KDDI Smart Mobile Safety Manager
iOS クライアント
リファレンスマニュアル

最終更新日　2025 年 4 月 17 日

Document ver1.18

（Web サイト ver.9.21.2）

変更履歴

日付	ver	変更箇所	変更内容
2018/12/13	1.0		新規作成
2019/3/26	1.1	7 削除防止構成プロファイルのインストール	「配信された構成プロファイルのインストール」から「削除防止構成プロファイルのインストール」に見出し名を変更 「iOS12.2 未満の場合」と「iOS12.2 以上の場合」の手順の詳細を追加
2019/4/25	1.2	16 ＋browser Safety Manager の使用	プライバシーポリシーについて追加
		17 Safety Manager App Catalog の使用	説明の追加
2019/12/5	1.3	1.2 OS サポートポリシー	サポート対象を最新に更新
		1.3 動作環境	対象 OS を変更
2020/6/18	1.4	全体	iOS 機器を iOS 端末に統一
		はじめに	注記追加
		1.3 動作環境	対応機種を追加 注記追加
2020/11/11	1.5	1.2 OS サポートポリシー	サポート対象を最新に更新
		1.3 動作環境	対応機種を最新に変更 対象 OS を変更
		1.5 ＋ browser Safety Manager 動作環境	対象 OS を変更
		1.6 Safety Manager App Catalog 動作環境	対象 OS を変更
2021/2/21	1.6		対応機種を最新に変更
		8 「App とブック」の割り当て	VPP を「App とブック」に名称変更
		12 エージェントからのポータル表示	セクション追加
		17.1 Safety Manager App Catalog をインストールする	データの取り扱い画面を追加
2021/7/25	1.7	6.1 配信されたアプリケーション	構成プロファイルの設定名を修正
		1.3 動作環境	ネットワーク接続を追加
		17.1 Safety Manager App Catalog をインストールする	配信でのインストール手順を追加 認証画面を追加
		16.1 ＋browser Safety Manager をインストールする	配信でのインストール手順を追加
		17.7.3 強制アップデートする	セクション追加
2021/10/22	1.8	1.2 OS サポートポリシー	サポート対象を最新に更新
		1.3 動作環境	対応機種を最新に変更 対象 OS を変更
		7.1.2 iOS12.2 以上の場合	iOS 15 対応（画像差し替え、注記追加）
		19.1 エージェントをアンインストール	iOS 15 対応（画像差し替え、注記追加）

日付	ver	変更箇所	変更内容
2022/2/20	1.9	1.3 動作環境	ネットワーク接続に注記追加 対応機種を最新に変更
		18.1 MDM 構成プロファイルをアンインストール	iOS 15 対応（画像差し替え、注記追加）
		18 MDM 構成プロファイルのアンインストール	削除防止についての注意追加
		17.7.1 非管理対象のアプリをアップデートする	見出し、説明を非管理対象のアプリに修正
		17.7.2 管理対象のアプリをアップデートする	見出し、説明を管理対象のアプリに修正
		18 プロファイルのアンインストール	セクション削除
2022/6/12	1.10	全体	OS バージョンに関連する以降を以上に修正
		1.3 動作環境	対応機種を修正、追加
2022/7/24	1.11	1.3 動作環境	対応機種を最新に変更
2022/11/20	1.12	はじめに	全体的に修正
		全体	リード文修正
		1.3 動作環境	対応機種、対応 OS を最新に変更
		6.1 配信されたアプリケーションをインストールする	「Apple Configurator 2 および iTunes からの App のインストールを許可」を「App のインストールを許可」に修正
		14.1 紛失モード画面の表示内容	表を追加
2023/3/26	1.13	1.3 動作環境	対応機種を最新に変更
		1.5 ＋browser Safety Manager 動作環境	対応 OS を最新に変更
		1.6 Safety Manager App Catalog 動作環境	
2023/8/6	1.14	全体	目次の構成変更 構成変更に伴う参照先の修正
		3.1 ユーザー情報を登録する	セクション追加
		3.2 機器情報を登録する	手順、画面の変更
		3.3 iOS 端末から管理サイトに同期する	
		はじめに	名称・呼称、用語集を追加 商標登録修正
2023/8/21	1.15	6.1.2.1 アプリケーション配信機能でインストールする	プライバシーポリシーの画面を最新に差し替え
		6.1.2.2 App Store からインストールする	
2024/1/14	1.16	全体	規約に従い、表記揺れなど統一
		6.2.6 Safety Manager App Catalog からアプリをインストールする	手順を変更
		1.2 OS サポートポリシー	サポート対象変更
		1.3 動作環境	ネットワーク接続の注記を削除、対象 OS 変更
		6.1.1 ＋browser Safety Manager の動作環境	対象 OS 変更

日付	ver	変更箇所	変更内容
		6.2.1 Safety Manager App Catalog の動作環境	
2024/7/21	1.17	1.3 動作環境	対応機種を追加
2024/10/28	1.18	6.2.2.3 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	セクション追加
		6.2.2 Safety Manager App Catalog をインストールする	上記のセクション追加に伴い、リード文、注記の変更
		1.3 動作環境	対応機種追加
		1.2 OS サポートポリシー	対象 OS 変更
		1.3 動作環境	
		6.1.1 ＋browser Safety Manager の動作環境	
		6.2.1 Safety Manager App Catalog の動作環境	

はじめに

本マニュアルでは、KDDI Smart Mobile Safety Manager（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うえ、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

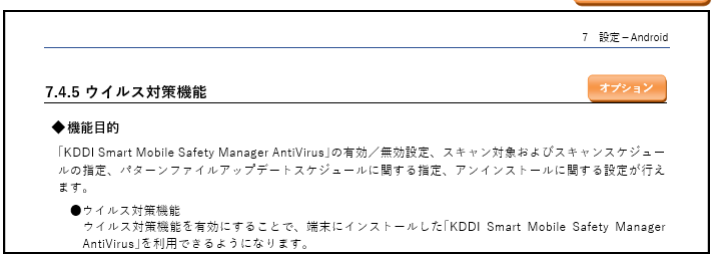
不明な用語は、以下を参照してください。

☞『よくあるご質問（FAQ）』

オプション機能

オプション機能は、オプション契約をした場合に使用できる機能です。

本マニュアルでは、オプション機能の説明の見出しに オプション（オプションマーク）を表示しています。



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。

商標登録

●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 iOS クライアントについて
2 MDM 構成プロファイル
3 ポータルの使用方法
4 エージェントの使用方法
5 管理サイトからの指示による動作
6 関連アプリの使用方法

1 iOS クライアントについて 9
1.1 概要 10
1.2 OS サポートポリシー 12
1.3 動作環境 12
1.4 iOS のソフトウェアアップデートについて 14

2 MDM 構成プロファイルについて 15
2.1 管理対象としてインストールされているアプリを確認する 16
2.2 構成プロファイルの機能制限を確認する 19
2.3 MDM 構成プロファイルをアンインストールする 21

3 ポータルの使用方法 24
3.1 ユーザー情報を登録する 25
3.2 機器情報を登録する 27
3.3 iOS 端末から管理サイトに同期する 29
3.4 配信されたアプリをインストールする 31
3.5 削除防止構成プロファイルをインストールする 33
3.5.1 iOS 12.2 未満の場合 33
3.5.2 iOS 12.2 以上の場合 37

4 エージェントの使用方法 41
4.1 エージェントを起動する 42
4.2 エージェントの基本情報を確認する 43
4.3 メッセージ 44
4.3.1 メッセージを確認する 44
4.3.1.1 iPhone の場合 44
4.3.1.2 iPad の場合 45
4.3.2 未開封メッセージを確認する 47
4.3.2.1 エージェントが起動中の場合 47
4.3.2.2 エージェントが起動していない場合 48
4.4 エージェントからポータルを表示する 49
4.5 エージェントのバージョン情報を確認する 50
4.6 エージェントをアンインストールする 51

5 管理サイトからの指示による動作 52
5.1 リモートロック画面の表示内容 53
5.2 紛失モード画面の表示内容 54
5.2.1 紛失モード中の表示 54
5.2.2 紛失モード解除後の表示 55
5.3 「App とブック」の利用規約に同意する 56

6 関連アプリの使用方法 58
6.1 ＋browser Safety Manager 59
6.1.1 ＋browser Safety Manager の動作環境 59
6.1.2 ＋browser Safety Manager をインストールする 60
6.1.2.1 アプリケーション配信機能でインストールする 60
6.1.2.2 App Store からインストールする 63
6.1.3 メイン画面 65
6.1.4 設定画面 66
6.1.5 ＋browser Safety Manager をアンインストールする 67
6.2 Safety Manager App Catalog 68
6.2.1 Safety Manager App Catalog の動作環境 68
6.2.2 Safety Manager App Catalog をインストールする 69
6.2.2.1 アプリケーション配信機能でインストールする 69
6.2.2.2 App Store からインストールする 72
6.2.2.3 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 74
6.2.3 メイン画面 83
6.2.4 グループ詳細画面 84
6.2.5 全体検索を行う 85
6.2.6 Safety Manager App Catalog からアプリをインストールする 86
6.2.7 Safety Manager App Catalog からアプリを更新する 87
6.2.7.1 非管理対象のアプリをアップデートする 87
6.2.7.2 管理対象のアプリをアップデートする 88
6.2.7.3 強制アップデートする 89
6.2.8 Safety Manager App Catalog をアンインストールする 91

1 iOS クライアントについて

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。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）ができます。iOS 端末にアプリ「KDDI Smart Mobile Safety Manager エージェント（以下、エージェントを呼ぶ）」をインストールすることもできます。

管理サイトの操作については、以下を参照してください。

『管理サイト リファレンスマニュアル』

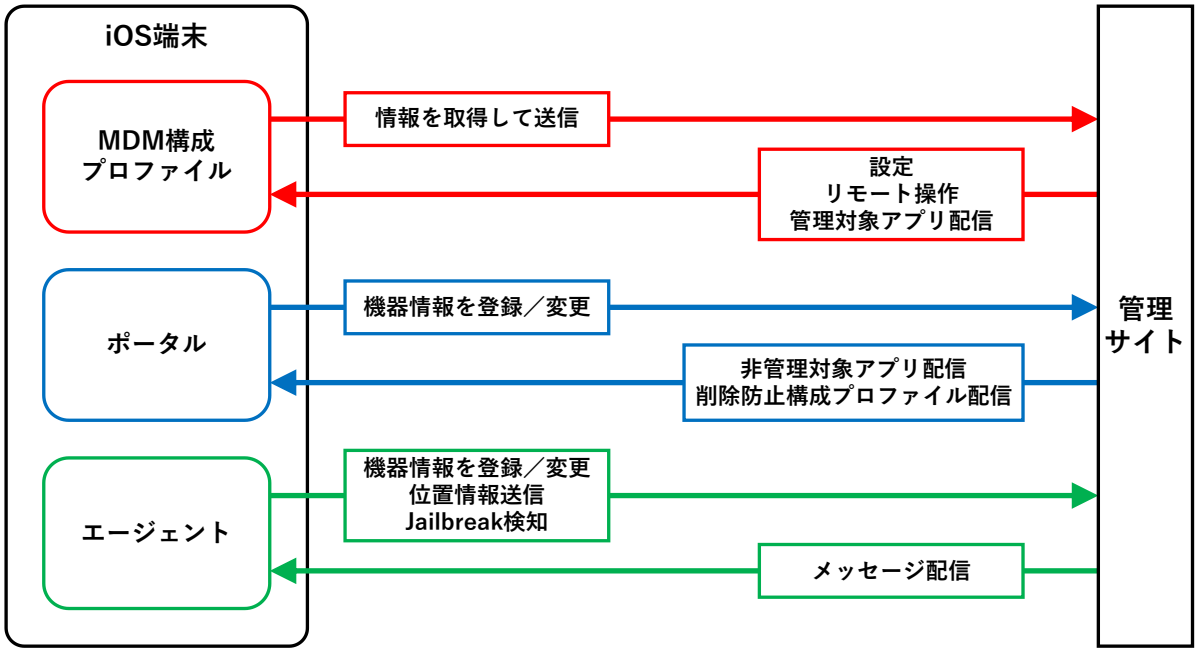
Apple の提供する「Automated Device Enrollment（ADE）」を利用した機器管理の詳細は、以下を参照してください。

『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順）』

『Apple School Manager（ASM）マニュアル（利用方法・年次更新手順）』

本製品で行えること

本製品は、MDM 構成プロファイル、ポータル、エージェントを利用して、iOS 端末を管理します。



◆MDM 構成プロファイル

MDM 構成プロファイルとは、iOS 端末の構成を制御するプロファイルです。

本製品を利用するには、MDM 構成プロファイルのライセンスを認証する必要があります。以下を参照して、MDM 構成プロファイルのライセンスを認証してください。

『iOS キッティングマニュアル』の「ライセンス認証を行う」／「ADE を利用してライセンス認証を行う」

MDM 構成プロファイルで行えることは、以下のとおりです。

●定期的に iOS 端末の情報を取得して、管理サイトに送信する。

●定期的に管理サイトからの設定を取得して、iOS 端末に設定する。

●管理サイトからリモート操作の指示を受けて、iOS 端末を操作する。

●管理サイトから管理対象アプリが送信される。

MDM 構成プロファイルについては、以下を参照してください。

「MDM 構成プロファイルについて」15 ページ

◆ポータル

ポータルとは、Web クリップです。アイコンをタップするとブラウザーでポータルホーム画面が表示されます。

ポータルのアイコンは、MDM 構成プロファイルのライセンス認証を行うと、iOS 端末のホーム画面に表示されます。管理サイトと同期するたびに、ポータルは再インストールされます。

ポータルで行えることは、以下のとおりです。

●機器情報を登録／変更する。

●管理サイトから非管理対象アプリが送信される。

●管理サイトから削除防止構成プロファイルが送信される。

ポータルの使用方法については、以下を参照してください。

「ポータルの使用方法」24 ページ

◆エージェント

エージェントとは、MDM 構成プロファイルのライセンス認証を行ったあと、App Store からインストール／認証して使用するアプリです。iOS 端末のホーム画面にエージェントのアイコンが表示されます。以下を参照して、エージェントのインストール／認証を行ってください。

『iOS キッティングマニュアル』の「エージェントを認証する」

エージェントで行えることは、以下のとおりです。

●機器情報を登録／変更する。

●位置情報を送信する。

●Jailbreak を検知する。

●管理サイトからメッセージが配信される。

エージェントの使用方法は、以下を参照してください。

「エージェントの使用方法」41 ページ

1.2 OS サポートポリシー

本製品では、確実な製品の動作とセキュリティ機能の提供を目的として、以下の OS サポートポリシーを定めています。

●本製品の最新対応 OS より 3 世代前の OS メジャーバージョンまでをサポート。

●最新対応 OS 追加に伴い、サポート対象外となった OS バージョンについては、サポート期限が切れた日から 1 年間に限り、お問い合わせには可能な限り対応いたします。ただし、動作保証や不具合対応はいたしません。

定期的に下位の OS バージョンのサポートを終了します。サポート対象外となる OS や端末を利用している場合は、OS アップデートまたは機種の変更をしてください。

