります。 ●全てのチェックをはずす 選択するとクライアント証明書一覧にあるすべての証明書のチェックボックスのチェックが外れます。 ●検索対象 検索対象をファイル名、発行先（証明書情報）のいずれかに変更できます。 ●並べ替え 昇順 ユーザー一覧をファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで昇順に並び替えます。 ●並べ替え 降順 ファイル名、発行先（証明書情報）、有効期間の開始、有効期間の終了のいずれかで降順に並び替えます。 ●一括削除 クライアント証明書一覧でチェックの入っている証明書を削除します。
4	クライアント証明書一覧	登録されているクライアント証明書一覧が表示されます。 ●（D） クライアント証明書のファイル名です。 ●（E） 発行先（クライアント証明書情報）です。 ●（F） 有効期間です。
5	クライアント証明書情報	クライアント証明書一覧から選択したクライアント証明書の情報が表示されます。

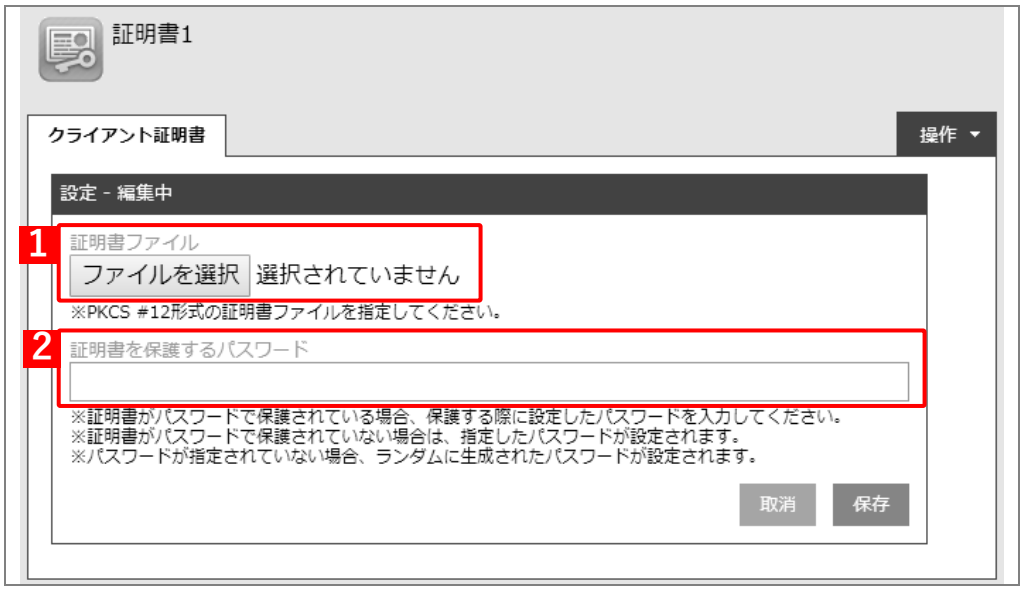
項番	項目	説明
6	［操作］	クリックすると以下のメニューが表示されます。 ●削除 クライアント証明書を削除します。
7	［編集］	クリックすると、登録されているクライアント証明書情報を編集できます。

◆画面（編集）

アップロード済みのクライアント証明書の差し替えやパスワードを変更する場合に内容を修正します。

設定項目は新規作成と同様です。

表示操作　**［設定］→［Windows］→［証明書管理］→［クライアント証明書管理］→一覧から対象を選択→［編集］**



項番	項目	説明
1	証明書ファイル	クライアント証明書一覧から再アップロードする証明書を指定します。
2	証明書を保護するパスワード	パスワードで保護されているクライアント証明書をアップロードする場合は、設定されているパスワードを入力します。パスワード未設定の場合は入力不要です。

9.6.2 クライアント証明書一括アップロード

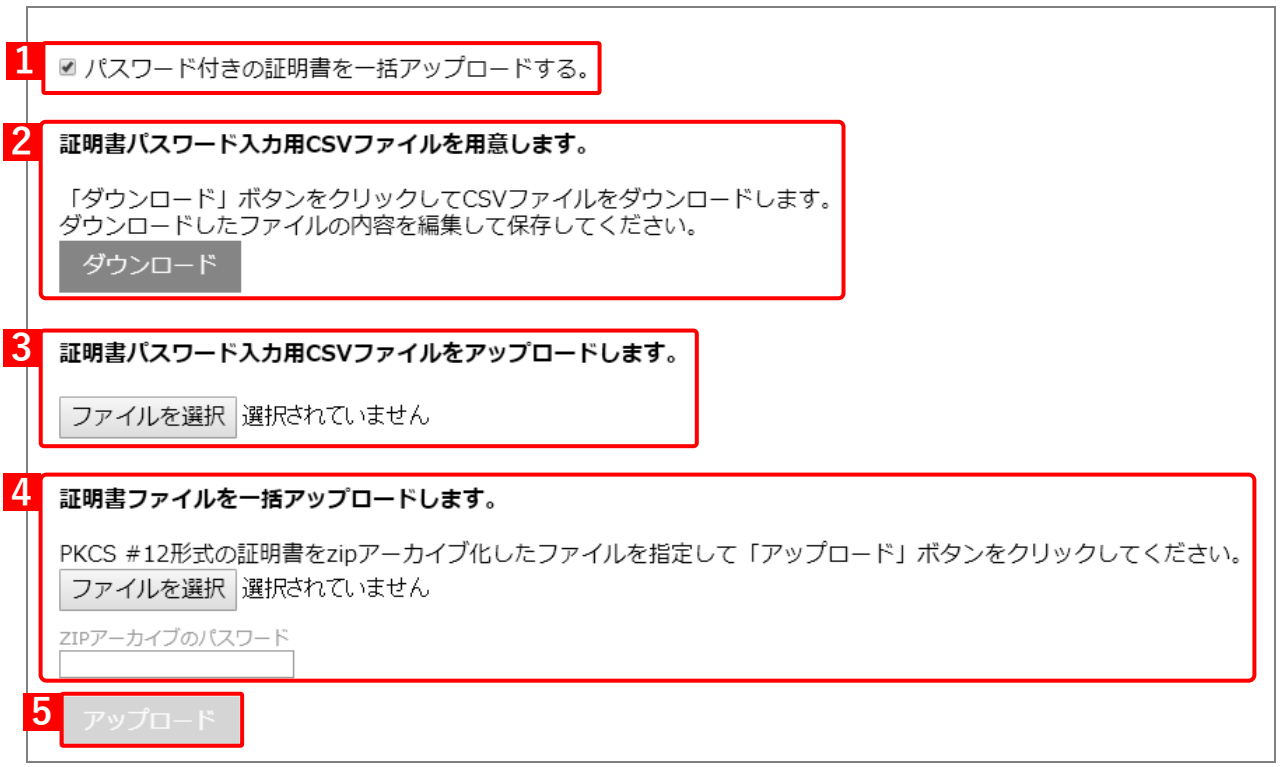
複数のクライアント証明書を ZIP ファイルにまとめて管理サイトにアップロードし、端末に配信するための設定セットを作成します。

本機能で作成したクライアント証明書の設定セットは、Android 端末、iOS 端末、Windows 端末で共有することができます。

- 事前にクライアント証明書を取得してください。
- アップロードする複数のクライアント証明書は、まとめて zip ファイル形式で保存してください。
- アップロード済みのクライアント証明書を差し替える場合は、以下を参照してください。
  ☞「画面（編集）」556 ページ
- 管理サイトにアップロードしたクライアント証明書は、以下の設定で利用します。
  ☞「（設定－Android）クライアント証明書」79 ページ
  ☞「（設定－iOS）クライアント証明書」86 ページ
  ☞「（設定－iOS）Exchange（ActiveSync）設定」89 ページ
  ☞「（設定－iOS）VPN 設定」94 ページ
  ☞「（設定－Windows）クライアント証明書」106 ページ

◆画面

表示操作 ［設定］→［Windows］→［証明書管理］→［クライアント証明書一括アップロード］→［パスワード付きの証明書を一括アップロードする］



項番	項目	説明
1	パスワード付きの証明書を一括アップロードする。	チェックを入れると、証明書パスワード入力用 CSV ファイルをアップロードできます。 パスワード付きのクライアント証明書でない場合は、チェックを入れません。

項番	項目	説明
2	証明書パスワード入力用 CSV ファイルを用意します。	証明書パスワード入力用 CSV ファイルをアップロードする場合、［ダウンロード］をクリックし、任意の場所に証明書パスワード入力用 CSV ファイルを保存します。保存したファイルを Excel やメモ帳で開き、クライアント証明書に設定されているパスワードを入力して保存します。 CSV ファイルの「[S]ファイル名」には、拡張子を除いたクライアント証明書のファイル名を入力してください。
3	証明書パスワード入力用 CSV ファイルをアップロードします。	［ファイルを選択］をクリックし、証明書パスワード入力用 CSV ファイルを選択します。
4	証明書ファイルを一括アップロードします。	［ファイルを選択］をクリックし、アップロードする ZIP ファイルを選択します。パスワードで保護された ZIP ファイルを選択した場合は、「ZIP アーカイブのパスワード」に設定されているパスワードを 255 文字以内の半角英数字で入力します。 一括でアップロードする PKCS #12 形式のクライアント証明書のファイルは、あらかじめ ZIP ファイルにまとめておく必要があります。 ファイル名は 30 文字以内で設定してください。
5	［アップロード］	クリックすると、ZIP ファイルに含まれるクライアント証明書の一覧が表示されます。表示内容に問題がないことを確認し、［アップロードを実行］をクリックします。 アップロード済みの同名のクライアント証明書を上書きする場合は「同じファイル名の証明書がすでに存在した場合は上書き保存する」にチェックを入れます。

9.6.3 クライアント証明書一括削除

管理サイトにアップロードされているクライアント証明書を、CSV ファイルを利用して一括で削除します。

操作手順については、以下を参照してください。

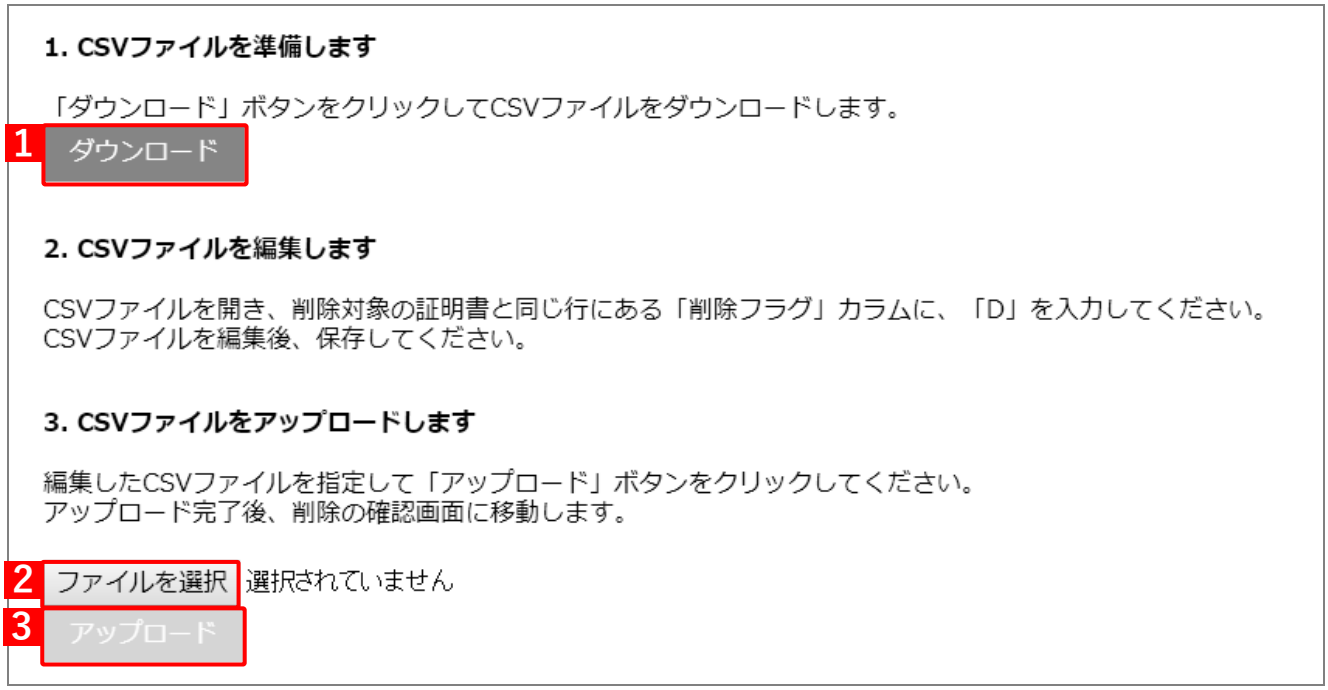
『かんたん初期設定マニュアル』の「補足・便利な操作」－「CSV ファイルの共通操作」