サポート対象
●iOS 18.x：最新対応 OS ●iOS 17.x：1 世代前 ●iOS 16.x：2 世代前 ●iOS 15.x：3 世代前 iOS 14.x のサポートは終了しました。問い合わせには 2025 年 9 月 16 日まで可能な限り対応します。

1.3 動作環境

エージェントのリリース日から 180 日間は、180 日間にリリースされたすべてのエージェントがサポートされます。ただし、リリース日から 180 日を超えた場合は、180 日以降最初にリリースされたエージェントから 2 つ前のエージェントまでが、サポートの対象になります。

エージェントは、日本国内でのみ利用が可能です。

対応機種	iPhone 6s iPhone 6s Plus iPhone 7 iPhone 7 Plus iPhone 8 iPhone 8 Plus iPhone X iPhone XS iPhone XS Max iPhone XR iPhone SE iPhone SE（第 2 世代） iPhone SE（第 3 世代） iPhone 11 iPhone 11 Pro iPhone 11 Pro Max iPhone 12 iPhone 12 mini iPhone 12 Pro iPhone 12 Pro Max iPhone 13 iPhone 13 mini iPhone 13 Pro iPhone 13 Pro Max iPhone 14

	iPhone 14 Plus iPhone 14 Pro iPhone 14 Pro Max iPhone 15 iPhone 15 Plus iPhone 15 Pro iPhone 15 Pro Max iPhone 16 iPhone 16 Plus iPhone 16 Pro iPhone 16 Pro Max iPad（第 5 世代） iPad（第 6 世代） iPad（第 7 世代） iPad（第 8 世代） iPad（第 9 世代） iPad（第 10 世代） iPad mini（第 4 世代） iPad mini（第 5 世代） iPad mini（第 6 世代） iPad Air（第 2 世代） iPad Air（第 3 世代） iPad Air（第 4 世代） iPad Air（第 5 世代） iPad Air（M2）11 インチ iPad Air（M2）13 インチ iPad Pro 9.7 インチ iPad Pro 10.5 インチ iPad Pro 11 インチ（第 1 世代） iPad Pro 11 インチ（第 2 世代） iPad Pro 11 インチ（第 3 世代） iPad Pro 11 インチ（第 4 世代） iPad Pro 12.9 インチ（第 1 世代） iPad Pro 12.9 インチ（第 2 世代） iPad Pro 12.9 インチ（第 3 世代） iPad Pro 12.9 インチ（第 4 世代） iPad Pro 12.9 インチ（第 5 世代） iPad Pro 12.9 インチ（第 6 世代） iPad Pro（M4）11 インチ iPad Pro（M4）13 インチ iPod touch（第 7 世代）
対応 OS	iOS 15.0 以上
ネットワーク接続	モバイルネットワークまたは Wi-Fi でインターネットへアクセスができること。 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）ができること。

1.4 iOS のソフトウェアアップデートについて

iOS 端末でソフトウェアアップデートを行うと、位置情報などの設定が変更される場合があります。

ソフトウェアアップデート終了後は、iOS 端末の設定を確認してください。

2 MDM 構成プロファイルについて

この章では、MDM 構成プロファイルで確認できること、MDM 構成プロファイルのアンインストールについて説明します。

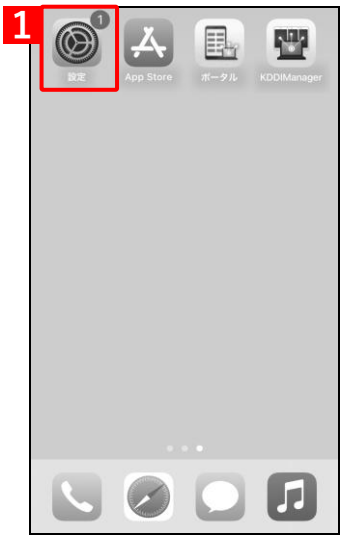
2.1 管理対象としてインストールされているアプリを確認する

「管理対象アプリ」が配信されると、サイレントインストールが行われてアプリが自動的にインストールされます。サイレントインストールされている「管理対象アプリ」の確認手順について説明します。

「管理対象アプリ」については、以下を参照してください。

- 『iOS アプリケーション配信　手順書』の「アプリケーション配信について」―「アプリケーション配信とは」
- 『管理サイト　リファレンスマニュアル』の「設定―iOS」―「アプリケーション」―「アプリケーション配信」

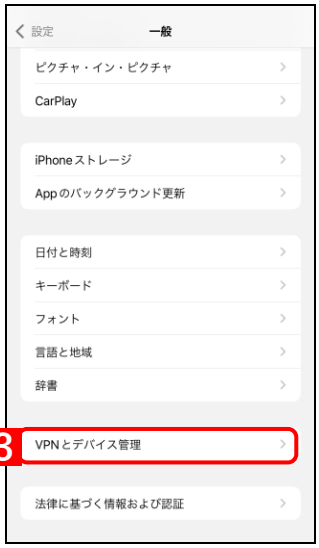
【1】［設定］をタップします。



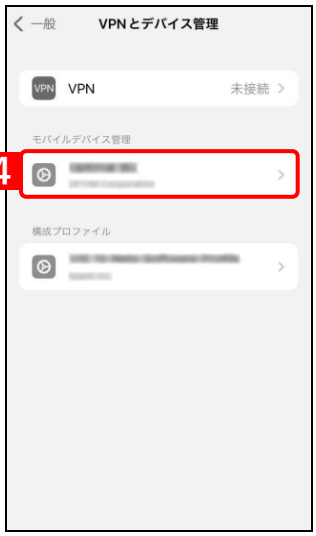
【2】［一般］をタップします。

【3】［VPN とデバイス管理］をタップします。

iOS のバージョンにより［VPN とデバイス管理］は、［プロファイル］や［デバイス管理］など、表記が異なる場合があります。



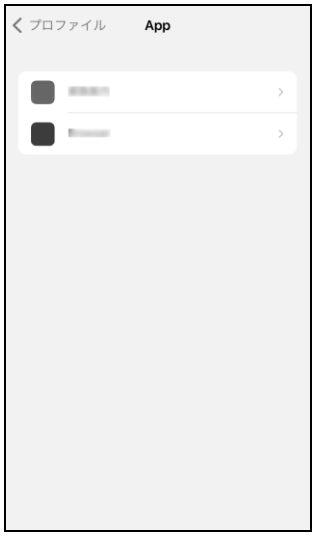
【4】モバイルデバイス管理の［KDDI Smart Mobile Safety Manager］をタップします。



【5】［App］をタップします。

iOS 16.4 以上では、「デバイス ID 証明書」が「SCEP デバイス ID 証明書」と表示されます。

⇒サイレントインストールされている管理対象アプリの一覧が表示されます。



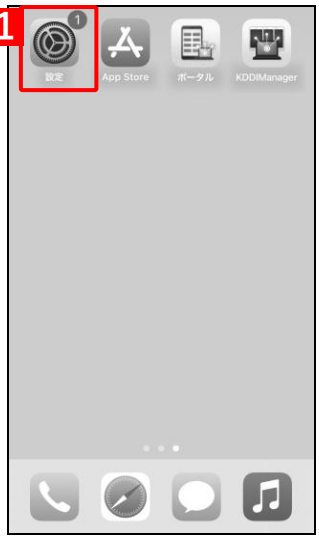
2.2 構成プロファイルの機能制限を確認する

構成プロファイルで適用されている機能制限の確認手順について説明します。

構成プロファイルについては、以下を参照してください。

『管理サイト　リファレンスマニュアル』の「設定―iOS」―「構成プロファイル」

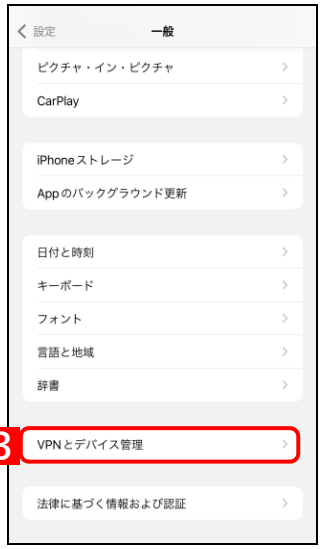
【1】［設定］をタップします。



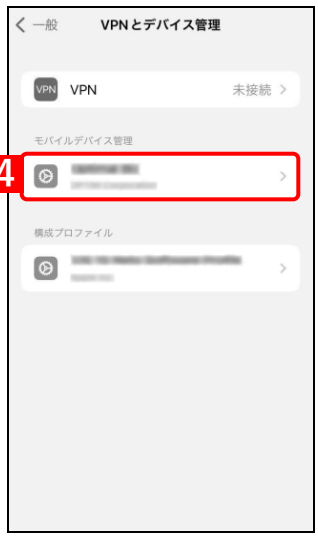
【2】［一般］をタップします。

【3】［VPN とデバイス管理］をタップします。

iOS のバージョンにより［VPN とデバイス管理］は、［プロファイル］や［デバイス管理］など、表記が異なる場合があります。



【4】モバイルデバイス管理の［KDDI Smart Mobile Safety Manager］をタップします。



【5】［機能制限］をタップします。

iOS 16.4 以上では、「デバイス ID 証明書」が「SCEP デバイス ID 証明書」と表示されます。

⇒構成プロファイルの機能制限が表示されます。

2.3 MDM 構成プロファイルをアンインストールする

管理者の指示、または許可をとってからアンインストールしてください。

エージェントを認証している場合は、先にエージェントをアンインストールしてください。

「エージェントをアンインストールする」51 ページ

「削除防止」を適用した端末は、本手順で MDM 構成プロファイルを削除することができません。設定セットを解除しても「削除防止」は解除されません。「削除防止」を適用した端末の MDM 構成プロファイルを削除するには、Apple Configurator2 を利用するか、端末を初期化してください。

MDM 構成プロファイルをアンインストールすると、端末から以下の設定も削除されます。

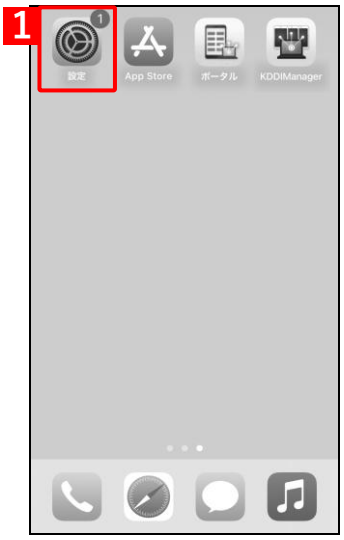
- 「削除防止」を適用していない構成プロファイル
- 管理対象アプリ

構成プロファイル、管理対象アプリについては、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定―iOS」―「構成プロファイル」

『管理サイト リファレンスマニュアル』の「設定―iOS」―「アプリケーション」―「アプリケーション配信」

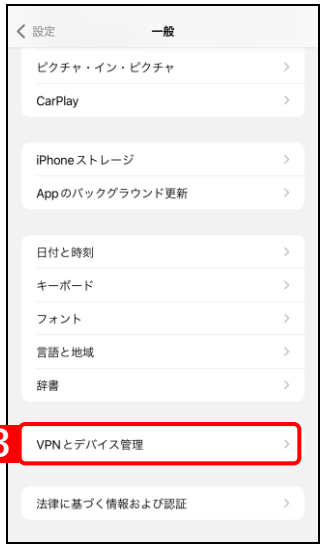
【1】［設定］をタップします。



【2】［一般］をタップします。

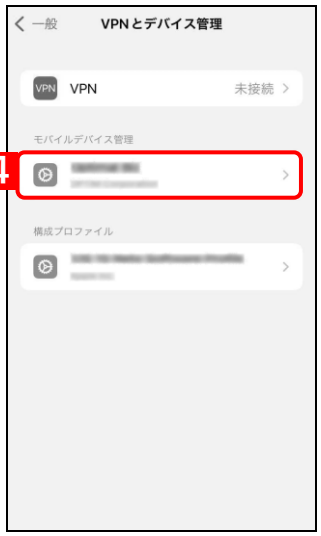
【3】［VPN とデバイス管理］をタップします。

iOS のバージョンにより［VPN とデバイス管理］は、［プロファイル］や［デバイス管理］など、表記が異なる場合があります。



【4】モバイルデバイス管理の［KDDI Smart Mobile Safety Manager］をタップします。

インストールされている MDM 構成プロファイルが 1 つの場合はこの画面は表示されません。



【5】［削除］をタップします。

iOS 16.4 以上では、「デバイス ID 証明書」が「SCEP デバイス ID 証明書」と表示されます。

【6】［削除］をタップします。

端末にパスコードが設定されている場合は、パスコード入力画面が表示されますのでパスコードを入力してください。

3 ポータルの使用方法

この章では、ポータルの使用方法について説明します。

注意

●管理サイトで、iOS ポータルを表示に設定してください。

『管理サイト リファレンスマニュアル』の「サービス環境設定」―「ポータル表示」

●共有 iPad（Shared iPad）では、ポータルアイコンは表示されません。

3.1 ユーザー情報を登録する

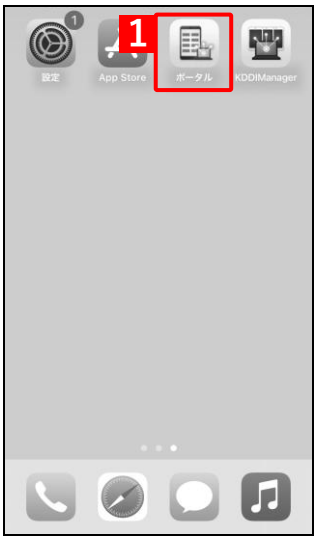
以下の場合は、ユーザー情報の登録を行ってください。

●ライセンスを認証したときに、ユーザー情報の登録を行わなかった場合

●設定しているユーザー情報を変更したい場合

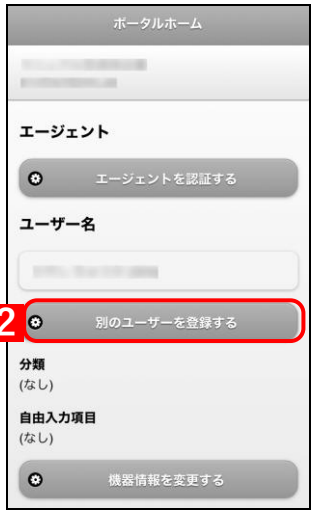
ベーシックパックプラスを利用している場合、ポータルからユーザーの登録および変更は行えません。

【1】［ポータル］をタップします。



【2】［別のユーザーを登録する］をタップします。

ライセンスを認証したときに、ユーザー情報の登録を行わなかった場合は、［ユーザーを登録する］と表示されます。



【3】社員番号、姓、名を入力します。

【4】［登録する］をタップします。

⇒ユーザー情報の登録が完了します。

【5】［OK］をタップします

ブラウザーを閉じてください。

3.2 機器情報を登録する

以下の場合は、機器情報の登録を行ってください。

●ライセンスを認証したときに、機器情報の登録を行わなかった場合

●設定している機器情報を変更したい場合

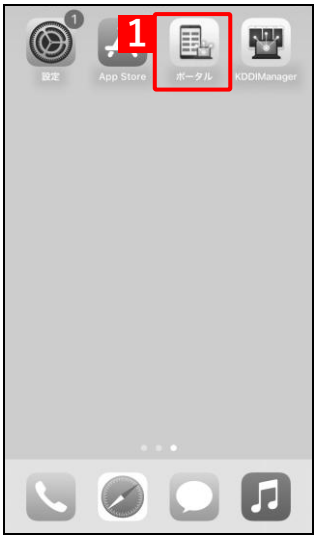
管理サイトの［入力項目のカスタマイズ］で入力項目の追加を行うと、「機器情報登録」画面に表示され、リストからの選択や直接入力で、端末情報の登録や変更を行うことができます。