端末に紐づけられているクライアント証明書を削除した場合は、端末に割り当てられている設定が動作しなくなることがあります。

削除対象のクライアント証明書は、管理サイトからのみ削除され、Windows 端末からは削除されません。

◆画面

表示操作　［設定］→［Windows］→［証明書管理］→［クライアント証明書一括削除］



項番	項目	説明
1	［ダウンロード］	任意の場所にクライアント証明書を削除するための CSV ファイルを保存します。保存した CSV ファイルを Excel やメモ帳で開き、削除したいクライアント証明書名の右側にある「[S]削除フラグ」列に「D」と入力して保存します。
2	［ファイルを選択］	項番 1 で保存した CSV ファイルを選択します。
3	［アップロード］	CSV ファイルのアップロードが開始されます。アップロードが完了すると、インポート画面が表示されます。

9.6.4 CA 証明書管理

Windows 端末にインストールする CA 証明書をアップロードし、端末に適用する設定セットを作成します。

本機能でアップロードした CA 証明書は、Android、Windows で共有することができます。

画面（新規作成）

画面（CA 証明書の情報）

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

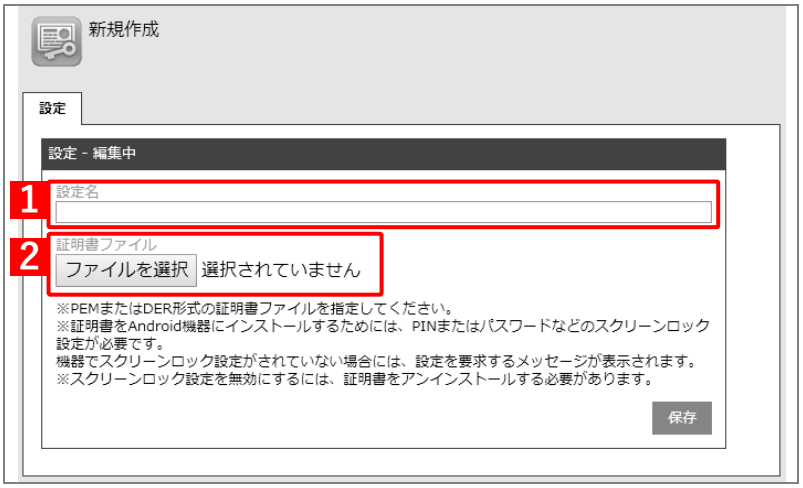
「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面（新規作成）

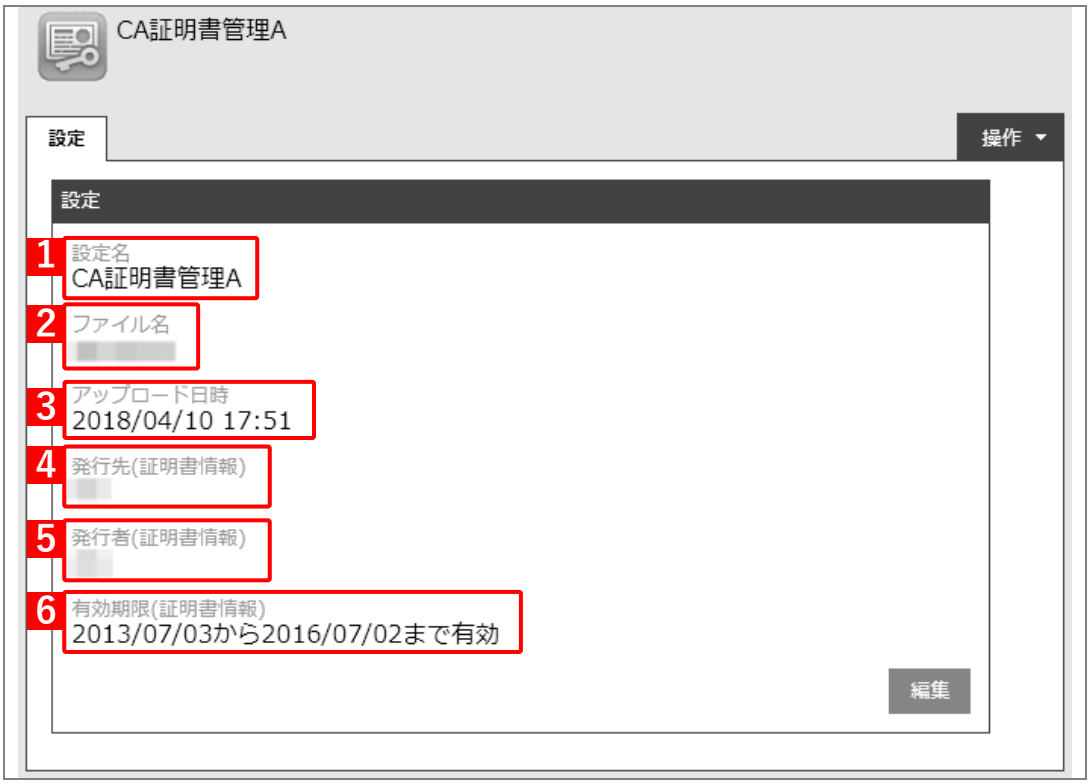
表示操作［設定］→［Windows］→［証明書管理］→［CA 証明書管理］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	証明書ファイル	［ファイルを選択］をクリックし、アップロードする CA 証明書を選択します。 PEM または DER 形式の CA 証明書ファイルを指定してください。 CA 証明書を Android 端末にインストールするには、PIN またはパスワードなどのスクリーンロック設定が必要です。機器でスクリーンロック設定がされていない場合は、設定を要求するメッセージが表示されます。 スクリーンロック設定を無効にするには、CA 証明書をアンインストールする必要があります。

◆画面（CA 証明書の情報）

表示操作　［設定］→［Windows］→［証明書管理］→［CA 証明書管理］→一覧から対象を選択



項番	項目	説明
1	設定名	設定した CA 証明書の名称が表示されます。
2	ファイル名	CA 証明書のファイル名が表示されます。
3	アップロード日時	CA 証明書ファイルのアップロード日時が表示されます。
4	発行先(証明書情報)	CA 証明書の発行先が表示されます。
5	発行者(証明書情報)	CA 証明書の発行者が表示されます。
6	有効期限(証明書情報)	CA 証明書の有効期限が表示されます。

9.7 Zone Management

特定のネットワーク・位置・時間帯を設定したゾーン設定と、Android 端末と Windows 端末に適用する各機能の設定セットを選択したポリシー設定を組み合わせ、ゾーンポリシー構成の設定セットを作成します。

学校や職場など、特定の条件下で使用する端末を設定する場合に有効な機能です。

本機能を Windows 端末に割り当てると、タスクトレイアイコンメニューに「ゾーン確認」、ツールバーに［ゾーン］のアイコンが表示されます。

『Windows クライアント リファレンスマニュアル』の「エージェントの基本操作」ー「タスクトレイアイコンメニューを表示する」、「ツールバーを表示する」

9.7.1 ゾーン

接続先のネットワーク・位置情報・時間帯を組み合わせ、ゾーン設定として保存します。

保存したゾーン設定をポリシー設定と組み合わせ、ゾーンポリシー構成の設定セットを作成します。

「ポリシー」628 ページ

「ゾーンポリシー構成」630 ページ

この設定は、Android と Windows で共有することができます。

単一のゾーンに複数の SSID を設定した場合は、いずれかの SSID が検知された場合に「ゾーン内」となります。また複数の位置情報とスケジュール設定も、いずれかの設定が満たされた場合に「ゾーン内」となります。SSID と位置情報、SSID とスケジュールなど、異なる設定を複数組み合わせる場合は、すべての設定を満たした場合に「ゾーン内」となります。

【複数の条件を組み合わせた場合】

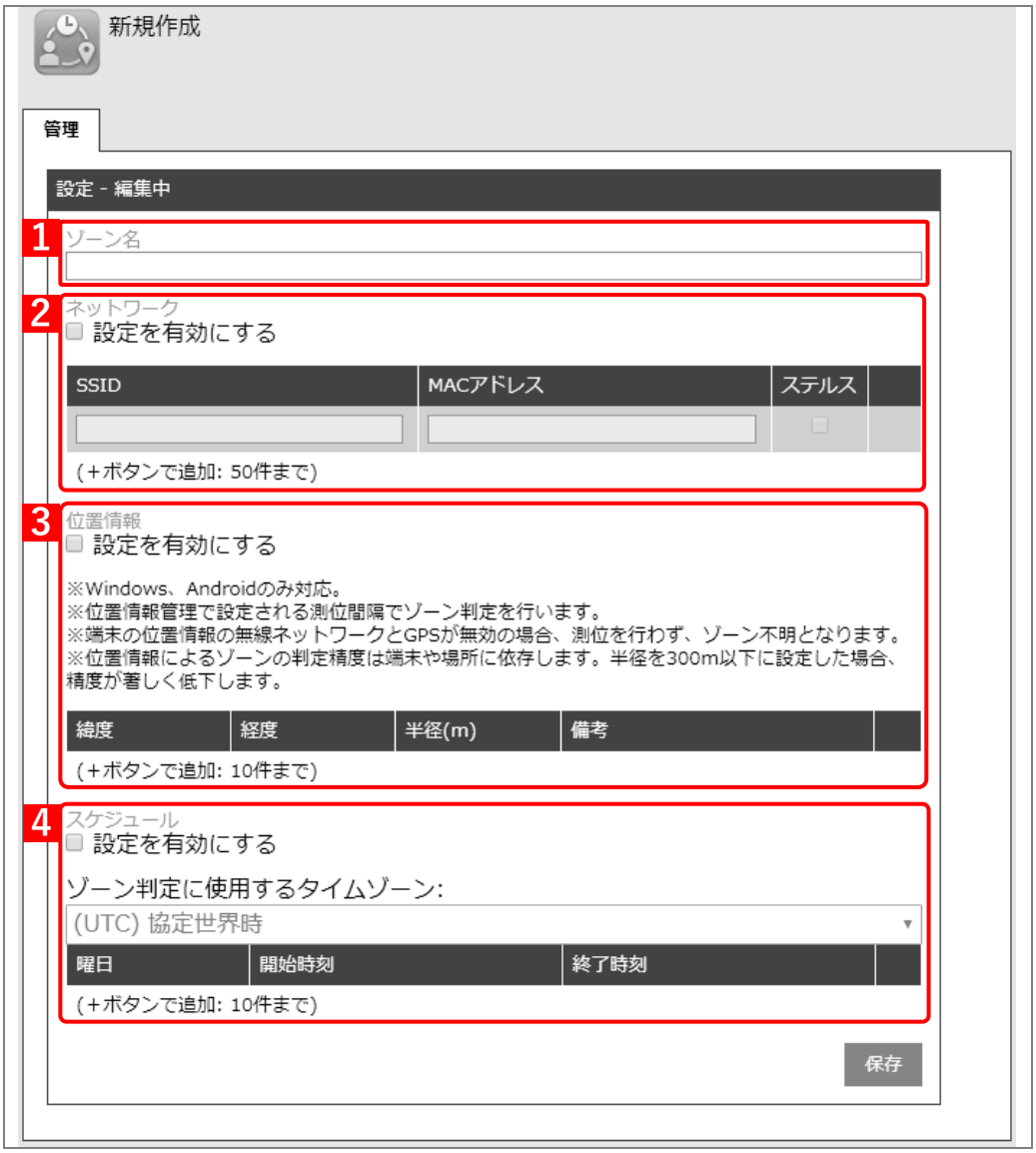
- 場所：SSID1、SSID2、SSID3
- 時間：月曜 17:00～18:00、土曜 16:00～17:30

  上記のゾーン設定では SSID が「SSID1」、「SSID2」、「SSID3」のいずれかに一致し、さらに日時が「月曜 17:00～18:00」、「土曜 16:00～17:30」のいずれかに一致した場合に「ゾーン内」となります。

ゾーン設定は、最大で 50 件まで作成できます。

◆画面

表示操作　［設定］→［Windows］→［Zone Management］→［ゾーン］→ ＋



項番	項目	説明
1	ゾーン名	ゾーンの名称を 1 文字から 30 文字で入力します。 先頭が「S」で始まる名称は設定できません。
2	ネットワーク	ゾーンに設定するネットワークの SSID、MAC アドレスの設定を行います。ネットワークは、50 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で、以降で設定するネットワークが有効になります。＋ をクリックし、必要なネットワークを追加します。 ●SSID ネットワークの SSID を 32 文字以内の半角英数字、「-」、「_」、「@」で入力します。 ●MAC アドレス アクセスポイントの MAC アドレスを入力します。「XX:XX:XX:XX:XX:XX」（X は大文字の 16 進数）という形式で入力してください。 ●ステルス SSID ステルスを有効としたネットワークの場合は、チェックを入れます。 SSID と MAC アドレスは重複しないものを入力してください。

項番	項目	説明
3	位置情報	ゾーンに設定する位置の緯度と経度、エリアの範囲を指定します。位置情報は 10 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で、以降で設定する位置情報が有効になります。 をクリックし、必要な位置情報を追加します。 ●緯度 -90 から 90 の範囲の値を入力します。 ●経度 -180 から 180 の範囲の値を入力します。 ●半径（m） 1 から 20037500 の範囲の値を入力します。 ●備考 備考が必要な場合は、30 文字以内で入力します。 端末の位置情報の無線ネットワークと GPS が無効な場合、または管理サイトの時刻と端末時刻の間に大幅な差がある場合は、測位を行わず「ゾーン不明」となります。「ゾーン不明」と判定された端末に特定のポリシーを適用できます。 ☞「ゾーンポリシー構成」362 ページ 位置情報の測位間隔の詳細については、以下を参照してください。 ☞「位置情報管理」576 ページ
4	スケジュール	ゾーンに設定するスケジュールを登録します。スケジュールは 10 件まで登録できます。 ●設定を有効にする チェックを入れると、Zone Management で以降で設定するスケジュールが有効になります。 をクリックし、必要なスケジュールを追加します。 ●ゾーン判定に使用するタイムゾーン タイムゾーンをリストボックスから選択します。 ●曜日 スケジュール設定を有効にする曜日にチェックを入れます。 ●開始時刻 開始時刻をリストボックスから選択して指定します。00:00 から 23:59 の間で指定します。 ●終了時刻 終了時刻をリストボックスから選択して指定します。00:00 から 35:59 の間で指定します。 土曜日に日またがりで Zone Management を設定する場合は、xx:xx から 24:00 までの設定と、日曜日 0:00 から 35:59 までの設定の 2 つを実施すると、日またがり後の制御ができます。

9.7.2 ポリシー

Android 端末と Windows 端末に適用する各機能の設定セットを選択し、ポリシー設定として保存します。

保存したポリシー設定をゾーン設定と組み合わせ、ゾーンポリシー構成の設定セットを作成します。

「ゾーン」625 ページ

「ゾーンポリシー構成」630 ページ

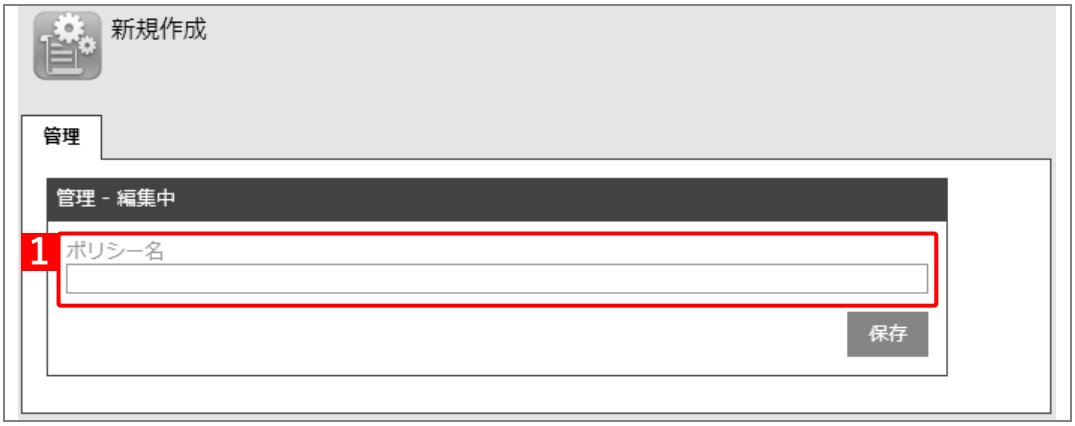
この設定は、Android と Windows で共有することができます。

設定セットは、最大 50 件まで作成できます。

9.7.2.1 ［管理］タブ

◆画面（新規作成）

表示操作　［設定］→［Windows］→［Zone Management］→［ポリシー］→ ＋



項番	項目	説明
1	ポリシー名	設定の名称を 1 文字から 30 文字で入力します。

9.7.2.2 ［Windows 設定］タブ

◆画面

表示操作 ［設定］→［Windows］→［Zone Management］→［ポリシー］→作成したポリシーを選択→［Windows 設定］タブをクリック→［編集］

項番	項目	説明
1	設定	ポリシーにおける Windows の設定セットの使用設定を行います。各機能に設定する内容を以下から選択します。 ●各機能の設定名 選択した設定セットを適用します。 ●(機器の設定に従う) ゾーンポリシー以外で設定されている設定が継承されます。 ●(所属組織に従う) 所属している組織の設定が適用されます。組織に所属していない場合は「(設定なし)」が適用されます。 ●(設定なし) 設定を変更しません。

9.7.3 ゾーンポリシー構成

ゾーン設定とポリシー設定を組み合わせて、ゾーンポリシー構成の設定セットを作成します。ゾーンポリシー構成を端末に適用すると、さまざまな場所や時間、ネットワークでの端末の動作を管理できます。

この設定は、Android と Windows で共有することができます。

事前にゾーンとポリシーを作成してください。

「ゾーン」625 ページ
「ポリシー」628 ページ

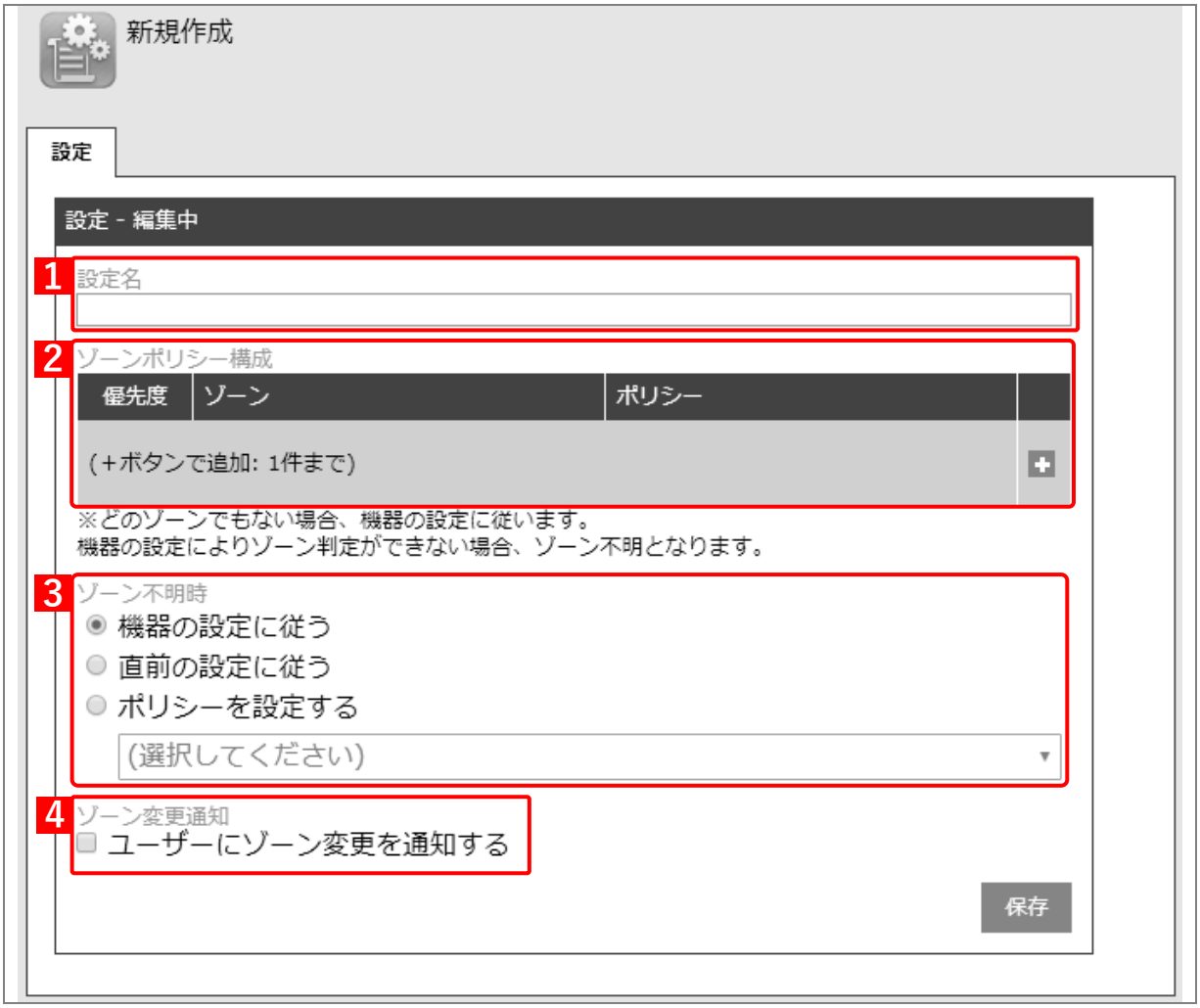
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「(設定－Windows) 設定セットの割り当て」103 ページ
「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作　［設定］→［Windows］→［Zone Management］→［ゾーンポリシー構成］→ ＋



項番	項目	説明
1	設定名	設定の名称を 1 文字から 30 文字で入力します。
2	ゾーンポリシー構成	ゾーンに設定するゾーン優先度、ゾーン、ゾーンポリシーを登録します。 ●ゾーン優先度 ゾーン優先度を入力します。 ●ゾーン ゾーンを選択します。 ☞「ゾーン」625 ページ ●ポリシー ゾーンのポリシーを選択します。 ☞「ポリシー」628 ページ
3	ゾーン不明時	ゾーン不明と判定された場合に適用される設定を以下から選択します。 ●機器の設定に従う ●直前の設定に従う ●ポリシーを設定する この設定を選択した場合は、適用するポリシーをリストボックスから選択します。 ゾーンで設定した項目ごとに以下の条件が当てはまる場合は、端末は「ゾーン判定不可」を検知して、管理サイトに「ゾーン不明」のステータスを送信します。 ・スケジュール 同期時にサーバーと端末の時刻が著しく異なる。 ・ネットワーク 機器設定により Wi-Fi が OFF に設定されている。 ・位置情報 「位置情報 OFF」に設定されている、または位置情報設定が「バッテリー節約」かつ「ネットワーク接続無し」に設定されている。 ゾーンの設定については、以下を参照してください。 ☞「ゾーン」625 ページ
4	ゾーン変更通知	端末のゾーンが変更されたときに、端末上に通知を表示します。 Android 端末では、通知領域、Windows 端末ではステータスバー上のバルーンに通知が表示されます。 スケジュールと位置情報によるゾーン設定によっては、大量の通知が発生する可能性があります。過度な情報通知により、ユーザーの利便性を下げてしまう可能性があるので慎重に設定してください。

10 サービス環境設定

この章では、サブヘッダーメニューの［サービス環境設定］画面に表示される、各種の設定について説明します。

10.1 通知設定

ログメール通知と無通信検知について設定します。

画面（ログメール通知の新規作成）

画面（無通信検知の新規作成）

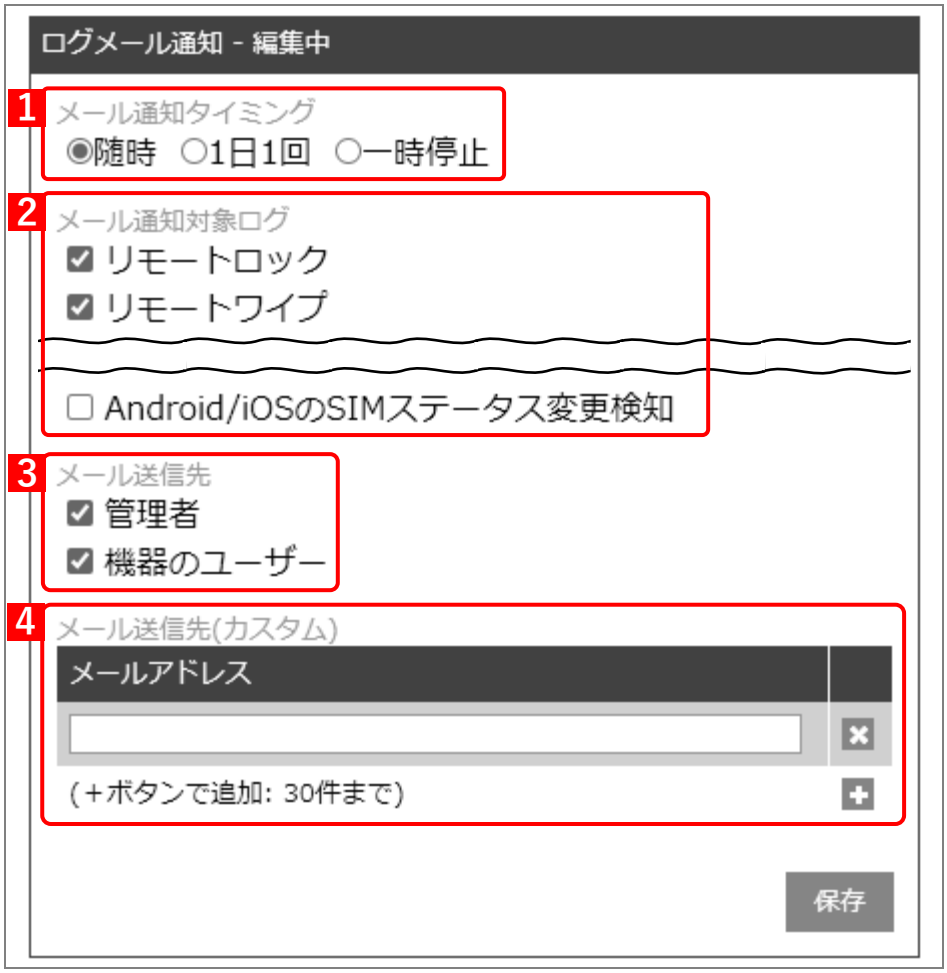
◆画面（ログメール通知の新規作成）

確認したいログをメールで通知します。

メールを通知するタイミング、対象となるログ、送信先などを指定することができます。

通知メールは「no-reply-biz@fxmits.optim.co.jp」から送信されます。

表示操作　［設定］→［サービス環境設定］→［通知設定］→「ログメール通知」の［新規作成］



項番	項目	説明
1	メール通知タイミング	メールで通知するタイミングを設定します。以下の項目から選択します。 ●随時 10 分ごとにメール通知を行います。 ●1 日 1 回 午前 3 時にメール通知を行います。 ●一時停止 メール通知を行いません。
2	メール通知対象ログ	通知対象とするログを指定します。必要な項目のチェックボックスにチェックを入れます。項目は複数指定できます。