あらかじめ、管理サイトの［入力項目のカスタマイズ］で入力項目を追加してください。追加するとき、「機器から入力可」にチェックを入れてください。チェックが入っていない場合は、項目が表示されません。

『管理サイト リファレンスマニュアル』の「機器」―「入力項目のカスタマイズ」

管理サイトの［入力項目のカスタマイズ］で設定した内容により、画面に表示される「分類」と「自由入力項目」の内容が異なります。

【1】［ポータル］をタップします。



【2】［機器情報を変更する］をタップします。

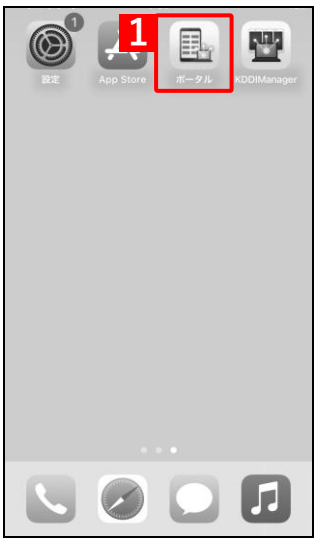
【3】必要事項を選択、入力します。
【4】［登録する］をタップします。
⇒機器情報の登録が完了します。

【5】［OK］をタップします。
ブラウザーを閉じてください。

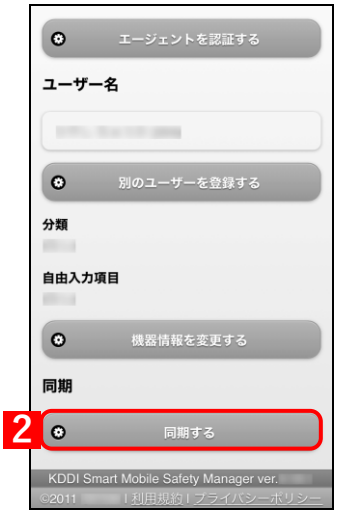
3.3 iOS 端末から管理サイトに同期する

管理サイトとの同期は定期的に行われますが、定期同期を待たずに自由なタイミングで同期することができます。情報や設定の更新を定期同期にかかわらず、行うことができます。

【1】［ポータル］をタップします。



【2】［同期する］をタップします。



【3】［同期する］をタップします。

⇒管理サイトと同期します。

【4】［OK］をタップします。

ブラウザーを閉じてください。

3.4 配信されたアプリをインストールする

管理サイトから配信されたアプリのインストール手順について説明します。配信されたアプリは管理状態によってインストール手順が異なります。「管理対象アプリ」が配信された場合は、サイレントインストールが行われてアプリが自動的にインストールされるため、端末の操作を行う必要はありません。「非管理対象アプリ」が配信された場合は、本操作を行い、アプリをインストールします。

「管理対象アプリ」、「非管理対象アプリ」については、以下を参照してください。

『iOS アプリケーション配信　手順書』の「アプリケーション配信について」―「アプリケーション配信とは」

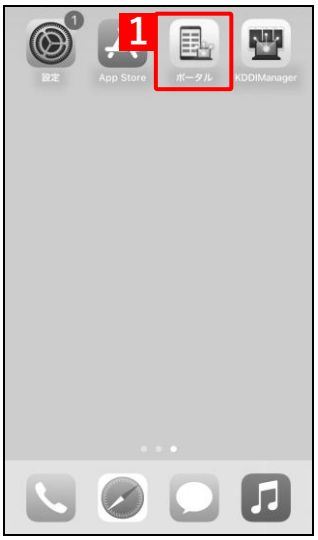
『管理サイト　リファレンスマニュアル』の「設定―iOS」―「アプリケーション」―「アプリケーション配信」

省データモードを設定している iOS 13.1 以上の端末に「管理対象アプリ」を配信した場合は、サイレントインストールは行われず、ホーム画面上にグレーアウトした「待機中」アイコンが表示されます。アイコンをタップしてインストールを行ってください。

アプリケーション配信については、以下を参照してください。

『iOS アプリケーション配信　手順書』

【1】［ポータル］をタップします。

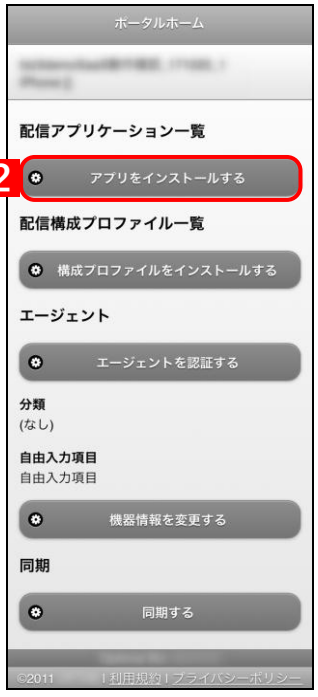


【2】［アプリをインストールする］をタップします。

管理サイトからアプリが 1 つも配信されていない場合、［アプリをインストールする］は表示されません。

アプリケーション配信の設定は、以下を参照してください。

『管理サイト　リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」



【3】インストールしたいアプリの［インストール］をタップします。

- オリジナルアプリの［インストール］をタップした場合、インストール確認メッセージが表示されますので、許可をしてください。インストールが開始されます。
- App Store アプリの［インストール］をタップした場合、App Store に接続されます。手順に従ってインストールを行ってください。
- iOS 10 以上は、Apple の仕様変更により、構成プロファイルの以下の設定が端末に適用されている場合、オリジナルアプリについてポータルからのインストールができなくなりました。

  「App Store からの App のインストールを許可(監視対象のみ)」を制限した場合
  ⇒iOS 10.0.0 以上でインストールできなくなりました。
  「App のインストールを許可」を制限した場合
  ⇒iOS 10.0.1 以上でインストールできなくなりました。

  回避方法としては、管理サイトから管理対象として配信を行ってください。管理対象としてのアプリケーション配信の設定については、以下を参照してください。

  『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」

3.5 削除防止構成プロファイルをインストールする

iOS 12.2 未満／以上で操作が異なります。端末で使用している iOS のバージョンに応じて、どちらかの方法を選択してください。

●iOS 12.2 未満の場合

●iOS 12.2 以上の場合

管理サイトから Web クリップが配信された場合は、管理サイトで指定したアイコンが Web クリップとして表示され、Web クリップへのブックマーカーが設定されます。ただし、Web ページによっては、ページ内で指定されているアイコンが強制的に適用される場合があります。また、Web クリップで配信された設定は、iOS 端末の操作では削除できません。Web クリップの設定については、以下を参照してください

『管理サイト リファレンスマニュアル』の「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▼] タブ／Web クリップ設定」

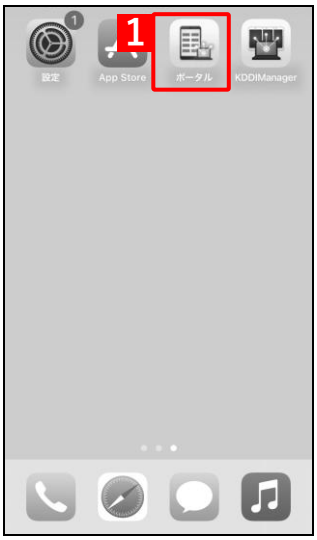
削除防止を設定した構成プロファイルをインストールした iOS 端末は、MDM 構成プロファイルを削除することができなくなります。

構成プロファイルについては、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定―iOS」―「構成プロファイル」

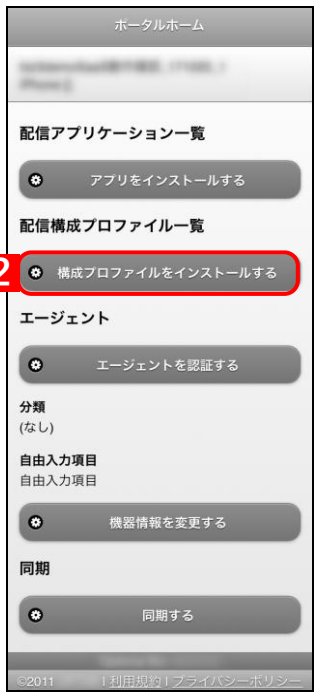
3.5.1 iOS 12.2 未満の場合

【1】［ポータル］をタップします。



【2】［構成プロファイルをインストールする］をタップします。

管理サイトから構成プロファイルが 1 つも配信されていない場合、［構成プロファイルをインストールする］は表示されません。



【3】インストールしたい構成プロファイルの［インストール］をタップし、構成プロファイルのインストールを行います。

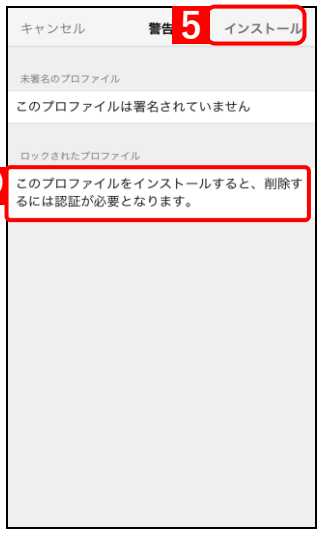
【4】［インストール］をタップします。

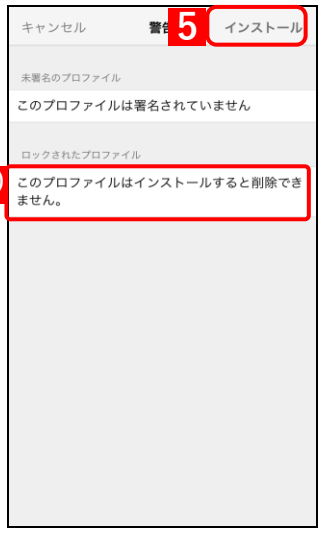
【5】［インストール］をタップします。

警告メッセージは、管理サイトの構成プロファイルの設定により（A）または（B）が表示されます。メッセージを確認のうえ、［インストール］をタップしてください。

構成プロファイルの設定の詳細は、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「構成プロファイル」－「構成プロファイル」



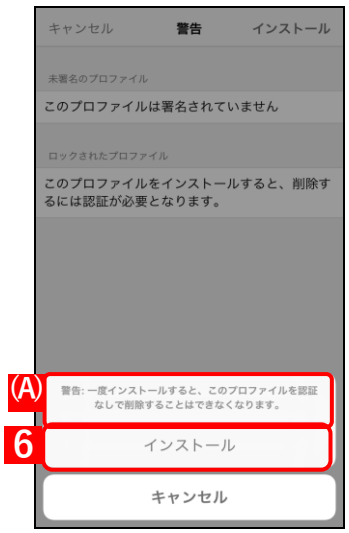


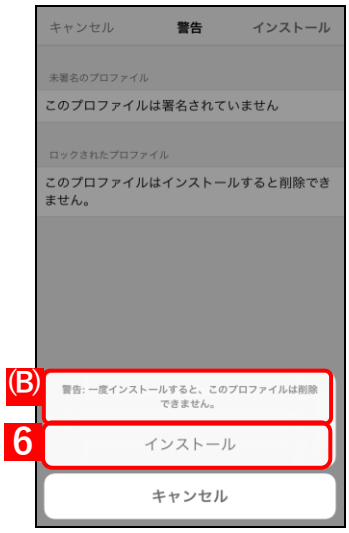
【6】［インストール］をタップします。

確認メッセージは、管理サイトの構成プロファイルの設定により（A）または（B）が表示されます。メッセージを確認のうえ、［インストール］をタップしてください。

構成プロファイルの設定の詳細は、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「構成プロファイル」－「構成プロファイルの作成」

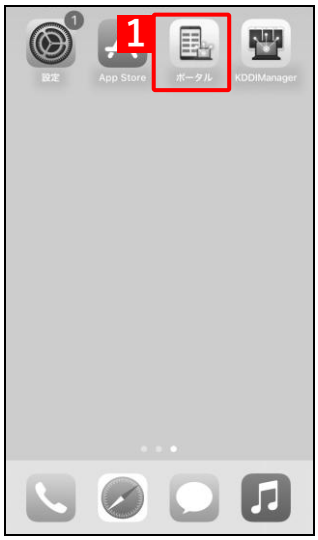




【7】［完了］をタップします。

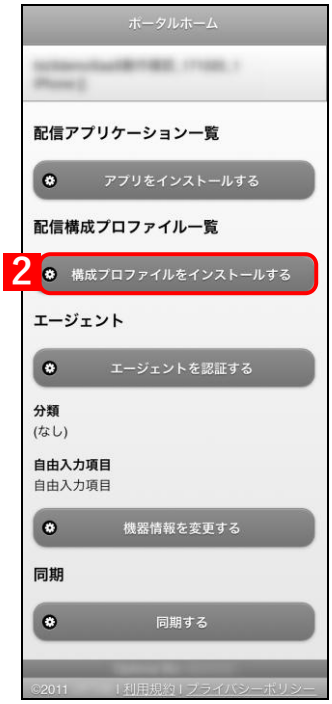
3.5.2 iOS 12.2 以上の場合

【1】［ポータル］をタップします。



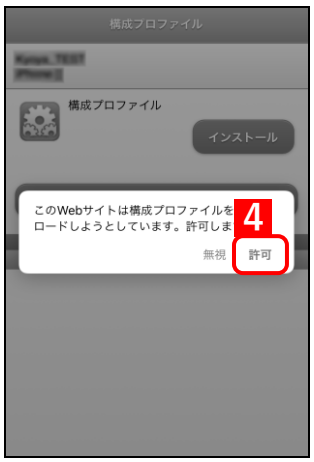
【2】［構成プロファイルをインストールする］をタップします。

管理サイトから構成プロファイルが 1 つも配信されていない場合、［構成プロファイルをインストールする］は表示されません。



【3】インストールしたい構成プロファイルの［インストール］をタップし、構成プロファイルのインストールを行います。

【4】メッセージを確認し、［許可］をタップします。

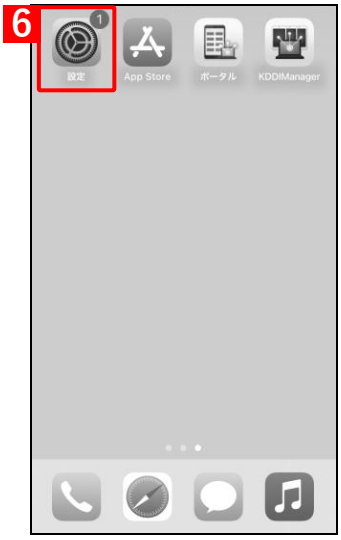


【5】右のようなポップアップ画面が表示されます。［閉じる］をタップします。

⇒構成プロファイルのダウンロードが完了します。

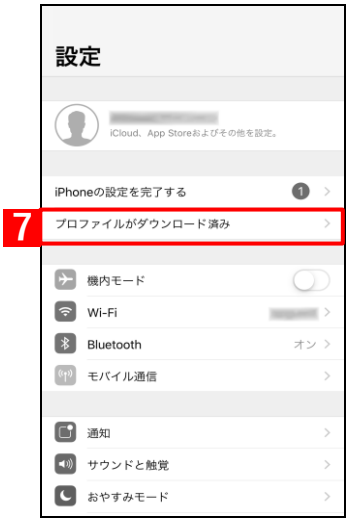
iOS のバージョンにより「プロファイルがダウンロード済み」は、「プロファイルがダウンロードされました」など、表記が異なる場合があります。

【6】iOS 端末のホーム画面から［設定］をタップします。



【7】［プロファイルがダウンロード済み］をタップします。

iOS のバージョンにより［プロファイルがダウンロード済み］は、［プロファイルがダウンロードされました］など、表記が異なる場合があります。



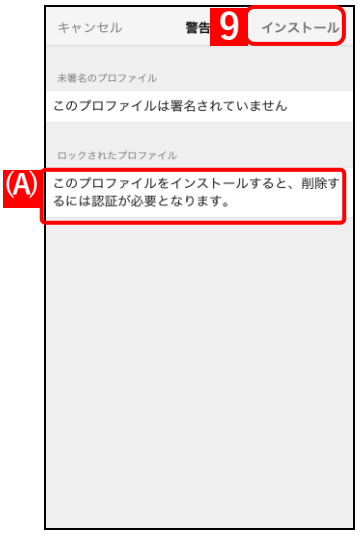
【8】［インストール］をタップします。

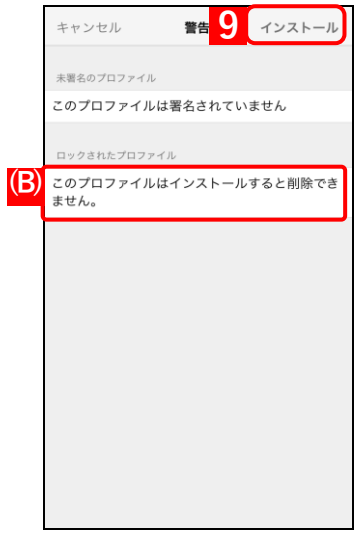
【9】［インストール］をタップします。

警告メッセージは、管理サイトの構成プロファイルの設定により（A）または（B）が表示されます。メッセージを確認のうえ、［インストール］をタップしてください。

構成プロファイルの設定の詳細は、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「構成プロファイル」－「構成プロファイル」

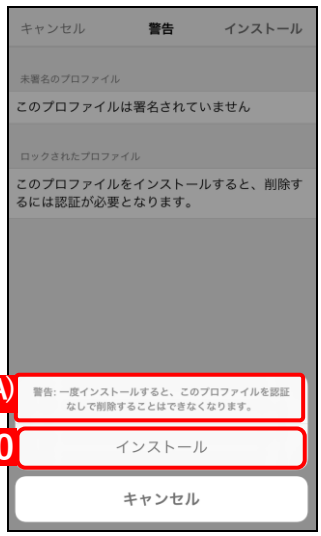


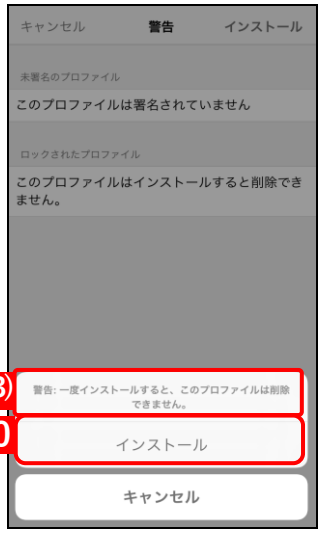


【10】［インストール］をタップします。

確認メッセージは、管理サイトの構成プロファイルの設定により（A）または（B）が表示されます。メッセージを確認のうえ、［インストール］をタップしてください。
構成プロファイルの設定の詳細は、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「構成プロファイル」－「構成プロファイル」





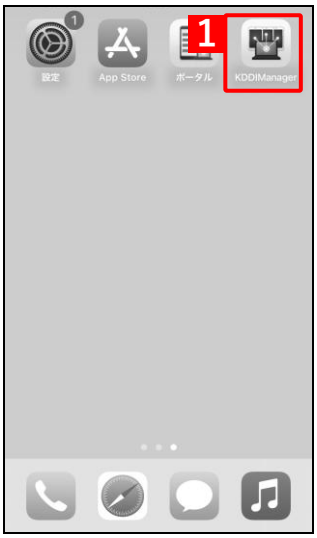
【11】［完了］をタップします。

4 エージェントの使用方法

この章では、エージェントの使用方法について説明します。

4.1 エージェントを起動する

【1】エージェントアイコン（KDDI Manager）をタップします。



【2】エージェントが起動されました。

エージェントが提供する機能を利用するには、エージェントが起動している必要があります。マルチタスク表示などからエージェントを終了した場合は、再度、本手順に沿って、エージェントを起動してください。

4.2 エージェントの基本情報を確認する

エージェントの基本情報（機器情報、ユーザー情報、更新情報）を確認します。

【1】左上の［≡］をタップしてメニューを開き、［ホーム］をタップします。

エージェントの起動方法は、以下を参照してください。

「エージェントを起動する」42 ページ

【2】エージェント基本情報が表示されました。

4.3 メッセージ

管理サイトから送信されたメッセージの確認方法や、未開封メッセージの通知が表示された場合について説明します。

本機能はオプション機能（追加機能）のため、別途契約が必要です。

メッセージの設定方法については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「機器」―「メッセージ通知」

4.3.1 メッセージを確認する

iPhone/iPad で操作が異なります。使用している iOS 端末に応じて、メッセージを確認します。

●iPhone の場合

●iPad の場合

4.3.1.1 iPhone の場合

【1】エージェントを起動します。

エージェントの起動方法は、以下を参照してください。

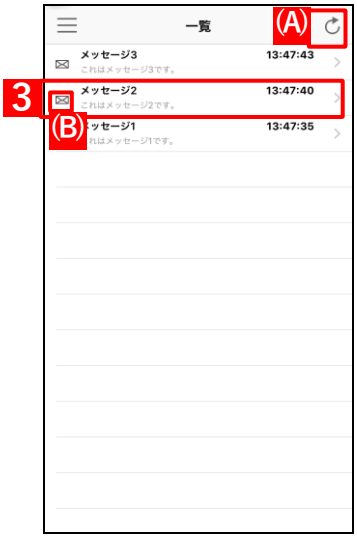
「エージェントを起動する」42 ページ

【2】［≡］をタップし、表示されるメニューから［メッセージ］をタップします。

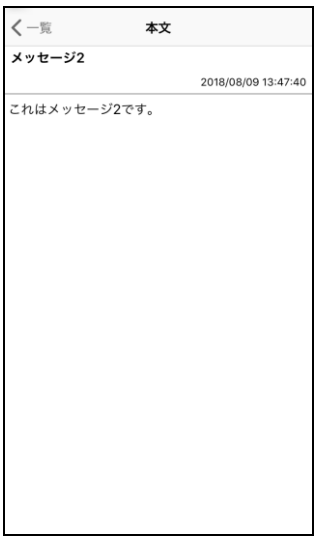
【3】確認するメッセージをタップします。

メッセージを更新するには（A）をタップします。機器情報、ユーザー情報もあわせて更新されます。

未開封のメッセージにはメッセージタイトルの左にメールアイコン（B）が表示されます。



【4】メッセージが表示されました。



4.3.1.2 iPad の場合

【1】エージェントを起動します。

エージェントの起動方法は、以下を参照してください。

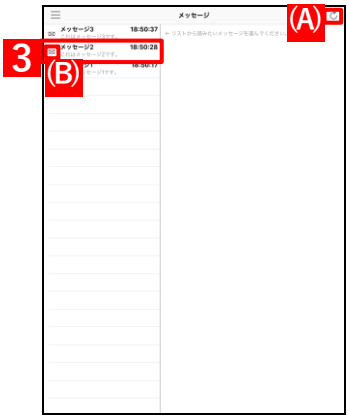
「エージェントを起動する」**42 ページ**

【2】［≡］をタップし、表示されるメニューから［メッセージ］をタップします。

【3】確認するメッセージをタップします。

メッセージを更新するには（A）をタップします。機器情報、ユーザー情報もあわせて更新されます。

未開封のメッセージにはメッセージタイトルの左にメールアイコン（B）が表示されます。



【4】メッセージが表示されました。

4.3.2 未開封メッセージを確認する

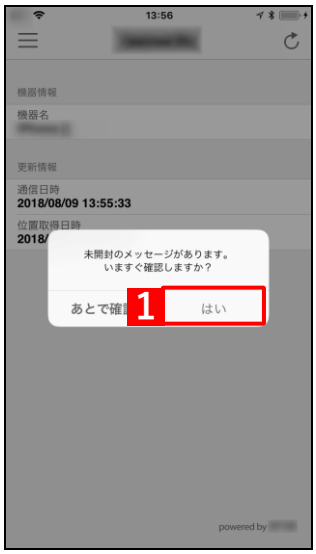
管理サイトから新しいメッセージが配信された場合などに、未開封メッセージがあることを通知するダイアログやバナーが表示されます。エージェントの起動状況によりメッセージの確認方法が異なるため、状況に合わせてメッセージを確認します。

●エージェントが起動中の場合

●エージェントが起動していない場合

4.3.2.1 エージェントが起動中の場合

【1】今すぐメッセージを確認する場合は、［はい］をタップします。



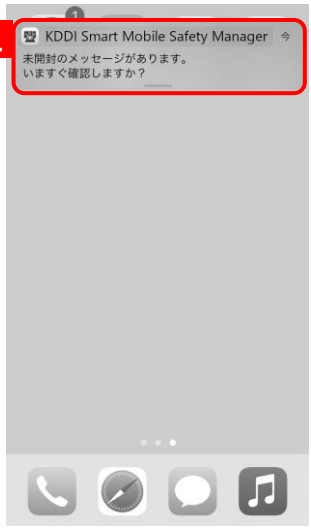
あとで確認する場合は、［あとで確認］をタップします。

メッセージの確認方法は、以下を参照してください。

「メッセージを確認する」44 ページ

4.3.2.2 エージェントが起動していない場合

【1】今すぐメッセージを確認する場合は、バナーをタップします。



一時的な表示になるか、持続的な表示になるかは、iOS 端末の設定により異なります。

右の画面は iOS 11.0 となります。iOS 10.0 以上では、ダイアログ表示はなくなり、以下の 2 つになりました。

- バナー表示：一時的
  バナーを表示したあと、数秒後に自動的に消えます。
- バナー表示：持続的
  バナーを表示したあと、通知をタップするか、ホームボタンを押下するまで表示し続けます。

iOS の「設定」アプリ→［通知］→［KDDI Smart Mobile Safety Manager］→「バナーとして表示」の画面より設定できます。

4.4 エージェントからポータルを表示する

エージェントからポータルを表示します。ポータルでは、機器情報の変更や配信されたアプリのインストールなどが行えます。

本機能は、エージェントバージョン 7.0.100.0 以上で使用できます。

MDM 構成プロファイルのインストールとエージェント認証はできません。

【1】エージェントを起動します。

エージェントの起動方法は、以下を参照してください。

「エージェントを起動する」42 ページ

【2】［≡］をタップし、表示されるメニューから［ポータル］をタップします。

【3】エージェント上にポータルが表示されました。

4.5 エージェントのバージョン情報を確認する

エージェントバージョンは、エージェント認証が完了していなくても確認ができます。本章では、エージェント認証が完了している場合の確認手順を説明しています。

【1】エージェントを起動します。

エージェントの起動方法は、以下を参照してください。

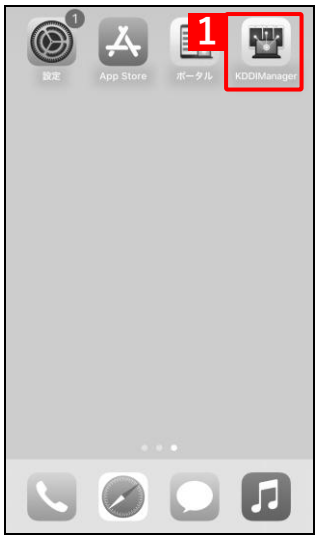
「エージェントを起動する」42 ページ

【2】［≡］をタップし、表示されるメニューから［情報］をタップします。

【3】エージェントのバージョン情報が表示されました。

4.6 エージェントをアンインストールする

【1】エージェントアイコン（KDDI Manager）を長押しします。



【2】［App を削除］をタップします。
⇒確認画面が表示されます。

【3】［App を削除］をタップします。
⇒アンインストールされ、アイコンも削除されます。

5 管理サイトからの指示による動作

この章では、管理サイトからの指示による動作について説明します。

5.1 リモートロック画面の表示内容

iOS 端末が紛失／盗難にあった場合に画面をロックし、管理サイトで設定された情報を画面に表示します。

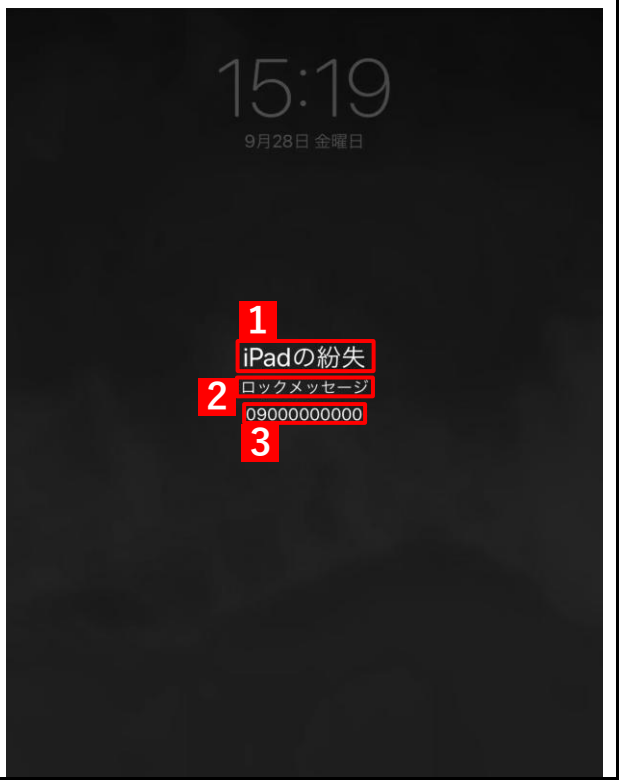
端末のロックは、管理サイトから行います。詳細については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「機器」―「一覧」―「機器の操作」―「(操作―iOS) リモートロック」

『管理サイト リファレンスマニュアル』の「機器」―「全機器一括設定」―「[その他▼] タブ／iOS リモート操作」

ロック中の iOS 端末は、iOS のパスコードで保護されています。

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。そのため、管理者が管理サイトで設定した連絡情報（ロックメッセージ、連絡先の電話番号）を、iOS 端末では確認できません。リモートロックのメッセージを受信するには、「設定」→「一般」→「パスコードロック」から「パスコードロックをオンにする」を選択し、パスコードロックを有効にしてください。