項番	項目	説明
		以下に記載のないログについて、メール通知は行えません。 ログが通知される対象 OS は以下を参照してください。 「メール通知対象ログの対象 OS 一覧」635 ページ ●リモートロック ●リモートワイプ ●スクリーンロック設定のパスワード変更 ●無通信検知 ●root 化状態検知 ●Jailbreak 状態検知 「Jailbreak 状態検知」は iOS エージェントがインストールされていない場合は表示されません。 ●管理外検知 「管理外検知」は、プロファイルをアンインストールした iOS 端末を検知する機能です。検知した場合はログに出力されます。また、機器画面に表示している通信日時に「管理外」の文字が付与され、赤字で表示します。検知対象は「プロファイルをアンインストールしたか」で判断しているため、リモートワイプなど、アンインストール以外の方法でプロファイルを削除しても検知対象となりません。 ●Microsoft Update 未実施 ●Office 更新プログラムの未適用 ●Windows 更新プログラムの未適用 ●ウイルス対策ソフト ●スパイウェア対策ソフト ●アプリケーション検知 ●機器検出 ●Apple Push 証明書有効期限 Apple Push 証明書の有効期間が一定の日数以内となったときに出力するログです。通知タイミングは、60 日前、30 日前、14 日前、7 日前から有効期限前日までの毎日です。 ●ADE トークン有効期限 ADE トークンの有効期間が一定の日数以内となったときに出力するログです。通知タイミングは、60 日前、30 日前、14 日前、7 日前から有効期限前日までの毎日です。 ●シングル APP モードの適用延期 ●スクリーンロック解除失敗時のリモートロック・ワイプ ●Windows の SIM 抜き差し監視 ●Windows のファイアウォール診断 ●Windows の Guest アカウント診断 ●Windows の自動アップデート診断 ●Windows 以外の Microsoft 製品のアップデート診断 ●Windows のスクリーンセーバー診断 ●Windows Defender のリアルタイム保護診断 ●Windows Defender のクラウド提供の保護診断 ●Windows Defender のサンプルの自動送信診断 ●Windows Defender のコントロールされたフォルダーアクセス診断 ●システムセキュリティの Office 設定結果 ●システムセキュリティのブラウザー設定結果 ●アカウントのロックアウト ●アプリケーション使用禁止 ●外部デバイス・CD/DVD/ブルーレイ禁止 ●位置情報設定の変更 ●エージェント認証解除時の機器削除

項番	項目	説明
		●デバイス管理者権限の無効化 ●ゼロタッチ利用規約更新 ●Android/iOS の SIM ステータス変更検知
3	メール送信先	メール通知の送信先を以下の項目から選択します。送信先は複数選択できます。 ●管理者 ユーザー種別が管理者として登録されているユーザーのメールアドレスに送信します。 ●機器のユーザー 機器に登録されているユーザーのメールアドレスに送信します。
4	メール送信先(カスタム)	「メール送信先」以外にも送信したいときに設定します。自由にメールアドレスを指定できます。「メール送信先(カスタム)」は 255 文字以内の半角英数字と記号で入力してください。@の前後にそれぞれ 1 文字以上入力してください。送信先は 30 箇所まで設定できます。また、「メール送信先」と併用できます。 をクリックすると、入力欄が追加されます。 をクリックすると、入力欄が削除されます。

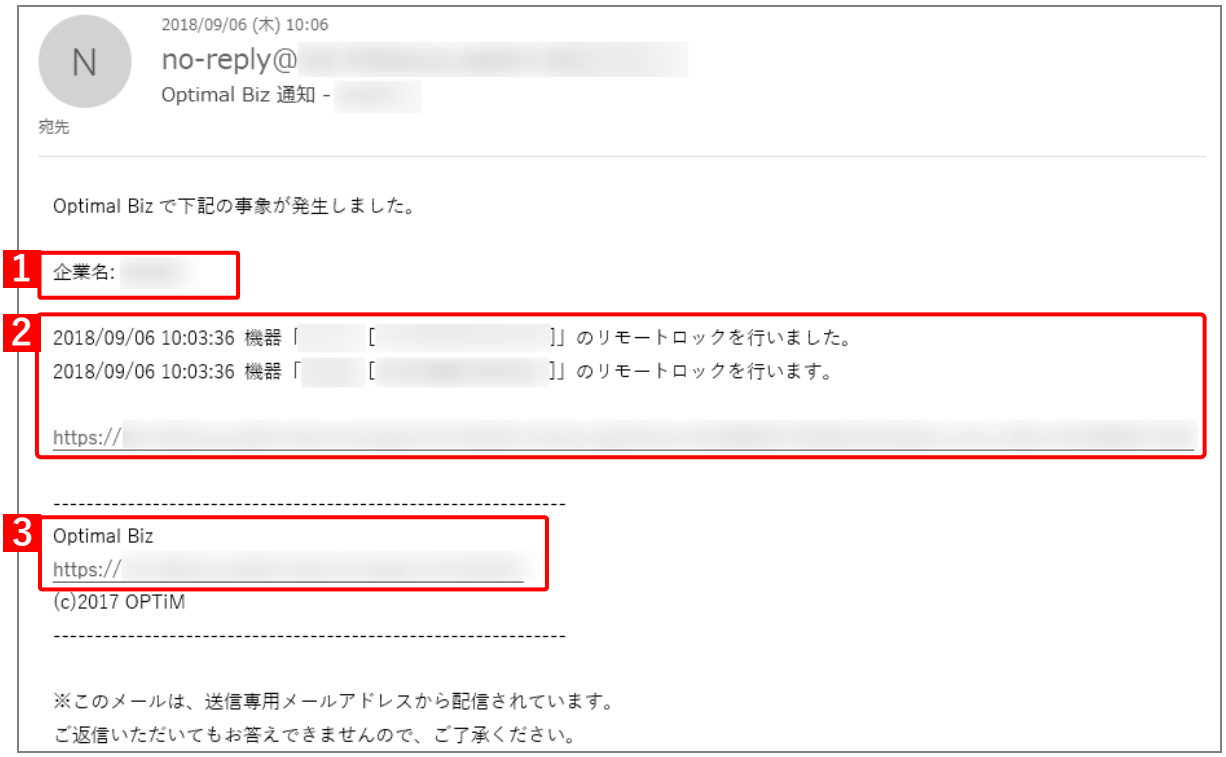
◆メール通知対象ログの対象 OS 一覧

メール通知対象ログ	Android	iOS	Windows
リモートロック	○	○	○
リモートワイプ	○	○	○
スクリーンロック設定のパスワード変更	○	–	–
無通信検知	○	○	○
root 化状態検知	○	–	–
Jailbreak 状態検知	–	○	–
管理外検知	–	○	–
Microsoft Update 未実施	–	–	○
Office 更新プログラムの未適用	–	–	○
Windows 更新プログラムの未適用	–	–	○
ウイルス対策ソフト	○	–	○
スパイウェア対策ソフト	–	–	○
アプリケーション検知	○	○	–
機器検出	–	–	○
Apple Push 証明書有効期限	–	○	–
ADE トークン有効期限	–	○	–
シングル APP モードの適用延期	–	○	–
スクリーンロック解除失敗時のリモートロック・ワイプ	○	–	○
Windows の SIM 抜き差し監視	–	–	○
Windows のファイアウォール診断	–	–	○
Windows の Guest アカウント診断	–	–	○
Windows の自動アップデート診断	–	–	○
Windows 以外の Microsoft 製品のアップデート診断	–	–	○
Windows のスクリーンセーバー診断	–	–	○
Windows Defender のリアルタイム保護診断	–	–	○
Windows Defender のクラウド提供の保護診断	–	–	○
Windows Defender のサンプルの自動送信診断	–	–	○

メール通知対象ログ	Android	iOS	Windows
Windows Defender のコントロールされたフォルダーアクセス診断	–	–	○
システムセキュリティの Office 設定結果	–	–	○
システムセキュリティのブラウザー設定結果	–	–	○
アプリケーション使用禁止	○	–	○
外部デバイス・CD/DVD/ブルーレイ禁止	–	–	○
位置情報設定の変更	○	–	–
エージェント認証解除時の機器削除	–	–	○
デバイス管理者権限の無効化	○	–	–
ゼロタッチ利用規約更新	○	–	–
Android/iOS の SIM ステータス変更検知	○	○	–

◆ログメール通知のサンプル

ログメール通知設定の「メール通知対象ログ」で対象とした事象が発生した場合に、以下のようなメールが「メール送信先」および「メール送信先(カスタム)」で設定した送信先に届きます。



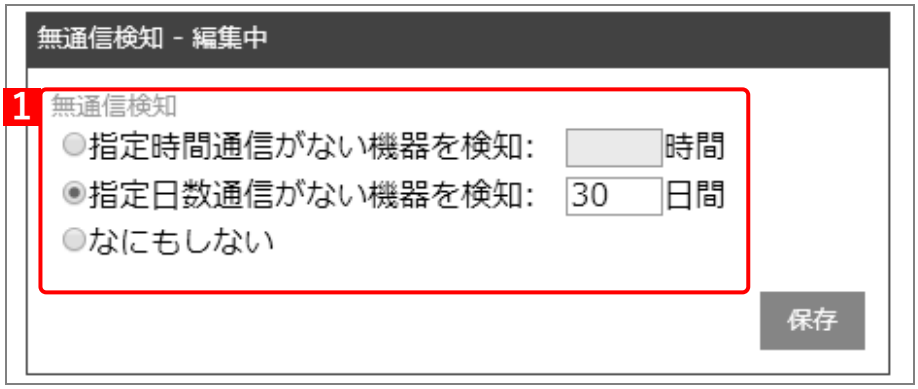
項番	項目	説明
1	企業名	企業名が表示されます。
2	ログ	発生した事象についてのログが表示されます。表示される内容は以下のとおりです。 ●日時 ●端末名 ●メール通知対象ログ ●URL URL をクリックするとログ画面にアクセスし、該当のログが表示されます。
3	管理サイト	URL をクリックすると管理サイトログイン画面が表示されます。

◆画面（無通信検知の新規作成）

指定した間隔で管理サーバーと通信が行われていない端末を検知します。検知した場合はログに出力されます。また、［機器］の一覧画面に表示している通信日時を赤字で表示します。

無通信検知の対象は「指定した間隔で管理サーバーと通信が行われているか」で判断しているため、端末の通信状態が良好でも管理サーバーと通信を行っていなければ検知対象となります。また、一般的なメールやインターネットの利用も管理サーバーと通信を行っていることになりません。

表示操作　［設定］→［サービス環境設定］→［通知設定］→「無通信検知」の［新規作成］



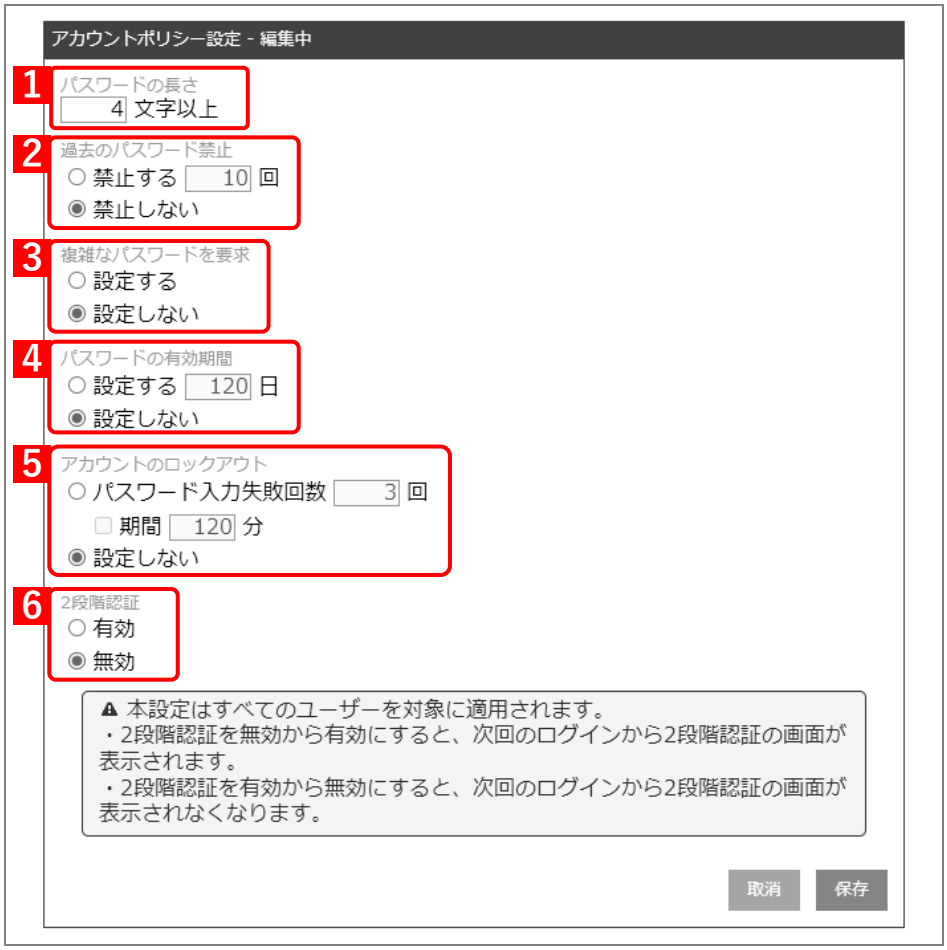
項番	項目	説明
1	無通信検知	無通信と判断する間隔を指定します。以下の項目から選択します。 ●指定時間通信がない機器を検知 選択した場合、時間を 1 から 23 の間の半角数字で入力してください。 ●指定日数通信がない機器を検知 選択した場合、日数を 1 から 365 の間の半角数字で入力してください。 ●なにもしない 無通信検知を行いません。