≪iPhone の場合≫	≪iPad の場合≫
	

項番	名称	説明
1	デフォルト ロックメッセージ	iOS 端末にデフォルトで設定されている紛失時のメッセージです。iOS のバージョンにより表示されるメッセージが異なります。
2	ロックメッセージ	管理サイトで設定されたロックメッセージが表示されます。
3	電話番号	紛失時の連絡先など、管理サイトで設定された電話番号が表示されます。
4	発信ボタン	タップすると項番【3】の電話番号に対して通話を行います。 SIM が入っていない場合は、発信ボタンは表示されません。
5	緊急	110、119 などの緊急通報ができます。

5.2 紛失モード画面の表示内容

紛失モードは、Apple が提供する iOS 端末の機能です。iOS 端末が紛失／盗難にあった場合に画面をロックし、管理サイトで設定された情報を紛失モード画面に表示します。端末のロック／ロック解除は、管理サイトから行います。詳細については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「機器」―「一覧」―「機器の操作」―「(操作―iOS) 紛失モード」、「(操作―iOS) 位置情報取得」、「(操作―iOS) 紛失モード解除」

『管理サイト リファレンスマニュアル』の「機器」―「全機器一括設定」―「[その他▼] タブ／iOS リモート操作」

紛失モード中の画面と紛失モードが解除された画面について説明します。

●紛失モード中の表示

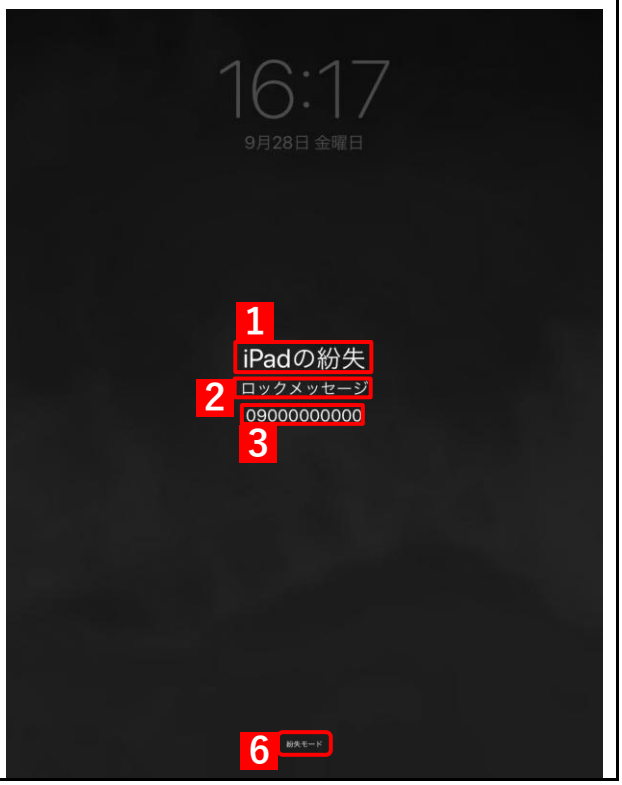
●紛失モード解除後の表示

iOS 9.3 以上の監視対象端末のみ使用できます。

紛失モード中は、低電力モードになります。

パスコードが設定されていない場合も使用できます。

5.2.1 紛失モード中の表示

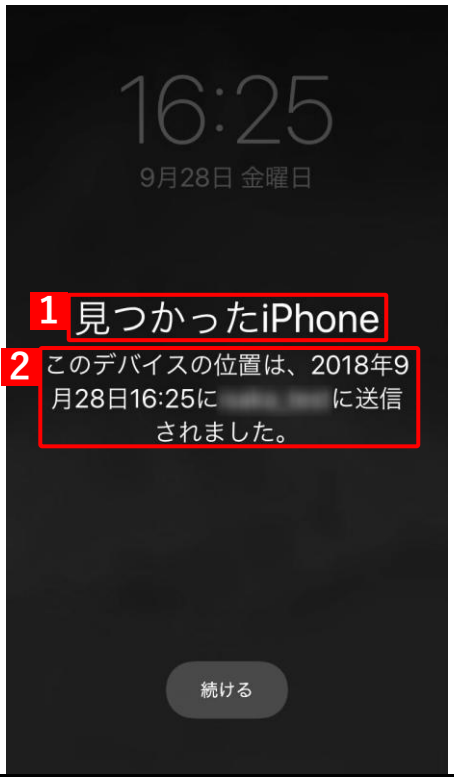
≪iPhone の場合≫	≪iPad の場合≫
	

項番	名称	説明
1	デフォルト ロックメッセージ	iOS 端末にデフォルトで設定されている紛失時のメッセージです。iOS のバージョンにより表示されるメッセージが異なります。
2	ロックメッセージ	管理サイトで設定されたロックメッセージが表示されます。
3	電話番号	紛失時の連絡先など、管理サイトで設定された電話番号が表示されます。
4	発信ボタン	タップすると項番【3】の電話番号に対して通話を行います。 SIM が入っていない場合は、発信ボタンは表示されません。

項番	名称	説明
5	緊急	110、119 などの緊急通報ができます。
6	脚注	管理サイトで設定された脚注が表示されます。

5.2.2 紛失モード解除後の表示

≪iPhone の場合≫



項番	名称	説明
1	デフォルト ロックメッセージ	iOS 端末にデフォルトで設定されている紛失時のメッセージです。iOS のバージョンにより表示されるメッセージが異なります。
2	解除後のメッセージ	位置情報を送信した場合は、管理サイトに位置情報を送信した日時が表示されます。iOS のバージョンにより表示されるメッセージは異なります。 位置情報が取得されていない場合には、表示されません。 iOS 9 の場合は、解除後にダイアログが出力されます。

5.3 「App とブック」の利用規約に同意する

「App とブック」を通じてアプリや書籍が配信された場合、「App とブック」の割り当てが端末に許可されていないと、管理サイトからの同期が行われるたびに「App とブック」の割り当てを求める画面が表示され、アプリや書籍が受信できません。そのため、初回配信時に「App とブック」を端末に割り当てる利用規約に同意して、アプリや書籍の受信が行えるようにします。

「App とブック」の詳細については、以下を参照してください。

- 『Apple Business Manager（ABM）マニュアル（利用方法・年次更新手順）』
- 『Apple School Manager（ASM）マニュアル（利用方法・年次更新手順）』
- 『iOS アプリケーション配信 手順書』

【1】［続ける］をタップします。

⇒Apple のアプリや書籍に関する使用条件とプライバシーポリシーが表示されます。

サインインしていない場合は、サインインを求める画面が表示されます。［続ける］をタップしてサインインしてください。

割り当てを許可しない場合は、管理サイトからの同期が行われたときに再度確認画面が表示されます。割り当てが許可されるまで、「App とブック」でアプリや書籍の配布は行われません。

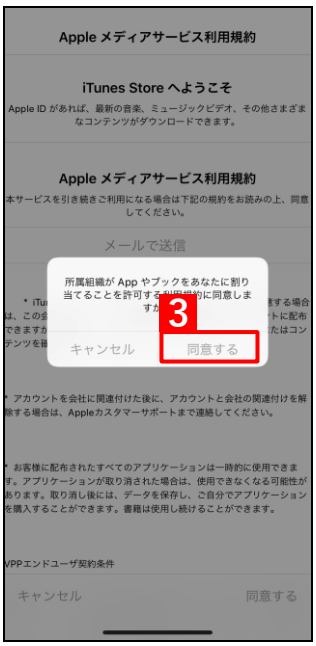
OS のバージョンによっては、要求画面が異なる場合があります。

【2】下までスクロールして、［同意する］をタップします。

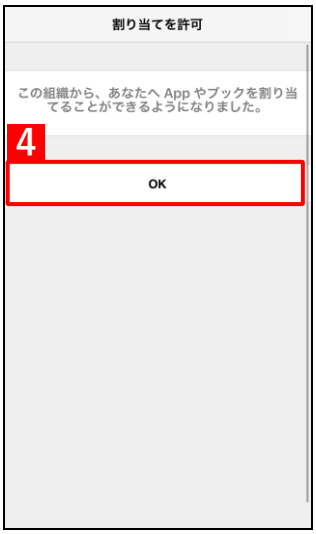
⇒確認画面が表示されます。

【3】［同意する］をタップします。

⇒割り当てが完了します。



【4】［OK］をタップします。



6 関連アプリの使用方法

この章では、本製品の関連アプリの使用方法について説明します。

☞「＋browser Safety Manager」59 ページ
☞「Safety Manager App Catalog」68 ページ

6.1 ＋browser Safety Manager

＋browser Safety Manager は、弊社が提供しているブラウザーです。iOS 端末の標準ブラウザーとは別にインストールが必要です。

＋browser Safety Manager は、ブックマーク追加、お気に入り設定、セキュリティ設定など、標準ブラウザーと同等の機能があります。

＋browser Safety Manager のみを使用することで、管理サイトの機能（Web フィルタリング、お気に入り、Web 閲覧履歴など）でブラウザーの使用を制限することもできます。

＋browser Safety Manager は、オプション機能（追加機能）のため、別途契約が必要です。

＋browser Safety Manager は、証明書認証の機能には対応していません。

＋browser Safety Manager は、他のサーバーを経由するアプリ（オンライン会議用アプリなど）の利用ができません。

＋browser Safety Manager で PDF ファイルは表示できません。別途、PDF ファイルを表示や印刷などができるアプリをインストールしてください。

＋browser Safety Manager は、エージェント認証されていないと、Web フィルタリング、Web 閲覧履歴、お気に入りなどのブラウザー関連機能が使用できません。エージェント認証については、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」

構成プロファイルの設定で Safari を使用禁止にした場合、以下の機能が使用できなくなります。

- KDDI Smart Mobile Safety Manager のポータル画面（一部機能はエージェントから利用できます）

「本製品で行えること」10 ページ

- Web クリップ機能（Safari のブックマーク機能）

Safari の使用禁止については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「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」－「画面（App の制限）」

＋browser Safety Manager の使用制限については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「インターネット」

6.1.1 ＋browser Safety Manager の動作環境

対応 OS	iOS 15.0 以上

6.1.2 ＋browser Safety Manager をインストールする

＋browser Safety Manager をインストールするには、以下の 2 通りあります。どちらかの方法を選択してください。

●アプリケーション配信機能でインストールする

●App Store からインストールする

6.1.2.1 アプリケーション配信機能でインストールする

管理サイトからアプリケーション配信機能で配信された＋browser Safety Manager のインストール手順について説明します。配信された＋browser Safety Manager は管理状態によってインストール手順が異なります。「管理対象アプリ」として＋browser Safety Manager が配信された場合は、サイレントインストールされるため、端末の操作を行う必要はありません。「非管理対象アプリ」として＋browser Safety Manager が配信された場合は、本操作でインストールを行います。

「管理対象アプリ」、「非管理対象アプリ」については、以下を参照してください。

『iOS アプリケーション配信　手順書』の「アプリケーション配信について」－「アプリケーション配信とは」

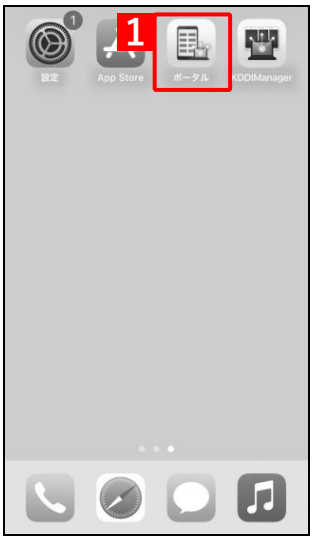
『管理サイト　リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」

省データモードを設定している iOS 13.1 以上の端末に「管理対象アプリ」として＋browser Safety Manager を配信した場合は、サイレントインストールは行われず、ホーム画面上にグレーアウトしたアイコンが表示されます。アイコンをタップしてインストールを行ってください。

あらかじめ管理サイトからアプリを配信します。詳細については、以下を参照してください。

『管理サイト　リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」

【1】［ポータル］をタップします。



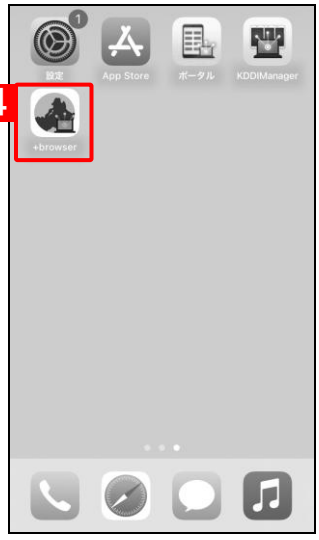
【2】［アプリをインストールする］をタップします。

【3】＋browser Safety Manager の［インストール］をタップします。

⇒ホーム画面にアイコン（+browser）が表示されます。

【4】アイコン（+browser）をタップし起動します。

⇒プライバシーポリシー同意画面が表示されます。



【5】［同意する］をタップします。

⇒メイン画面が表示されます。

☞「メイン画面」65 ページ

「同意しない」をタップした場合は、＋browser Safety Manager を使用することができず、再びこの画面が表示されます。

エージェントバージョン 2.2.0.100 未満では、本画面は表示されません。

6.1.2.2 App Store からインストールする

App Store から＋browser Safety Manager をインストールする手順について説明します。

管理サイトで App Store を表示させる制限（「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」）は、有効に設定してください。

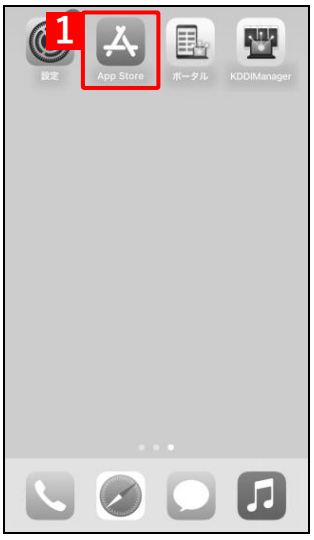
『管理サイト リファレンスマニュアル』の「設定―iOS」－「構成プロファイル」－「構成プロファイルのアップロード」－「［iOS 制限設定］タブ」