10.2 アカウントポリシー

パスワードの発行や制限、ロックアウトするまでの入力回数を設定します。

◆画面

表示操作　［設定］→［サービス環境設定］→［アカウントポリシー］→［編集］



項番	項目	説明
1	パスワードの長さ	ログインパスワードの長さを 4 文字以上 32 文字以内で指定します。
2	過去のパスワード禁止	以前使用したパスワードの利用可否の設定です。以下の項目から選択します。 ●禁止する 一度使用したパスワードを指定回数禁止するときに使用します。選択すると回数の設定が必須となり、「再利用できるまでに必要な新しいパスワードの設定回数」を設定します。回数は 1 から 100 の整数で入力してください。指定した変更回数を超えない限り、以前使用したパスワードは利用できません。例えば 3 回とした場合、新しいパスワードが 3 回設定されるまで以前のパスワードは利用できません。 ●禁止しない 以前使用したパスワードの再利用を禁止しません。即座に再利用できます。

項番	項目	説明
3	複雑なパスワードを要求	パスワードの設定に複雑なパスワードを要求するかどうかの設定です。以下の項目から選択します。 ●設定する 複雑なパスワードの規則を適用します。設定した場合、新しく設定するパスワードは、以下の複雑さの要件を満たす必要があります。 ・ユーザーのアカウント名またはメールアドレスに含まれる 3 文字以上連続する文字列を使用しない。 ・長さは 8 文字以上。 ・以下の 4 つのカテゴリのうち 3 つから文字を使う。 ・英大文字（A から Z）。 ・英小文字（a から z）。 ・10 進数の数字（0 から 9）。 ・アルファベット以外の文字（!、$、#、%など）。 ●設定しない 複雑なパスワードの規則を適用しません。
4	パスワードの有効期間	パスワードの有効期間を指定します。以下の項目から選択します。 ●設定する パスワードの有効期間を日数で指定します。日数を 1 から 999 の整数で入力してください。 設定した場合、パスワードの有効期間が切れるとログイン時にパスワード再設定画面が表示されますので、新しいパスワードを設定してください。 『かんたん初期設定マニュアル』の「補足・便利な操作」－「ログイン／ログアウト」－「期限切れパスワードを更新する」 ●設定しない パスワードの有効期間を指定しません。
5	アカウントのロックアウト	パスワードの入力を失敗したときにアカウントをロックアウト（ログインできない状態）するかどうか指定します。以下の項目から選択します。 ●パスワード入力失敗回数 設定した回数、パスワードの入力を失敗するとアカウントをロックアウトします。ロックアウトまでの連続ログイン失敗回数を 1 から 10 の間で入力してください。 ・期間 チェックを入れると、自動でロックアウトが解除されるまでの分数を指定できます。チェックを入れない場合は、自動でロックアウトの解除は行われません。手動でロックアウトの解除を行ってください。 ロックされたアカウントの解除は以下を参照してください。 「［操作］タブ」261 ページ ●設定しない パスワードの入力を失敗してもアカウントをロックアウトしません。
6	2 段階認証	ログイン時に 2 段階認証を使用するかを以下の項目から選択します。 ●［有効］ 次回ログインから、2 段階認証の画面が表示されます。 ●［無効］ 次回ログインから、2 段階認証の画面は表示されません。 ［有効］から［無効］に変更すると、設定している設定値は、すべて削除されます。

10.3 機器認証制御

すべての端末にライセンス認証を行うか、認証待ち機器として事前登録されている端末のみにライセンス認証を行うかを設定します。

端末の事前登録については、以下を参照してください。

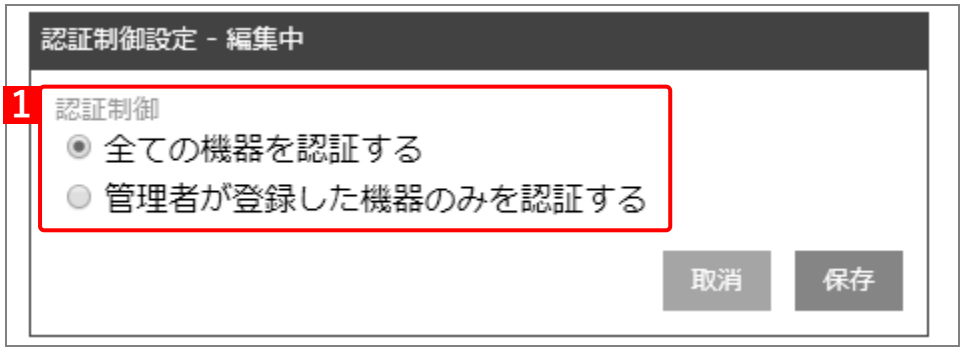
「機器の新規作成」61 ページ

設定を保存した時点ですべての端末に適用されます。ただし、設定が端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。

OS ごとに機器認証制御を設定することはできません。

◆画面

表示操作　［設定］→［サービス環境設定］→［機器認証制御］→［編集］



項番	項目	説明
1	認証制御	認証制御について以下の項目から選択します。 ●全ての機器を認証する すべての機器でライセンス認証が行えます。認証待ち機器としての事前登録は不要です。 ●管理者が登録した機器のみを検証する 認証待ち機器として事前登録されている機器でのみライセンス認証が行えます。

10.4 ポータル表示

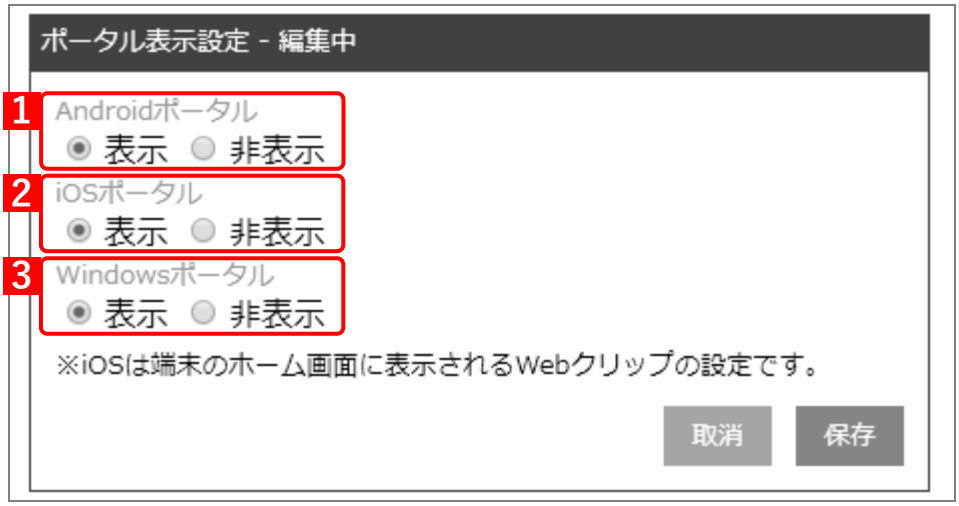
端末のポータルメニュー（端末から直接、ユーザーや機器カスタム項目の選択などを行うための機能）を表示するか非表示を設定します。

設定は OS ごとに行います。端末単位での設定はできません。

設定を保存した時点ですべての端末に適用されます。ただし、設定が端末に反映されるまでの時間は、サーバーや端末の通信状態に依存します。

◆画面

表示操作［設定］→［サービス環境設定］→［ポータル表示］→［編集］



項番	項目	説明
1	Android ポータル	Android ポータルの表示または非表示を指定します。 ●表示 ●非表示
2	iOS ポータル	iOS ポータルの表示または非表示を指定します。 ●表示 ●非表示
3	Windows ポータル	Windows ポータルの表示または非表示を指定します。 ●表示 ●非表示

10.5 Android Enterprise（企業アカウント登録）

Android Enterprise（企業アカウント登録）は、Android 端末のキッティング、managed Google Play ストアのアプリのサイレントインストールを行います。

Android Enterprise（企業アカウント登録）を利用するには、企業アカウントを Google play に登録する必要があります。登録方法の詳細は、以下のマニュアルを参照してください。

『Android キッティングマニュアル』

アプリの配信については、以下のマニュアルを参照してください。

『Android Enterprise アプリケーション配信 手順書』

10.6 Apple Push 証明書

iOS 端末の管理に必要な Apple Push 証明書を登録します。

Apple Push 証明書の詳細については以下を参照してください

『Apple Push 証明書年次更新マニュアル』

10.7 かんたん初期設定

本製品ではじめて端末の管理を行うときは、［かんたん初期設定］を使用して、セキュリティ設定などの初期設定を管理サイトで作成し、端末に反映します。

［かんたん初期設定］の設定手順は、以下を参照してください。

『かんたん初期設定マニュアル』の「端末の管理を開始する」－「初期設定をする」

［かんたん初期設定］では、一括で以下の機能の設定、設定セットが作成されます。設定セットは「EasySetup」という設定名で作成されます。設定内容は、必要に応じて変更することができます。機能や設定内容の詳細は、各機能の説明ページを参照してください。

項番	OS	機能		設定内容
1	Android	設定テンプレート		項番 2～3 で作成されたセキュリティ機能の設定セットが適用されます。
2		セキュリティ	画面ロック	端末のロック画面でパスワードの入力が必須に設定されます。 ●パスワードポリシーは英数字を含む 8 文字以上 ●自動ロックまでの時間 5 分
3			位置情報管理	「エージェントによる測位」が［定期的に測位する：30 分］に設定されます。
4	iOS	設定テンプレート		項番 6 で作成された［構成プロファイル］の設定セットが適用されます。
5		構成プロファイルアップロード［パスコード設定］タブ		端末のロック画面でパスワードの入力が必須に設定されます。 ●パスワードポリシーは英数字を含む 8 文字以上 ●自動ロックまでの時間 5 分
6		構成プロファイル		項番 5 で作成された［構成プロファイルのアップロード］の設定セットが適用されます。
7	Windows	設定テンプレート		項番 8～10 で作成されたセキュリティ機能の設定セットが適用されます。
8		セキュリティ	画面ロック	端末のロック画面でパスワードの入力が必須に設定されます。 ●パスワードポリシーは英数字を含む 8 文字以上 ●自動ロックまでの時間 5 分
9			暗号化	「BitLocker」が［有効化する］に設定されます。
10			位置情報管理	「エージェントによる測位」が［定期的に測位する：30 分］に設定されます。

11 ログ

この章では、ヘッダーメニューの［ログ］画面に表示される、各種の項目について説明します。

ログ一覧は、以下を参照してください。

『ログ一覧』の「ログ一覧」

11.1 ログ画面の見かた

ログ画面では、管理サイトの操作状況や端末の設定、操作の発生時間、操作概要を確認できます。また、端末に対する設定や操作が正常に行われたかどうかを確認する場合も、本画面から確認することができます。