【1】［App Store］をタップします。

【2】「＋browser Safety Manager」を検索してインストールします。

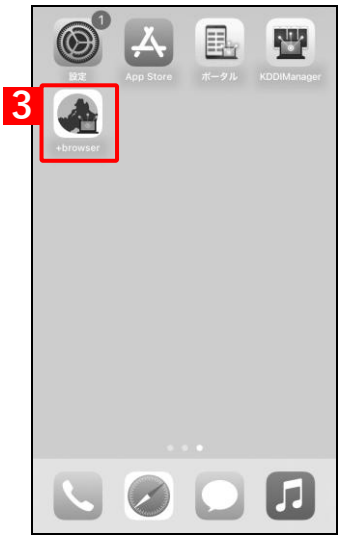
手順は App Store のインストール手順に従ってください。

⇒ホーム画面にアイコン（+browser）が表示されます。



【3】アイコン（+browser）をタップし起動します。

⇒プライバシーポリシー同意画面が表示されます。



【4】［同意する］をタップします。

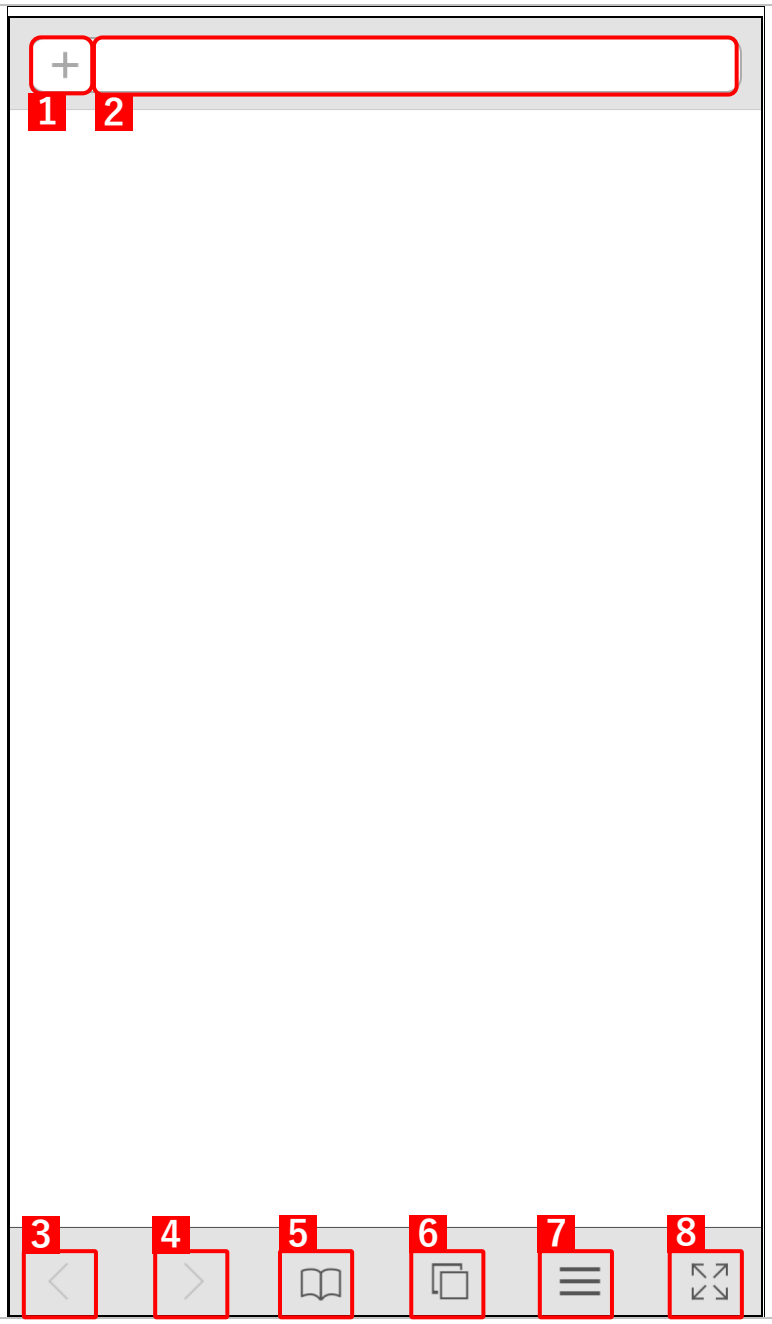
⇒メイン画面が表示されます。

☞「メイン画面」65 ページ

「同意しない」をタップした場合は、＋browser Safety Manager を使用することができず、再びこの画面が表示されます。

エージェントバージョン 2.2.0.100 未満では、本画面は表示されません。

6.1.3 メイン画面



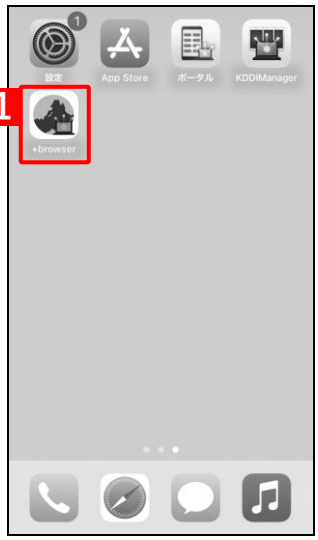
項番	名称	説明
1	ブックマーク追加	現在閲覧しているページをブックマークに登録します。
2	アドレスバー	閲覧しているページの URL が表示されます。 Web ページを閲覧していると、[更新]ボタンが右側に表示されます。
3	前のページへ戻る	前のページへ戻ります。
4	次のページへ進む	次のページへ進みます。
5	ブックマーク一覧	ブックマークの一覧を表示します。
6	タブ一覧	タブ一覧を表示します。
7	設定	設定画面が表示されます。
8	拡大	メイン画面を拡大する場合にタップします。

6.1.4 設定画面

項番	名称	説明
1	バージョン	＋browser Safety Manager のバージョン情報が表示されます。
2	通信日時	管理サイトとの最後の通信日時が表示されます。
3	Cookie を受け入れる	Cookie の受け入れ許可設定を行います。以下から選択します。 ●しない ●訪問先のみ ●常に
4	パスワードを保存する	ブラウザー内で入力したパスワードを自動保存する設定を行います。
5	プライバシーポリシー	プライバシーポリシーが表示されます。
6	履歴を削除	ブラウザーの履歴を削除します。
7	Cookie とデータを削除	Cookie、キャッシュ、フォームデータ、位置情報のデータを削除します。
8	パスワードを削除	パスワードのデータを削除します。

6.1.5 ＋browser Safety Manager をアンインストールする

【1】アイコン（+browser）を長押しします。



【2】［App を削除］をタップします。
⇒確認画面が表示されます。

【3】［App を削除］をタップします。
⇒アンインストールされ、アイコンも削除されます。

6.2 Safety Manager App Catalog

Safety Manager App Catalog とは、管理者が推奨／承認しているアプリを iOS 端末にインストールするツールです。配信されたアプリ一覧からアプリやアプリの詳細を確認して、インストールをすることができます。

アプリ一覧を配信するには、管理サイトで設定を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。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリカタログ」

6.2.1 Safety Manager App Catalog の動作環境

対応 OS	iOS 15.0 以上

6.2.2 Safety Manager App Catalog をインストールする

Safety Manager App Catalog をインストールするには、以下の 3 通りがあります。どちらかの方法を選択してください。

- アプリケーション配信機能でインストールする
- App Store からインストールする
- 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

App Store からインストールすると、管理サイトとの同期が正常にできない場合があるため、アプリケーション配信でのインストールを推奨しています。

エージェントの認証が完了している場合は、Safety Manager App Catalog も自動的に認証済みとなります。エージェントの認証が完了していない、またはエージェントを利用していない場合は、Safety Manager App Catalog で認証を行います。ただし、エージェントを利用していない場合でも、アプリケーション配信時に App Configuration を設定した場合は、自動的に認証済みとなります。

『iOS キッティングマニュアル』の「エージェントを認証する」

6.2.2.1 アプリケーション配信機能でインストールする

管理サイトからアプリケーション配信機能で配信された Safety Manager App Catalog のインストール手順について説明します。配信された Safety Manager App Catalog は管理状態によってインストール手順が異なります。「管理対象アプリ」として Safety Manager App Catalog が配信された場合は、サイレントインストールされるため、端末の操作を行う必要はありません。「非管理対象アプリ」として Safety Manager App Catalog が配信された場合は、本操作でインストールを行います。

「管理対象アプリ」、「非管理対象アプリ」については、以下を参照してください。

『iOS アプリケーション配信 手順書』の「アプリケーション配信について」－「アプリケーション配信とは」

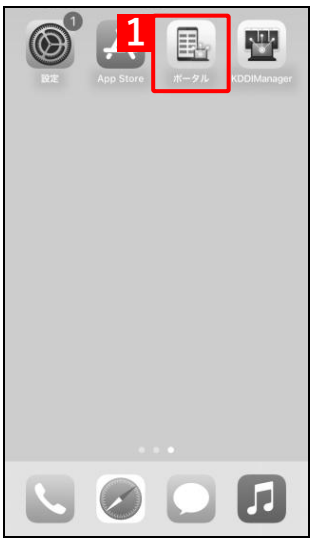
『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」

省データモードを設定している iOS 13.1 以上の端末に「管理対象アプリ」としてアプリカタログを配信した場合は、サイレントインストールは行われず、ホーム画面上にグレーアウトした「待機中」アイコンが表示されます。アイコンをタップしてインストールを行ってください。

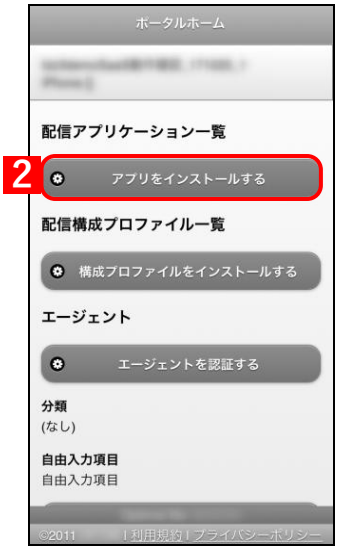
あらかじめ管理サイトからアプリを配信します。詳細については、以下を参照してください。

『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」

【1】［ポータル］をタップします。



【2】［アプリをインストールする］をタップします。

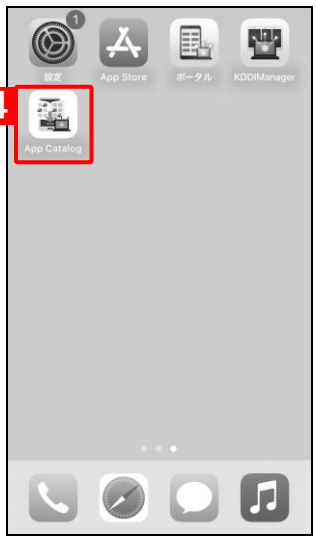


【3】Safety Manager App Catalog の［インストール］をタップします。

⇒ホーム画面にアイコン（App Catalog）が表示されます。

【4】アイコン（App Catalog）をタップし起動します。

⇒プライバシーポリシー同意画面とデータの取り扱いについてが表示されます。



【5】［同意する］をタップします。

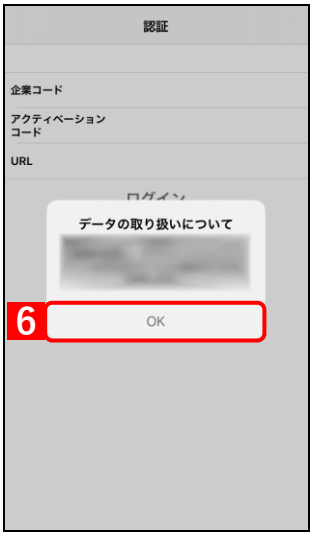
「同意しない」をタップした場合は、Safety Manager App Catalog を使用することができず、再びこの画面が表示されます。

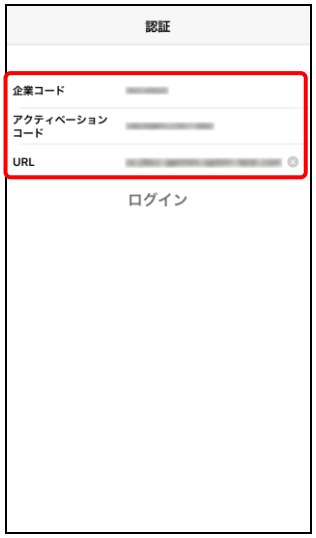
【6】「OK」をタップします。

⇒メイン画面が表示されます。

「メイン画面」83 ページ

エージェント認証が完了していない、もしくはエージェントを利用していない場合は、認証画面が表示されます。
企業コード、アクティベーションコード、URL を管理者にお問い合わせのうえ、入力してください。





6.2.2.2 App Store からインストールする

App Store から Safety Manager App Catalog をインストールする手順について説明します。

App Store からインストールを行うと管理サイトとの同期が正常にできない場合があるため、アプリケーション配信でのインストールを推奨します。

「アプリケーション配信機能でインストールする」69 ページ

管理サイトで App Store を表示させる制限（「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」）は、有効に設定してください。

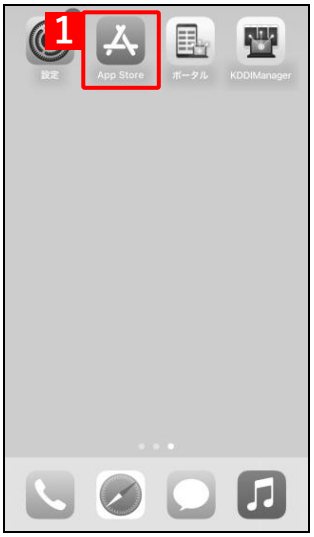
『管理サイト リファレンスマニュアル』の「設定―iOS」－「構成プロファイル」－「構成プロファイルのアップロード」－「［iOS 制限設定］タブ」

【1】［App Store］をタップします。

【2】「Safety Manager App Catalog」を検索してインストールします。

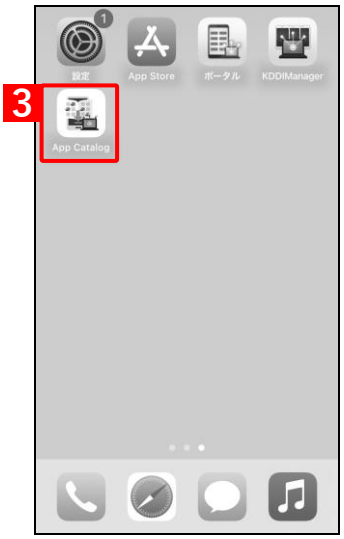
手順は App Store のインストール手順に従ってください。

⇒ホーム画面にアイコン（App Catalog）が表示されます。



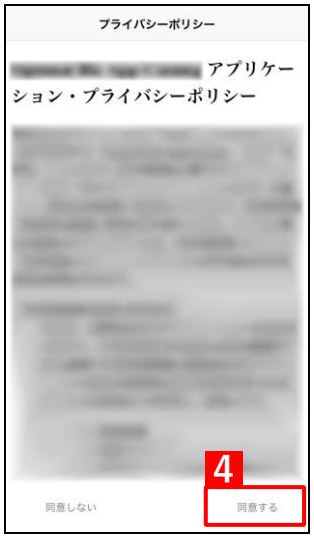
【3】アイコン（App Catalog）をタップし起動します。

⇒プライバシーポリシー同意画面とデータの取り扱いについてが表示されます。



【4】［同意する］をタップします。

「同意しない」をタップした場合は、アプリカタログを使用することができず、再びこの画面が表示されます。

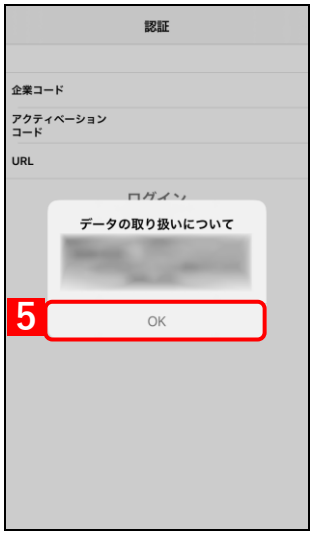


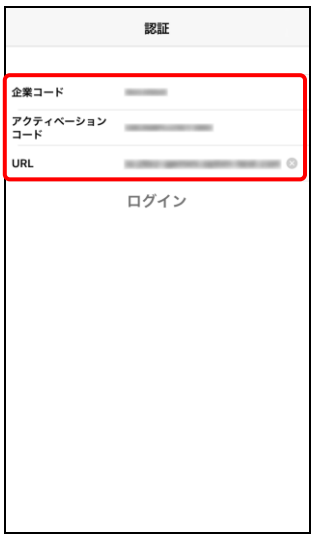
【5】「OK」をタップします。

⇒メイン画面が表示されます。

☞「メイン画面」83 ページ

エージェント認証が完了していない、もしくはエージェントを利用していない場合は、認証画面が表示されます。企業コード、アクティベーションコード、URL を管理者にお問い合わせのうえ、入力してください。





6.2.2.3 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

端末上のポータルと App Store をどちらも非表示の設定にしている場合は、管理サイトのアプリケーション配信機能と App Configuration 機能を利用することで、Safety Manager App Catalog をインストール／自動認証することができます。

Safety Manager App Catalog を端末に配信するための設定（アプリケーション配信設定）と、エージェントを自動認証するための設定（App Configuration 設定）を作成します。

機能および操作の詳細については、以下を参照してください。

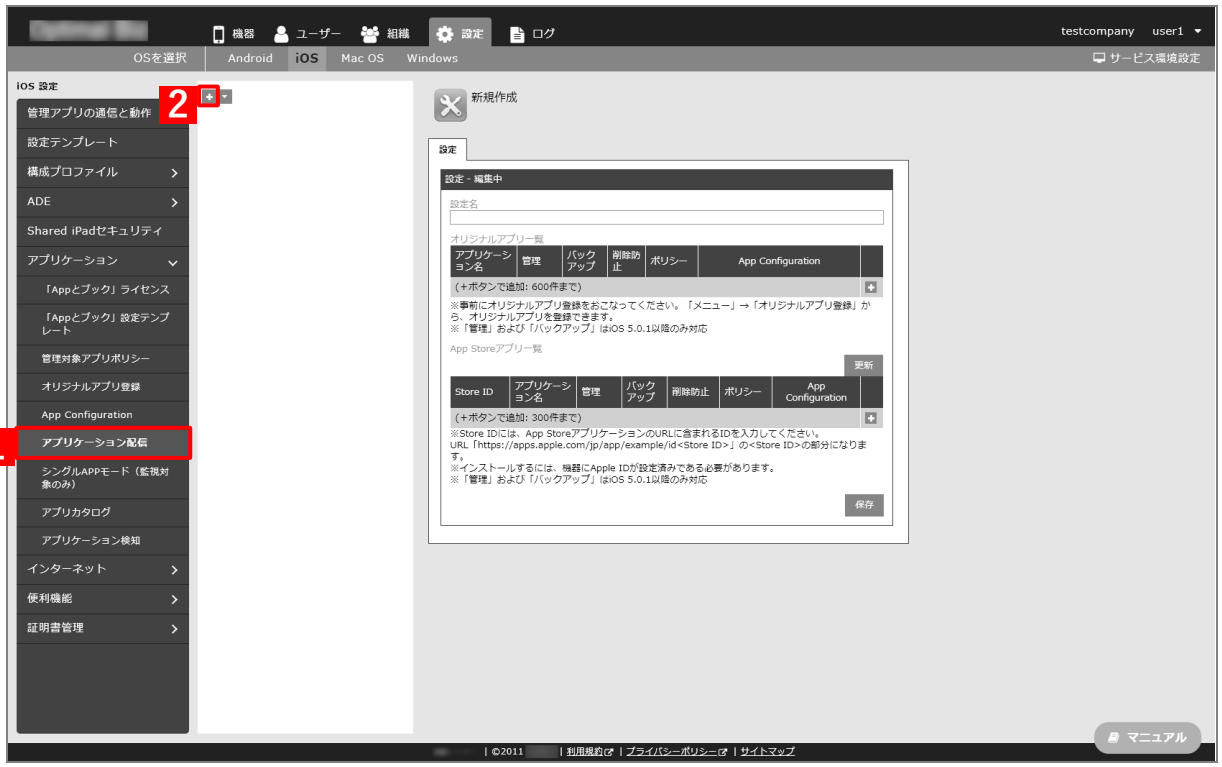
- 『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「アプリケーション配信」、「App Configuration」
- 『管理サイト リファレンスマニュアル』の「機器」－「一覧」－「機器の設定」－「(設定－iOS) 設定の割り当て」

バージョン 2.10 以上の Safety Manager App Catalog は、起動時に以下の条件を満たしている場合、すでに認証済みでも自動で認証を解除し、App Configuration 設定の認証情報に基づいて再認証します。

- 端末が App Configuration 設定を受信している。
  管理サイトで端末に割り当てている Safety Manager App Catalog のアプリケーション配信設定に App Configuration 設定を追加後、同期したときに端末は App Configuration 設定を受信します。
- 端末に Safety Manager App Catalog がインストールされてから、一度も App Configuration 設定の認証情報を利用した自動認証が行われていない。

App Configuration 設定を利用して認証済みになった端末は、そのあと App Configuration 設定の認証情報を変更しても変更後の認証情報を利用した再認証は行われません。設定変更後の認証情報を反映させたい場合は、Safety Manager App Catalog をアンインストールしてから再配信してください。

【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。



【3】「設定名」に任意の設定名を入力します。

【4】「App Store アプリ一覧」の ＋ をクリックします。

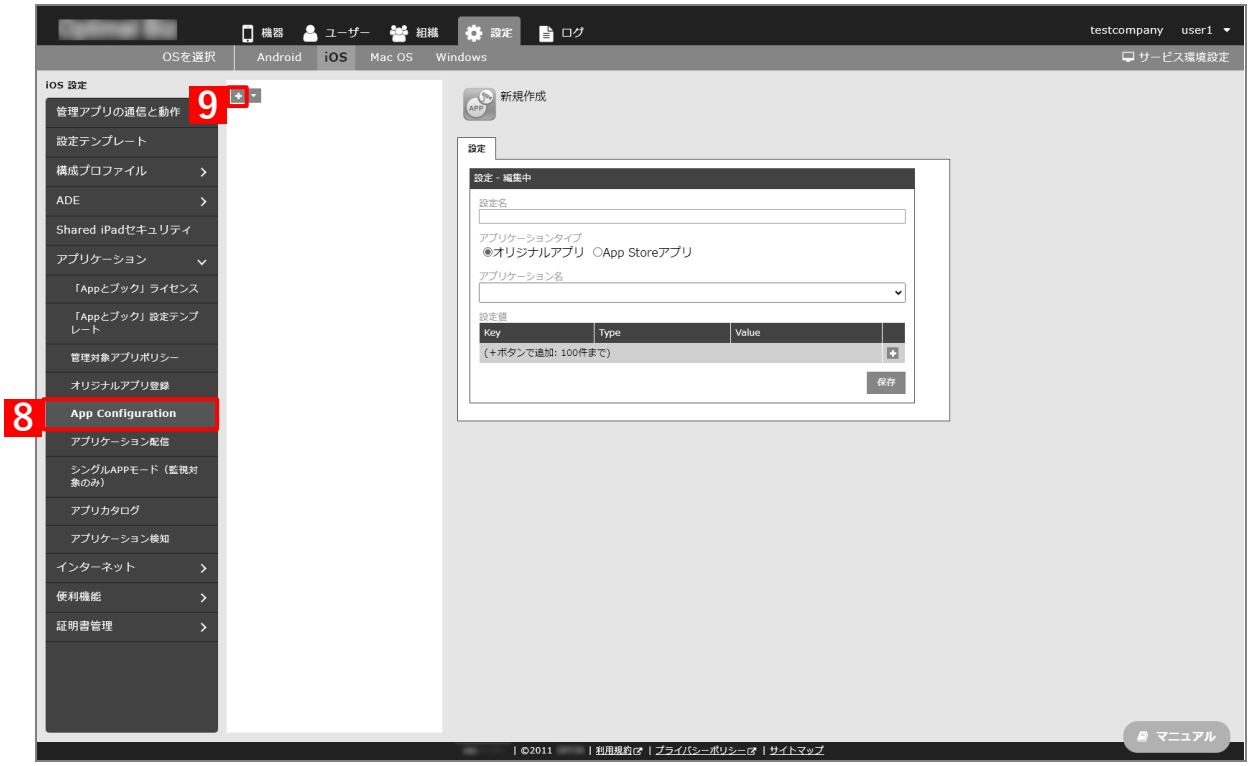
【5】「Store ID」に「1459071904」（Safety Manager App Catalog の Store ID）を入力します。

【6】「管理」の［有効］にチェックを入れます。

【7】［保存］をクリックします。

⇒アプリケーション配信設定が作成されます。

【8】［設定］→［iOS］→［アプリケーション］→［App Configuration］をクリックします。
【9】 をクリックします。



【10】「設定名」に任意の設定名を入力します。

【11】「アプリケーションタイプ」の［App Store アプリ］を選択します。

【12】「アプリケーション名」のプルダウンメニューから、［Safety Manager App Catalog］を指定します。

【13】「設定値」の ＋ をクリックして設定項目を追加し、各項目に（A）企業コード、（B）管理サイト URL、および（C）アクティベーションコードを設定します。

（A）企業コードの「Key」および「Value」に、それぞれ以下の値を入力してください。

- Key：company_code
- Value：（特定の企業コード）または%COMPANY_CODE%

（B）管理サイト URL の「Key」および「Value」に、それぞれ以下の値を入力してください。

- Key：server_url
- Value：https://ausl.smartmanager.jp/または%SERVER_URL%

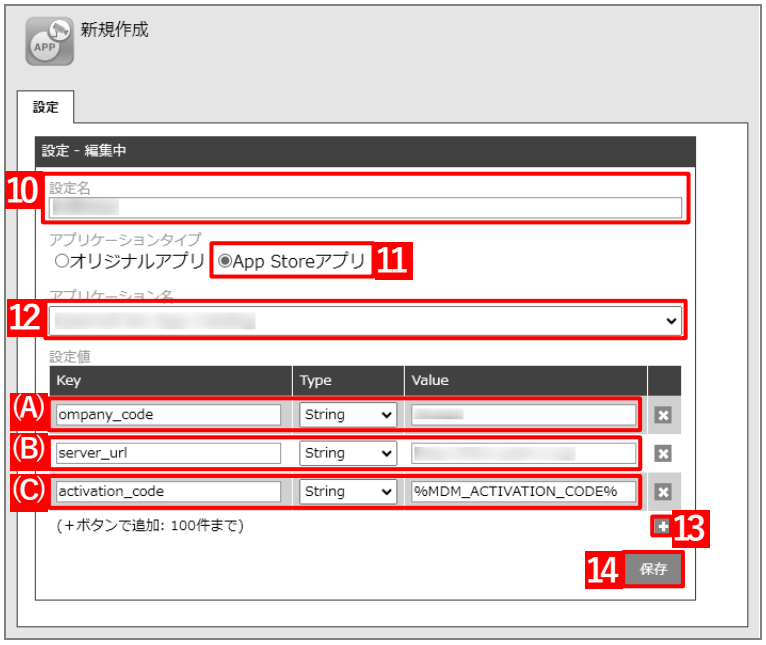
（C）アクティベーションコードの「Key」および「Value」に、それぞれ以下の値を入力してください。

- Key：activation_code
- Value：%MDM_ACTIVATION_CODE%

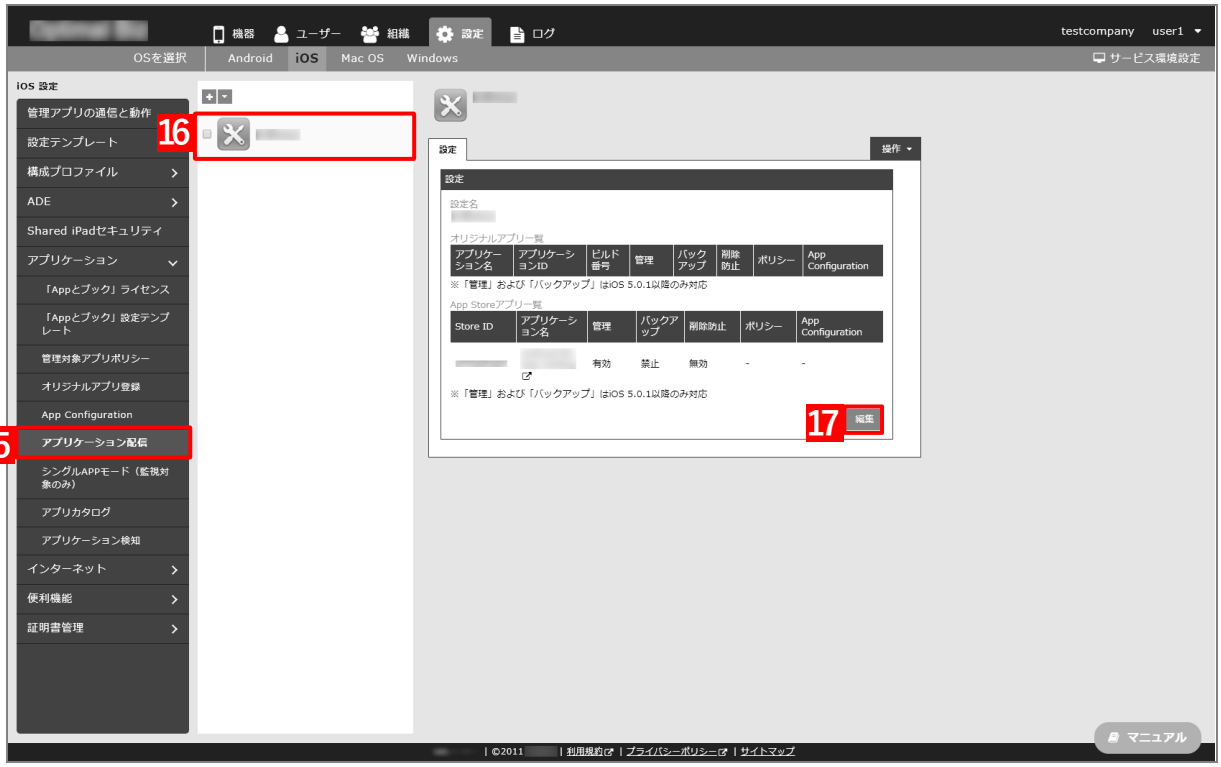
（A）企業コード、（B）管理サイト URL、および（C）アクティベーションコードともに、「Type」は［String］を選択してください。