検索機能で特定の端末を検索すると、ログの一覧を CSV ファイルにダウンロードすることができます。

画面

画面（ログの絞り込み）

画面（ログのダウンロード）

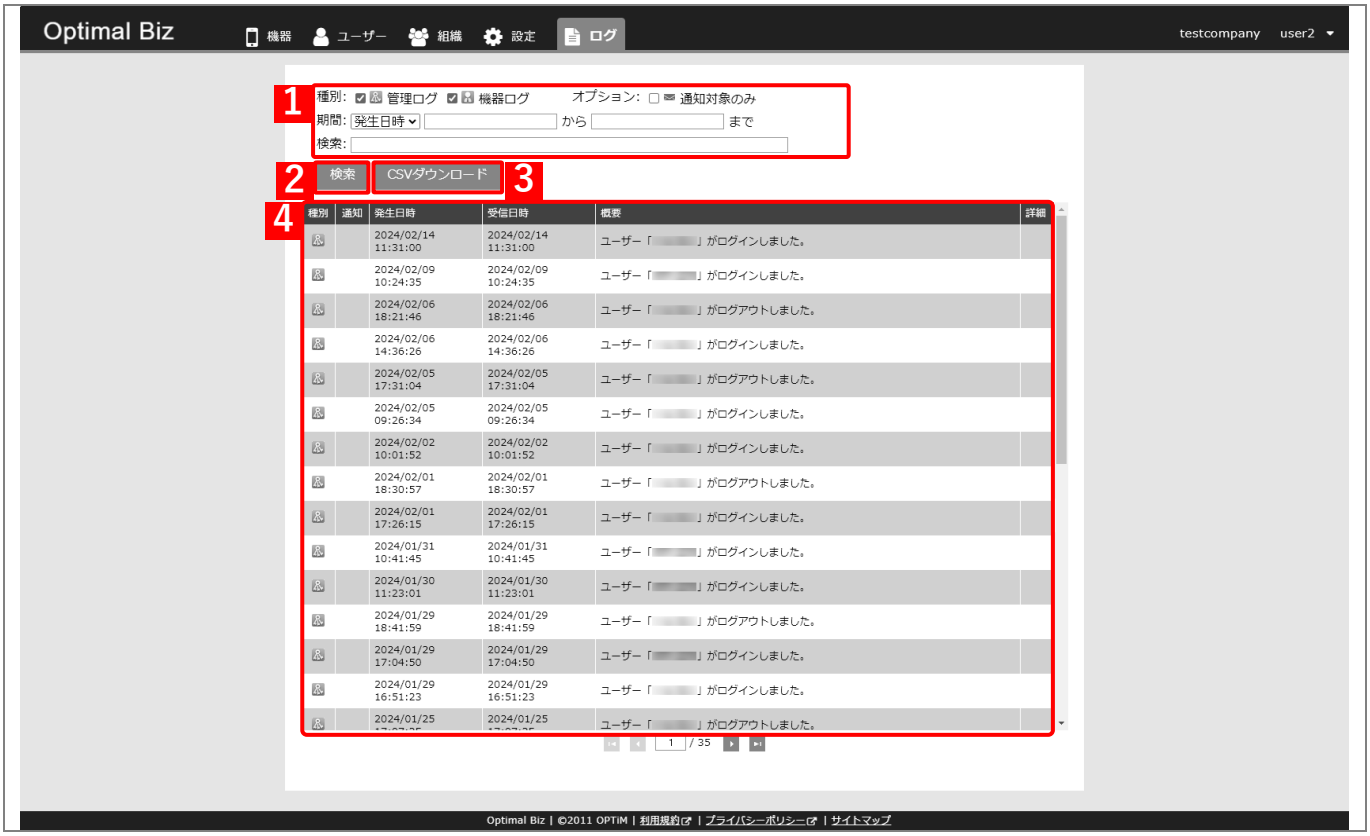
直近一年間のログを確認できます。ログの保存期間は一年間で、それ以前のログは削除されます。

［機器］→［一覧］→→［ログ］で確認するログは、一覧で選択した端末のログのみを表示します。

1 回のログに最大 255 文字が出力されます。機器、ユーザー、組織の一括削除を行った場合は、削除した件数により、機器名、ユーザー名、組織名がログに表示されないことがあります。削除したすべての機器名、ユーザー名、組織名を確認したい場合は、「詳細」のリンクをクリックして、ログの詳細情報から確認してください。

◆画面

表示操作［ログ］



項番	項目	説明
1	検索条件	表示するログを絞り込むための条件を設定できます。絞り込みについては、以下を参照してください。 「画面（ログの絞り込み）」648 ページ
2	［検索］	クリックすると、項番【1】で設定した検索条件でログの絞り込みが実行されます。絞り込みについては、以下を参照してください。 「画面（ログの絞り込み）」648 ページ

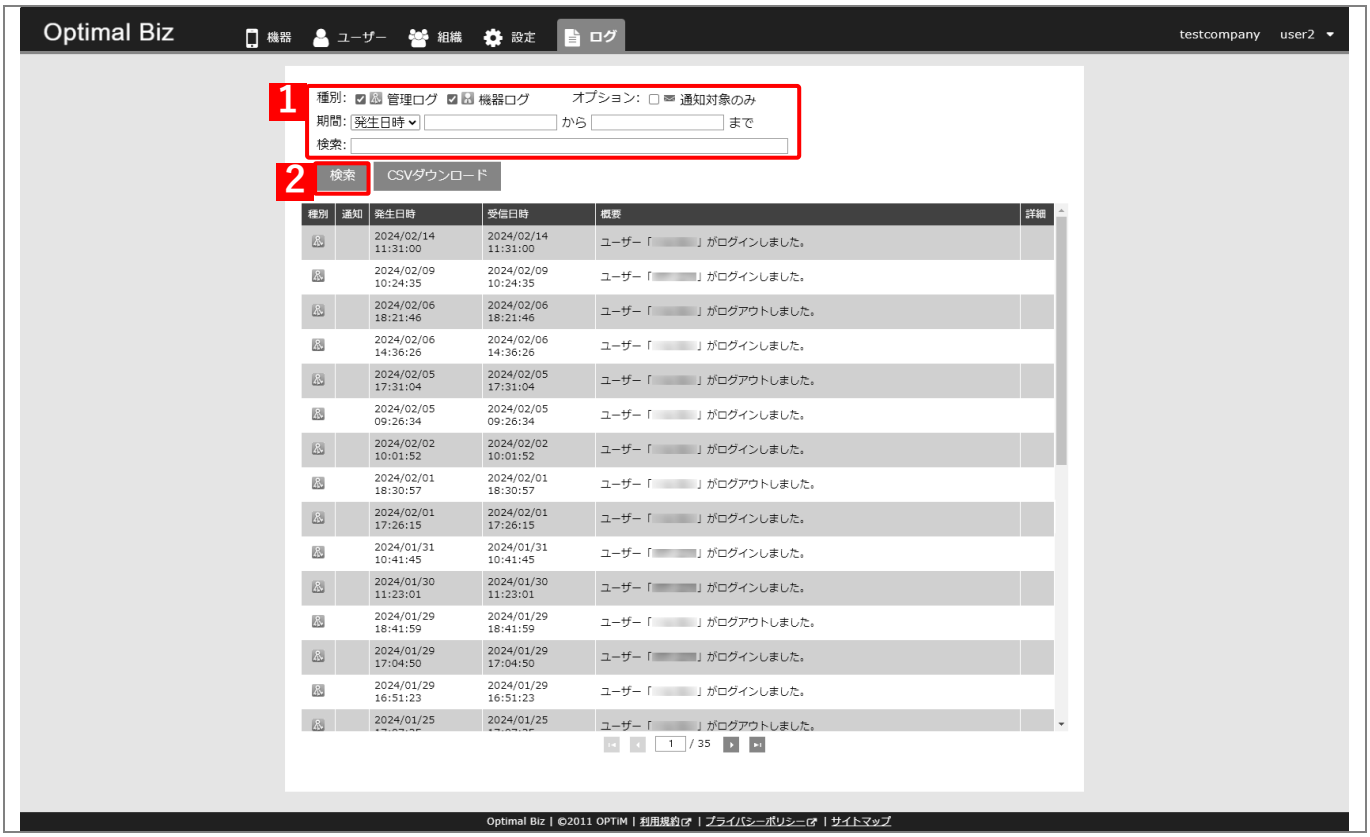
項番	項目	説明
3	［CSV ダウンロード］	クリックすると、ログの CSV がダウンロードします。詳細については、以下を参照してください。 ☞「画面（ログのダウンロード）」649 ページ
4	ログ一覧	管理サイトの操作ログや端末の操作や動作のログが表示されます。 ●種別 ・管理サイト操作ログの場合は が表示されます。 ・エージェントの動作ログの場合は が表示されます。 ●通知 ・メール通知済みの場合は が表示されます。 ・メール未通知の場合は が表示されます。 メール通知対象外の場合は何も表示されません。 ●発生日時 該当アクションが発生したときのエージェント（端末）の日時が表示されます。 ●受信日時 該当アクションが発生し、サーバーで受信した日時が表示されます。 ●概要 アクションの概要が表示されます。 ●詳細 詳細情報がある場合は、「詳細」のリンクが表示されます。クリックすると、対象のログの詳細情報が表示されます。

◆画面（ログの絞り込み）

検索条件を指定して、表示するログを絞り込みます。

期間のみ入力されている場合は、指定した期間のログがすべて表示されます。
検索キーワードのみ入力されている場合は、そのキーワードを含むログがすべて表示されます。

表示操作［ログ］



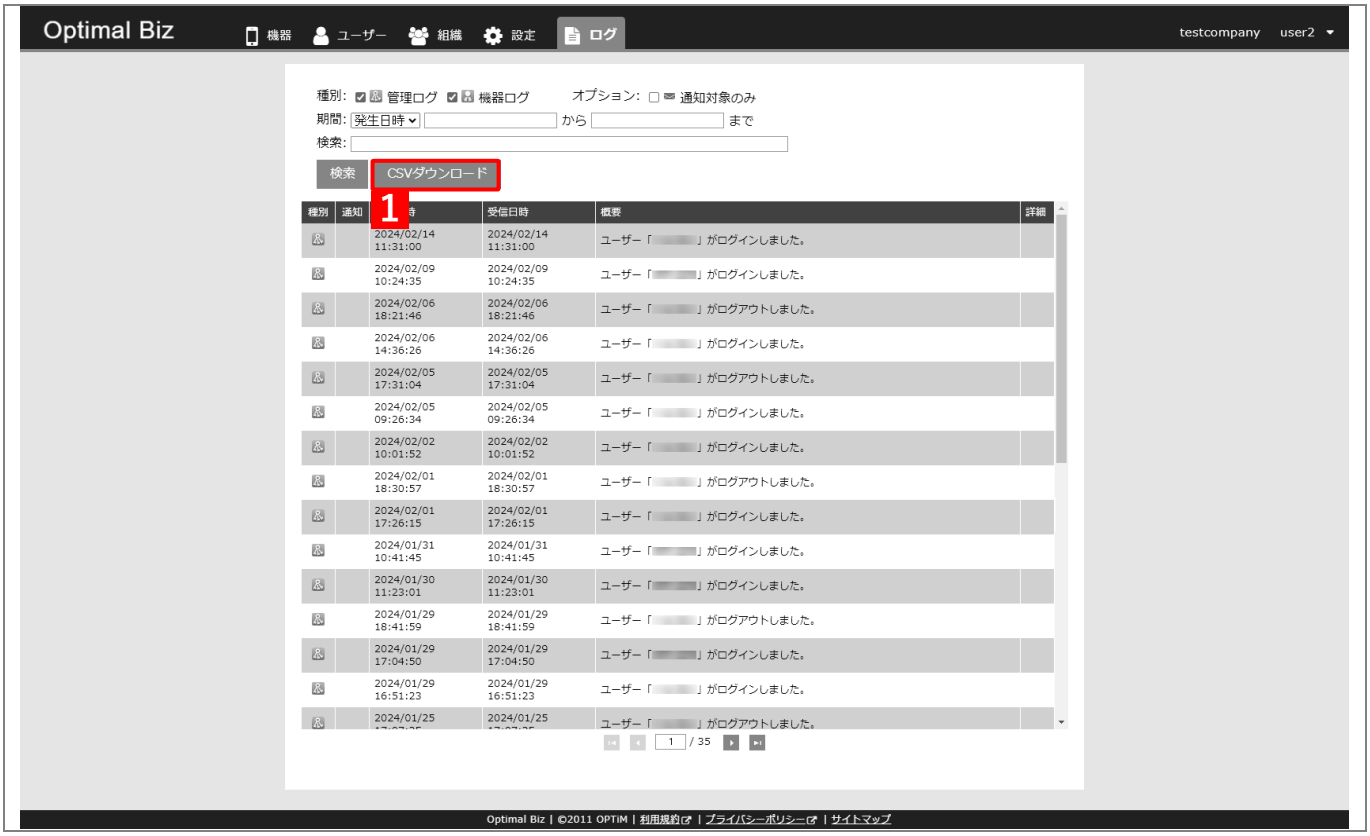
項番	項目	説明
1	検索条件	絞り込み条件を指定します。 ●種別 種別を指定します。以下のいずれか 1 つまたは両方にチェックを入れます。 ・管理ログ 管理サイトで行われた操作についてのログを表示します。 ・機器ログ 端末で行われた操作および端末の挙動についてのログを表示します。管理サイトの操作により端末で行われた挙動も該当します。 ●オプション ・通知対象のみ チェックするとログメール通知の対象となっているログのみを表示します。 ☞「画面」646 ページ ●期間 検索対象の日時の種類を選択し、日時の範囲を指定します。 ・発生日時 発生日時で期間を絞り込む場合に選択し、絞り込む日時の期間を設定します。 ・受信日時 受信日時で期間を絞り込む場合に選択し、絞り込む日時の期間を設定します。 日時の期間は「[　] から [　] まで」の形式で指定できます。「[　] から」のみ、「[　] まで」のみの指定もできます。

項番	項目	説明
		日時の入力欄をクリックするとカレンダーが表示され、日付、時間を設定できます。入力欄に直接入力もできます。 ●検索 ログの「概要」に表示されるキーワードで内容を絞り込みます。入力した文字列が概要に含まれるログを表示します。
2	［検索］	クリックすると、条件に合ったログの絞り込み検索が実行され、検索結果がログの一覧に表示されます。 再度すべてのログを表示するには、以下のいずれかを行う必要があります。 ・ログの一覧で、キーボードの［F5］キーでブラウザーを再読み込みします。 ・検索条件の「期間」、「検索」を空欄にし、［検索］をクリックします。

◆画面（ログのダウンロード）

現在ログ画面に表示されているすべてのログを、CSV ファイルとしてダウンロードします。最大 100,000 件のログをダウンロードできます。

表示操作　［ログ］



項番	項目	説明
1	［CSV ダウンロード］	表示されているすべてのログを CSV ファイルとしてダウンロードします。実行するには、確認画面で［OK］をクリックします。取り消す場合は、［キャンセル］をクリックします。 件数によってはダウンロードに時間がかかる場合があります。

12 サイトマップ

この章では、ダッシュボードの［サイトマップ］画面にのみ表示される一部の機能について説明します。

サイトマップへのアクセス方法については、以下を参照してください。

☞「管理サイト画面の構成」18 ページ

12.1 組織図

登録されている組織をツリー状の組織図で表示します。組織構造を視覚的に確認することができます。また、各組織アイコンをクリックすると、［組織］画面が表示されます。組織の詳細については、以下を参照してください。

☞「一覧」282 ページ

◆画面

表示操作　［**サイトマップ**］→［**組織図**］

項番	名称	説明
1	組織図	登録されている組織をツリー状に表示します。 ＋ をクリックすると直下の組織を表示します。 － をクリックすると表示されている直下の組織を非表示にします。
2	全てを展開する	クリックするとすべての組織を表示します。 組織図中のすべての ＋ をクリックした場合と同様の動きです。
3	全てを閉じる	クリックすると最上位の組織のみを表示します。 組織図中のすべての － をクリックした場合と同様の動きです。

12.2 管理外機器エクスポート

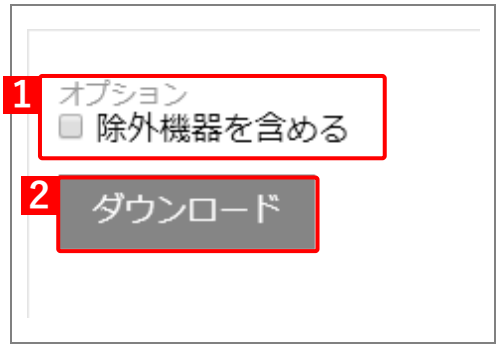
管理外機器の一覧を出力（エクスポート）します。管理外機器の詳細については、以下を参照してください。

☞「機器の種類」190 ページ

出力時の文字コードは日本語環境では Shift-JIS（CP932）、その他の環境では UTF-8 です。

◆画面

表示操作［**サイトマップ**］→［**管理外機器エクスポート**］



項番	名称	説明
1	オプション	●除外機器を含める ダウンロードするファイルに除外機器を含める場合は、チェックボックスにチェックを入れます。除外機器の詳細については、以下を参照してください。 ☞「機器の種類」190 ページ
2	［ダウンロード］	クリックするとファイルのダウンロードが開始されます。任意の場所に CSV ファイルを保存します。

12.3 ネットワーク

マップで検出されたネットワークに、ネットワーク名の設定や管理外機器の検出の設定を行うことができます。

ネットワークは、グローバルネットワークとローカルエリアネットワークの 2 種類があり、グローバルネットワークは新規作成や編集が行えます。また、ローカルエリアネットワークは編集のみ行えます。

画面

画面（新規作成）

画面（ローカルネットワークの編集）

◆画面

表示操作［**サイトマップ**］→［**ネットワーク**］

以下の画面は、特定のネットワーク設定をネットワーク一覧から選択すると表示されます。

項番	名称	説明
1	検索／表示条件	ネットワーク一覧から絞り込む、「検索」(検索項目)、「フィルター」(フィルター項目)、「昇順」または「降順」(並べ替え項目) が表示されます。各項目は をクリックして選択します。
2		クリックするとネットワーク設定の「新規作成」画面が表示されます。「画面（新規作成）」655 ページ

項番	名称	説明
3		クリックすると以下のメニューが表示されます。 ●全てにチェックを入れる 選択すると、ネットワーク一覧にあるすべてのネットワーク設定のチェックボックスにチェックが入ります。 ●全てのチェックをはずす 選択すると、ネットワーク一覧にあるすべてのネットワーク設定のチェックボックスのチェックが外れます。 ●検索対象 検索対象をネットワーク名、グローバル IP アドレス、ネットワークアドレス、ローカルネットワーク、備考のいずれかに変更します。 ●フィルター フィルターの対象をグローバルネットワーク、ローカルエリアネットワーク、全てのいずれかに変更します。 ●並べ替え 昇順 ネットワーク一覧をネットワーク名、グローバル IP アドレス、ネットワークアドレス、検出日時のいずれかで、昇順に並び替えます。 ●並べ替え 降順 ネットワーク一覧をネットワーク名、グローバル IP アドレス、ネットワークアドレス、検出日時のいずれかで、降順に並び替えます。 ●一括削除 ●ネットワーク一覧でチェックの入っているネットワーク設定を削除します。
4	検索キーワード入力ボックス	検索するキーワードを入力して をクリックすると、ネットワーク一覧からキーワードで絞り込まれたネットワーク設定が表示されます。 検索したあとにすべてのネットワーク設定を再表示するには、ブラウザーを再読み込み、またはボックスを空欄にして再度 をクリックします。
5	ネットワーク一覧	保存されているネットワーク設定の一覧が表示されます。
6	管理情報	●グローバルネットワーク名 グローバルネットワークの名称が表示されます。 ●管理外機器の検出 管理外機器を検出してマップに表示する、管理外機器の検出の設定内容が表示されます。 ●管理外機器のアラート 管理外機器をマップ上で赤く表示する、管理外機器のアラートの設定内容が表示されます。 ●備考 備考欄です。 管理情報の設定内容については、以下を参照してください。 「画面（新規作成）」655 ページ
7	グローバル IP アドレス	●グローバル IP アドレス グローバル IP アドレスが表示されます。 ●検出日時 検出日時が表示されます。

項番	名称	説明
8	ローカルネットワーク	●デフォルトゲートウェイの MAC アドレス デフォルトゲートウェイの MAC アドレスを入力します。 ＋をクリックして 300 件まで登録できます。

◆画面（新規作成）

表示操作［**サイトマップ**］→［**ネットワーク**］→ ＋ （**一覧から対象を選択**→［**編集**］）

項番	名称	説明
1	グローバルネットワーク名	グローバルネットワークの名称を 1 文字から 30 文字以内で入力します。
2	管理外機器の検出	管理外機器検出の有効または無効を設定します。 ●有効 管理外機器を検出し、マップに表示します。 「有効」に設定してもネットワーク内に Windows エージェントが入っている機器がない場合、管理外機器の検出は行えません。 ●無効 管理外機器の検出はせず、マップにも表示しません。
3	管理外機器のアラート	管理外機器アラートの有効または無効を設定します。 ●有効 管理外機器をマップ上で赤く表示します。 ●無効 管理外機器をマップ上で赤く表示することはなく、その他の機器と同様に表示します。
4	備考	備考があれば 255 文字以内で入力します。

◆エラー一覧

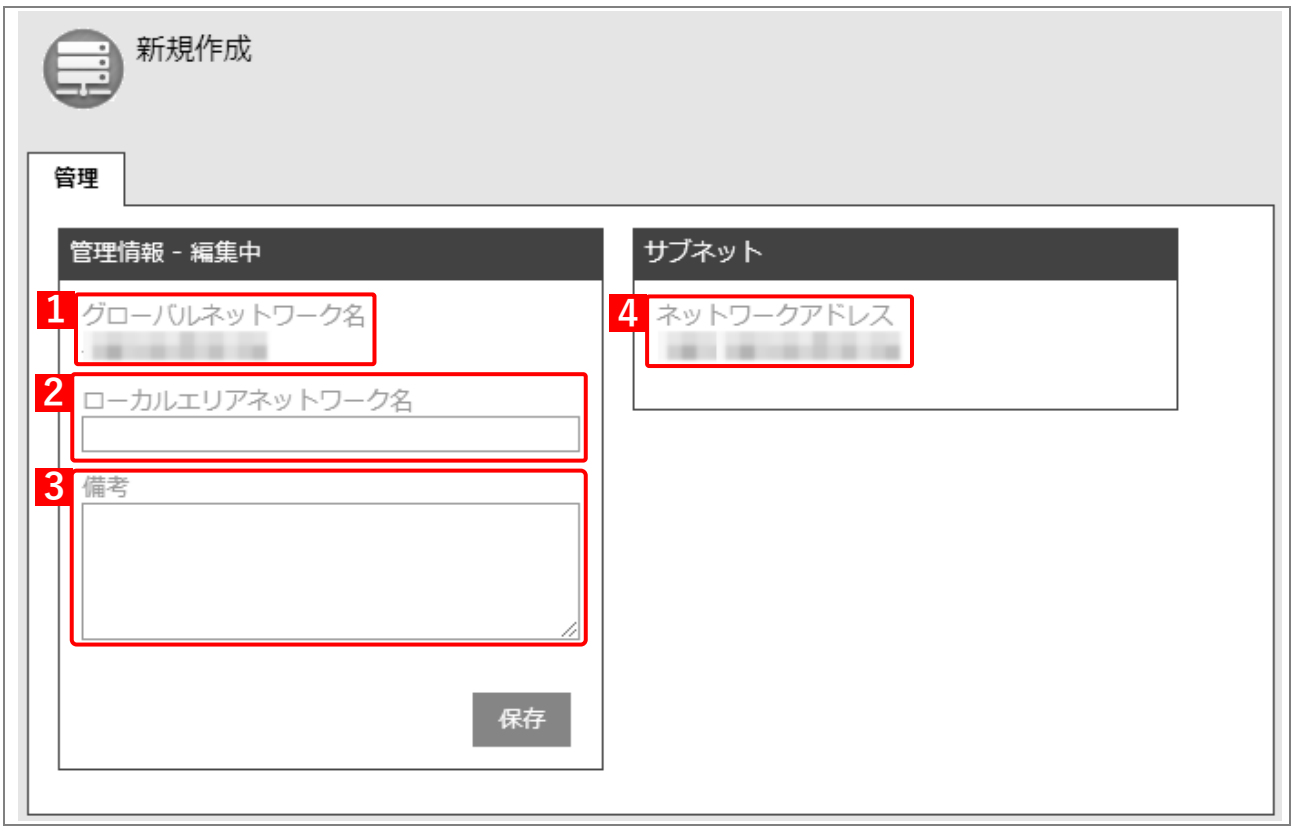
文言	発生契機	対処方法
⚠ 配下の管理ネットワークが存在するため削除できません。	削除しようとしているネットワークの配下にローカルネットワークが存在している。	削除したいネットワークの配下にあるすべてのローカルネットワークを先に削除してください。
⚠ 配下の管理ネットワークが存在するため一括削除できません。	一括削除対象のネットワークのうち、配下にローカルネットワークが存在するネットワークが含まれている。	一括削除対象のネットワーク配下にローカルネットワークが存在しないように、先に削除してください。

◆画面（ローカルネットワークの編集）

ローカルエリアネットワークを編集します。

ローカルエリアネットワークの新規作成はできません。編集のみ行えます。

表示操作　［サイトマップ］→［ネットワーク］→一覧から対象を選択→［編集］



項番	名称	説明
1	グローバルネットワーク名	グローバルネットワークの名称が表示されます。このグローバルネットワーク名を変更する場合は、該当の「グローバルネットワーク」をネットワーク一覧から選択して編集します。
2	ローカルエリアネットワーク名	ローカルエリアネットワークの名称を 1 文字から 30 文字以内で入力してください。
3	備考	備考を 255 文字以内で入力してください。
4	ネットワークアドレス	ローカルエリアネットワークのネットワークアドレスが表示されます。

◆エラー一覧

文言	発生契機	対処方法
⚠ ネットワークアドレスは既存のネットワークアドレスと重複しないものを入力してください。	登録しようとしたネットワークアドレスの情報が、すでに管理サイト上に存在している。	すでに管理サイト上に存在しているネットワークアドレスとは重複しない情報を入力し、登録してください。

12.4 Android エージェント個別管理

Android エージェントに、Push 通知に関する設定を行うための設定セットを作成します。

本機能では、Push 通知の利用や停止、Wi-Fi 接続時のみ利用を停止するなどの設定を行うことができます。

エージェント個別管理が未設定の場合は、Push 通知を［利用する］に設定した場合と同じ動作になります。

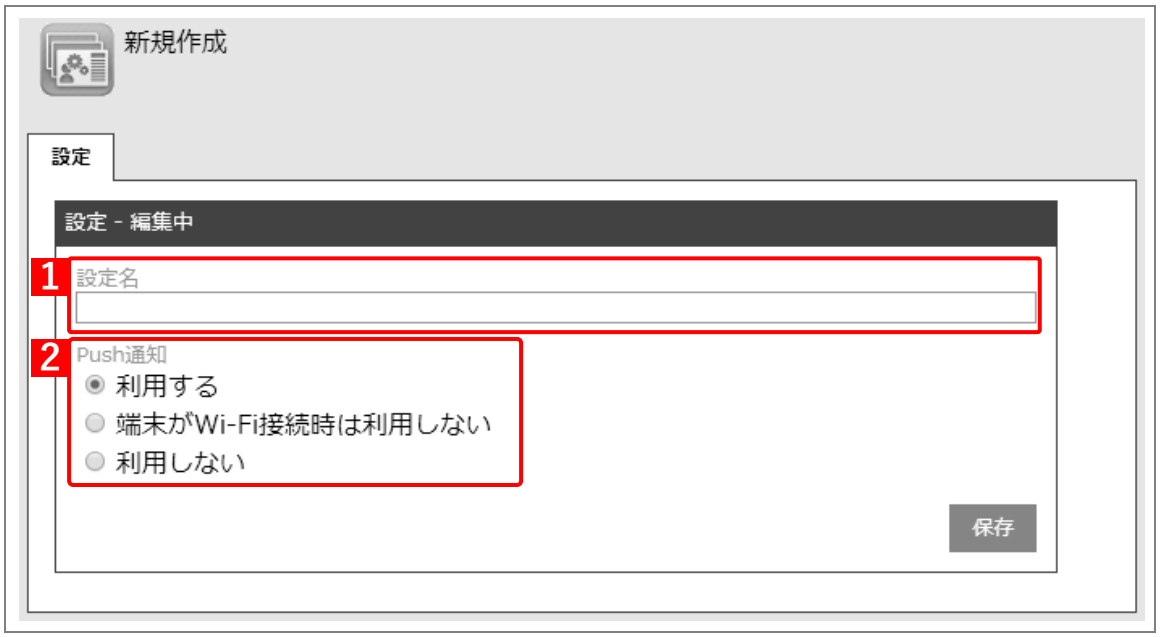
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

◆画面

表示操作［サイトマップ］→「Android」の［エージェント個別管理］→ ＋ または［編集］



項番	名称	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で入力します。
2	Push 通知	Push 通知の利用可否を指定します。 ●利用する ●端末が Wi-Fi 接続時は利用しない Push 通知を利用します。ただし、Wi-Fi 接続時は利用しません。 ●利用しない

12.5 Android リモートロック

対象の Android 端末をリモートロックするための設定セットを作成します。

リモートロックの設定セットを割り当てておくと、同期するたびに端末がロックされるため、定期的にリモートロックを行いたい場合に有効です。

リモートロックを行うと本製品独自のロック画面が表示され、端末を操作できなくなります。また、ロック画面に表示させるメッセージや、警告音の有無なども設定できます。

リモートロックの解除は、「リモートロック」項目で［ロックしない］を選択した設定セットを作成し、端末に同期します。

「ロック解除」機能で、本リモートロックを解除することもできます。ただし、「リモートロック」機能で端末をロックしている場合は、本機能で［ロックしない］を選択した設定セットを作成し、端末に同期しても、ロックは解除されません。「ロック解除」機能については、以下を参照してください。

「（操作－Android）ロック解除」113 ページ

「リモートロック」機能で端末をロックすることもできます。ただし、本機能よりも「リモートロック」機能が優先されるため、「リモートロック」機能で端末がロックされている場合に本機能でロックを行っても、本機能のロック内容は端末に反映されません。また、本機能でロック中に「リモートロック」機能のロックが行われた場合は、「リモートロック」機能のロック内容に変更されます。「リモートロック」機能については、以下を参照してください。

「（操作－Android）リモートロック」110 ページ

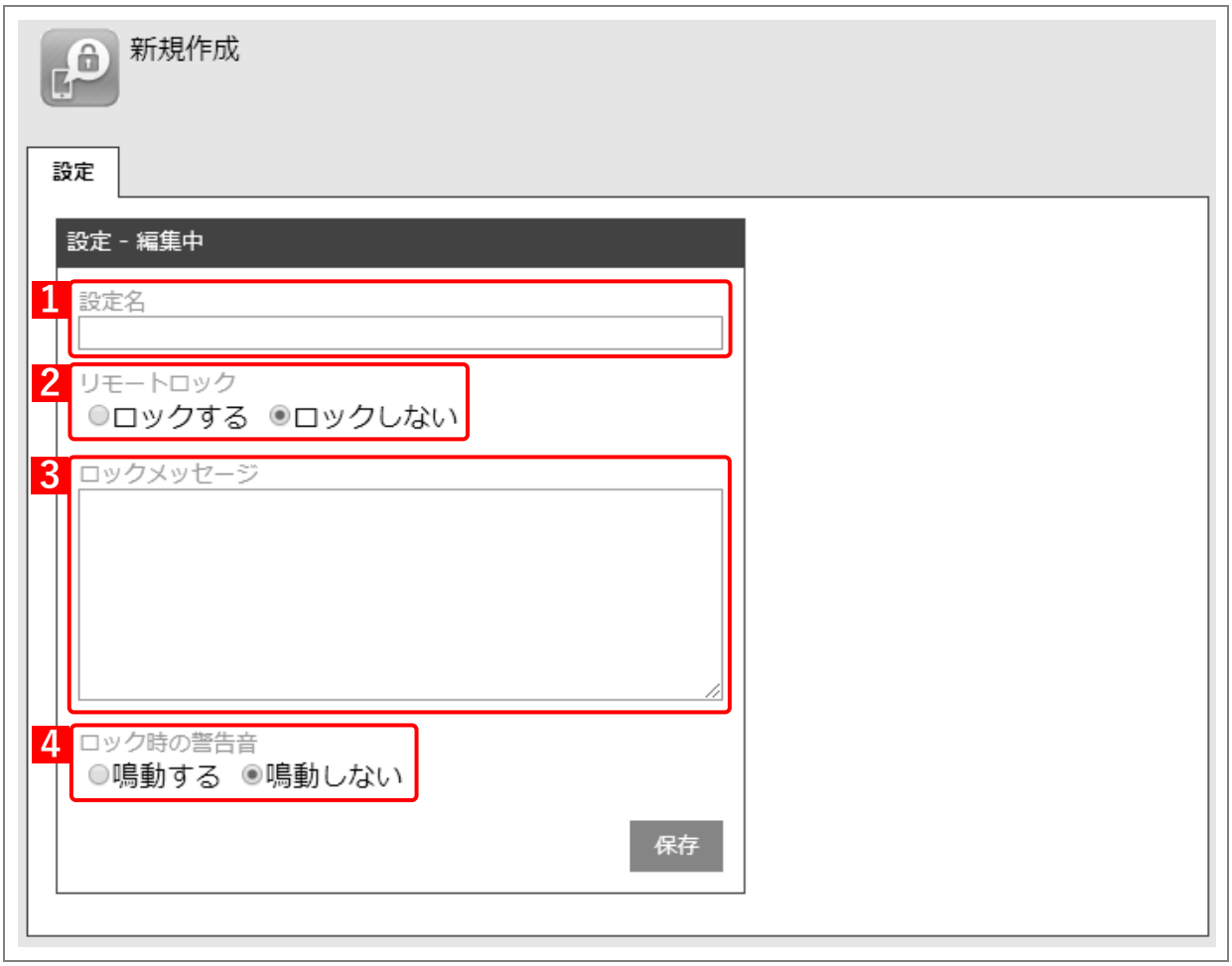
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

◆画面

表示操作　［サイトマップ］→「Android – 使用制限」の［リモートロック］→ ＋（一覧から対象を選択→［編集］）



項番	名称	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	リモートロック	端末のリモートロック設定を行います。 Android 5.0～6.0 の場合、Device Owner Mode 化せずにマルチユーザー機能を使用している端末では、本機能を利用できません。 ●ロックする 端末のリモートロック設定を有効設定します。 ●ロックしない 端末のリモートロック設定を無効または解除設定します。
3	ロックメッセージ	端末のリモートロック設定時に端末に表示させるメッセージを 200 文字以内で設定します。空白類（タブ、改行など）は入力できます。

項番	名称	説明
4	ロック時の警告音	リモートロックした端末から警告音を鳴らすかどうかを、以下から選択します。 本機能は Android 4.0 以上に対応しています。 ●鳴動する リモートロックされた端末で、警告音を鳴らします。 ロック画面が表示されている間、警告音として端末に設定されている通知音が最大音量で鳴り続けます。本設定にする場合は、十分に注意してください。 イヤホン利用時の動作は機種によって異なります。 ハードウェアスイッチによりサイレントモードになっている端末は鳴動しませんのでご注意ください。 ●鳴動しない リモートロックされた端末で、警告音を鳴らしません。

12.6 Android リモートワイプ

対象の Android 端末にリモートワイプを行うための設定セットを作成します。

本機能を実行すると対象の端末が初期化されます。

本機能を実行すると操作を取り消すことはできません。十分に注意してください。

リモートワイプで端末を初期化した場合、端末の OS は初期化したときと同じバージョンになります。ただし、アップデートの方法や仕様により、初期化する直前の OS バージョンにならない場合もあります。

同期タイミングのたびにリモートワイプが指示されるため、リモートワイプを行ったあとは、［設定割り当て］の［リモートワイプ］から設定セットを外してください。

「（設定－Android）設定の割り当て」75 ページ

「リモートワイプ」機能でリモートワイプを行うこともできます。「リモートワイプ」機能については、以下を参照してください。

「（操作－Android）リモートワイプ」114 ページ

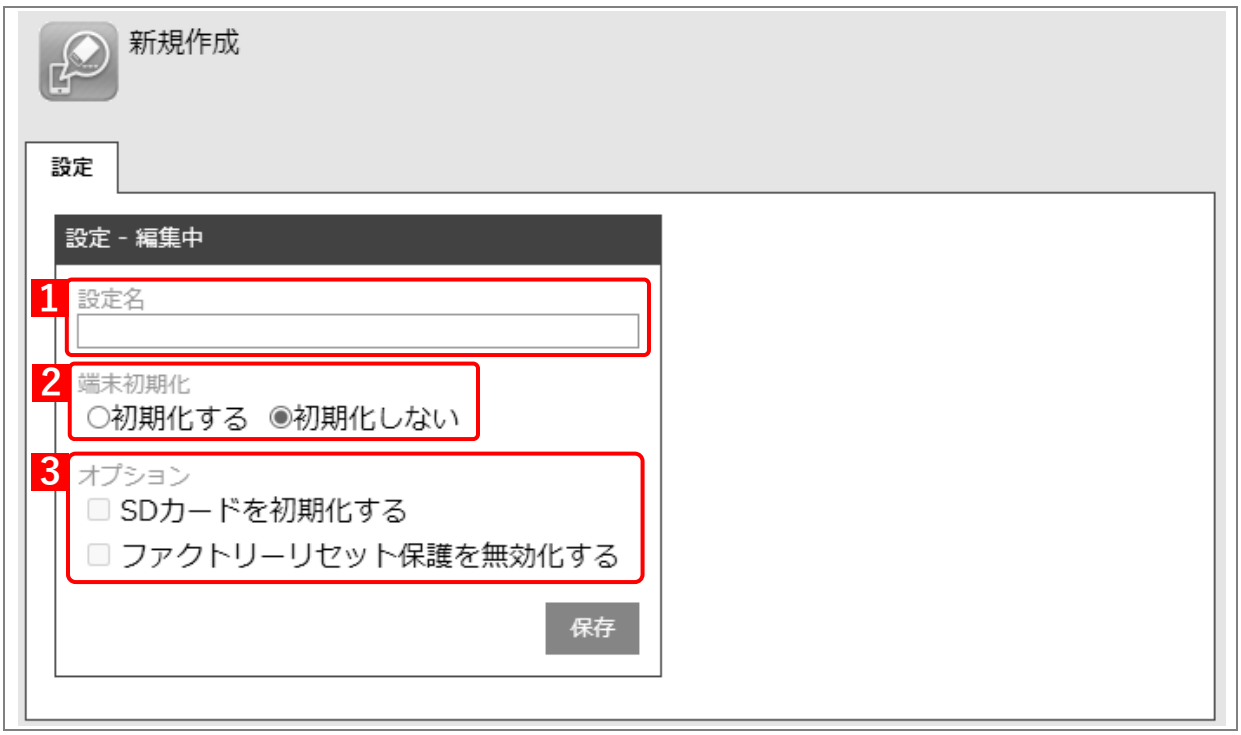
作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Android）設定の割り当て」75 ページ

「全機器一括設定」200 ページ

◆画面

表示操作［サイトマップ］→「Android － 使用制限」の［リモートワイプ］→ ＋ （一覧から対象を選択→［編集］）



項番	名称	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	端末初期化	端末のリモートワイプ設定を行います。 ●初期化する チェックを入れることで端末を初期化する設定とします。 ●初期化しない チェックを入れることで端末を初期化しない設定とします。
3	オプション	●SD カードを初期化する チェックを入れることで端末の初期化時に SD カードも初期化を行います。 ●ファクトリーリセット保護を無効化する チェックを入れることでファクトリーリセット保護を無効化にします。 ファクトリーリセット保護とは、Android 端末を初期化したとき、Google アカウントの認証が必要になることで、キッティングが完了できないようにする機能です。Android 端末の盗難防止になります。

12.7 Windows エージェント個別管理

Windows エージェントに、管理外機器の検出に関する設定を行うための設定セットを作成します。

本機能では、管理外機器の検出機能を有効、または無効に設定することができます。

作成した設定セットは、端末ごと、または全端末に一括で割り当てることで、端末に反映されます。

「（設定－Windows）設定セットの割り当て」103 ページ

「全機器一括設定」200 ページ

設定セットは、最大 50 件まで作成できます。

◆画面

表示操作［**サイトマップ**］→「**Windows**」の［**エージェント個別管理**］→ ＋（**一覧から対象を選択→**［**編集**］）

項番	名称	説明
1	設定名	設定セットの名称を 1 文字から 30 文字以内で指定します。
2	管理外機器の検出	管理外機器の検出の利用可否を以下の項目から指定します。 ●有効 ●無効