【14】［保存］をクリックします。

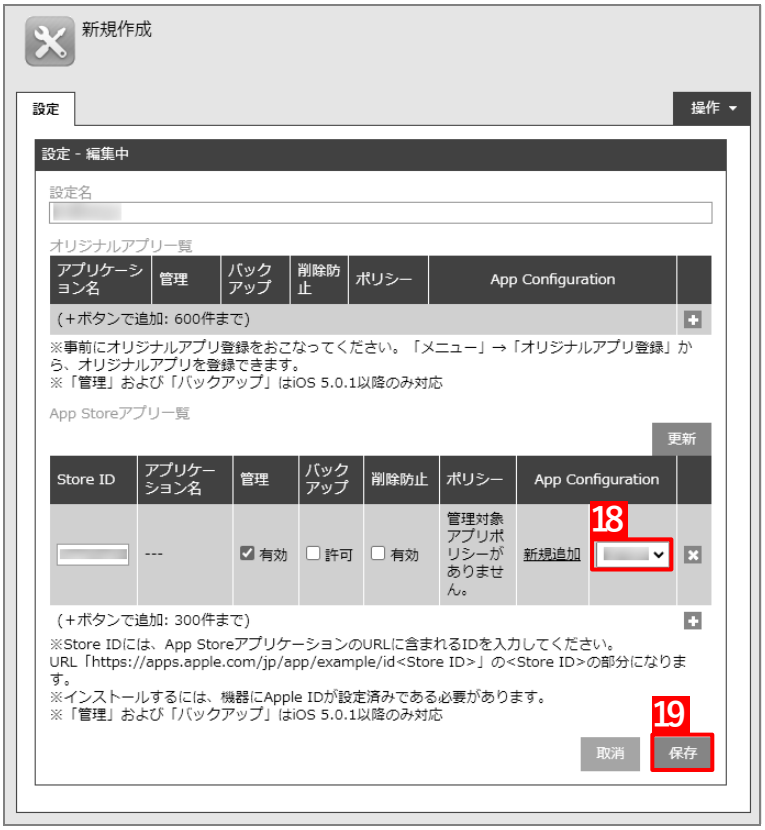
⇒App Configuration 設定が作成されます。



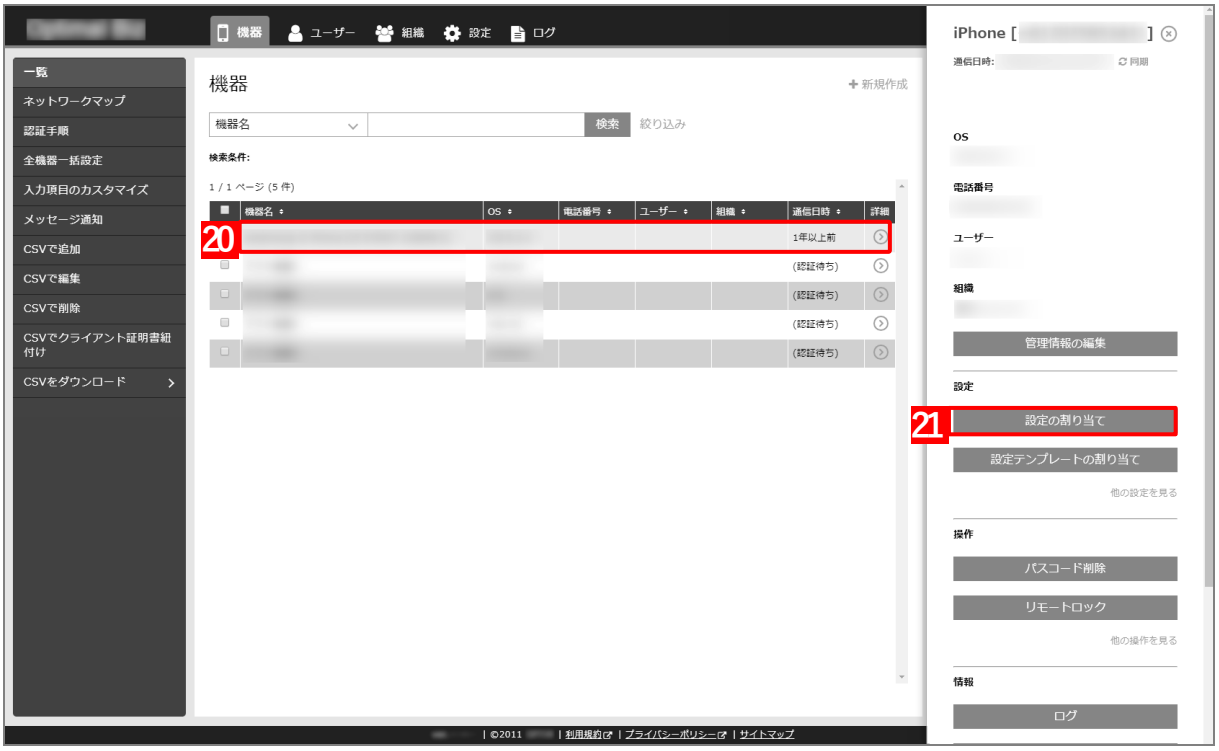
【15】［設定］→［iOS］→［アプリケーション］→［アプリケーション配信］をクリックします。
【16】一覧から、手順【7】で作成したアプリケーション配信設定をクリックします。
【17】［編集］をクリックします。



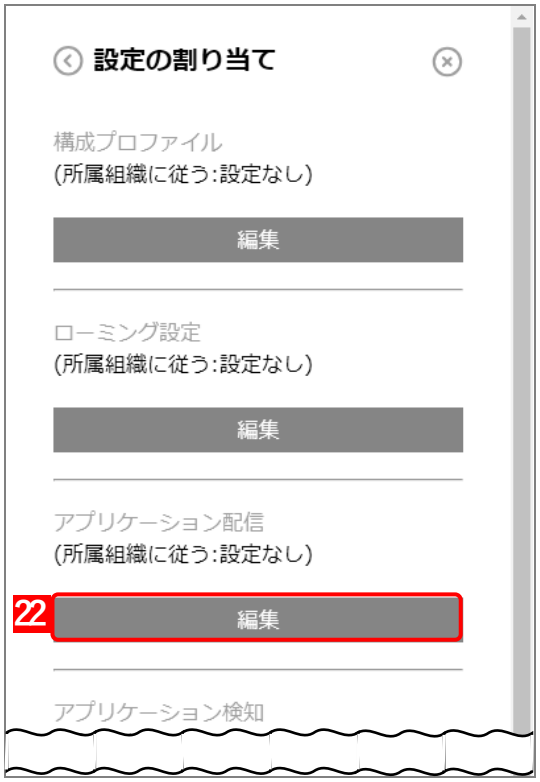
【18】「App Configuration」のプルダウンメニューから、手順【10】で設定した設定名を指定します。
【19】［保存］をクリックします。



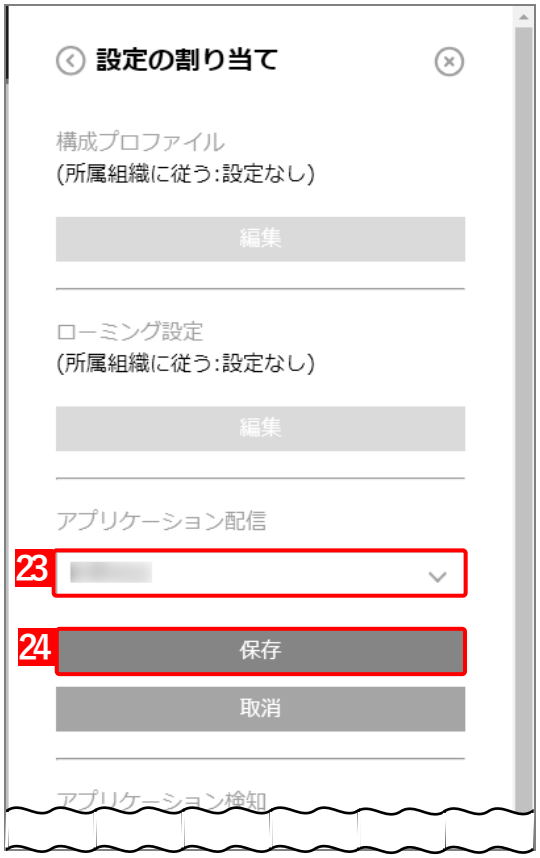
【20】［機器］→［一覧］→一覧から対象端末をクリックします。
【21】「設定」の［設定の割り当て］をクリックします。



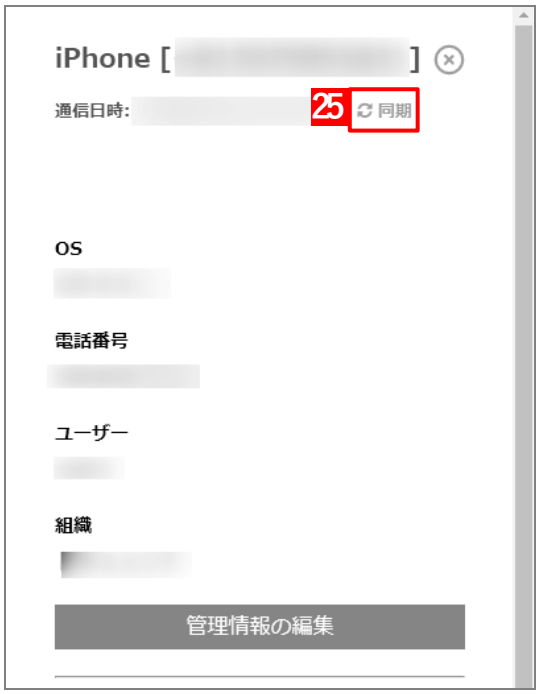
【22】「アプリケーション配信」の［編集］をクリックします。



【23】「アプリケーション配信」のプルダウンメニューから、手順【3】で設定した設定名を指定します。
【24】［保存］をクリックします。



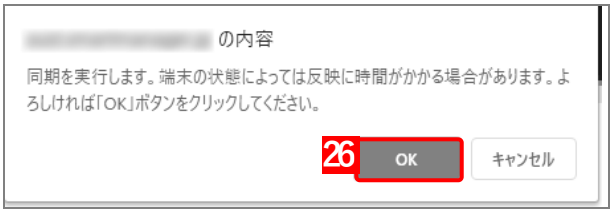
【25】［同期］をクリックします。



【26】［OK］をクリックします。

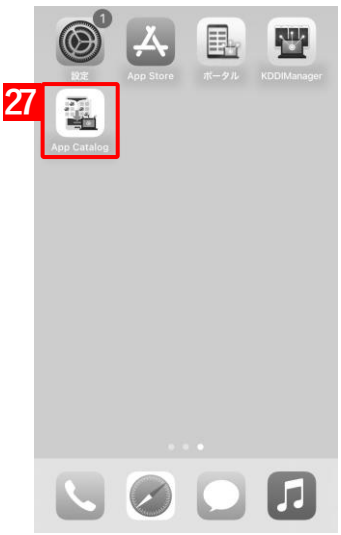
⇒端末に Safety Manager App Catalog がインストールされます。端末のホーム画面に、[App Catalog] のアイコンが表示されるまでお待ちください。

Safety Manager App Catalog が端末にインストールされるまでに、多少時間がかかることがあります。



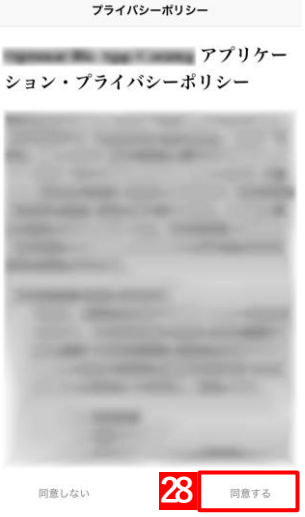
【27】アイコン（App Catalog）をタップし起動します。

⇒プライバシーポリシー同意画面とデータの取り扱いについてが表示されます。



【28】［同意する］をタップします。

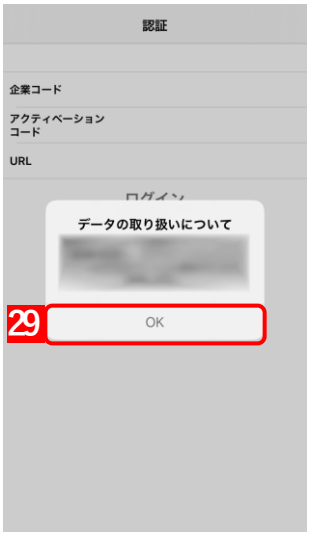
［同意しない］をタップした場合は、Safety Manager App Catalog を使用することができず、再びこの画面が表示されます。



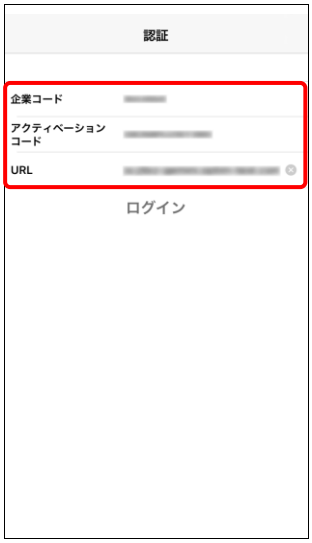
【29】「OK」をタップします。

⇒メイン画面が表示されます。

☞「メイン画面」83 ページ



エージェント認証が完了していない、もしくはエージェントを利用していない場合は、認証画面が表示されます。企業コード、アクティベーションコード、URL を管理者にお問い合わせのうえ、入力してください。



6.2.3 メイン画面

アプリカタログを起動している場合やバックグラウンドからフォアグラウンドに戻したときは、情報の更新は行われません。最新の情報を確認する場合は、注意してください。情報の取得、更新のタイミングは、以下のとおりです。

- 初期表示時
- 全体検索時
- グループ内遷移時（該当グループのみ更新）
- ［同期］タップ時

項番	名称	説明
1	グループ名	グループをソートします。
2	［同期］	Safety Manager App Catalog の情報を同期します。 メイン画面の表示タイミングでは、情報の同期はされません。インストール状況など、最新の情報を見るには［同期］ボタンをタップしてください。
3	［全体検索］	Safety Manager App Catalog 上のすべてのアプリについて、検索を行います。 詳細については、以下を参照してください。 「全体検索を行う」85 ページ
4	アプリ一覧	アプリ一覧が表示されます。タップするとアプリの詳細が確認できます。 各グループ内からランダムで 10 件表示されます。 アプリアイコンを左右にスワイプすると表示されていないアプリを表示できます。
5	［全て見る］	タップすると各グループ内のすべてのアプリを表示します。 詳細については、以下を参照してください。 「グループ詳細画面」84 ページ

6.2.4 グループ詳細画面

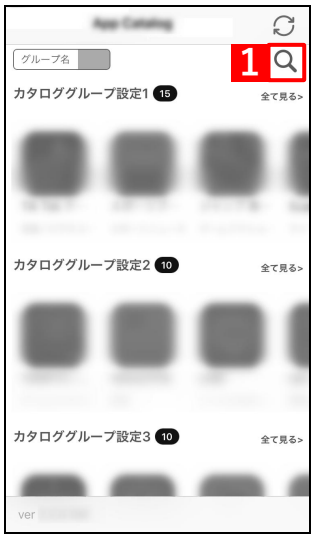
項番	名称	説明
1	アプリ名	アプリをソートします。長押しでソートの種類を切り替えます（更新日、アプリ名）。
2	🔍［検索］	グループ内のアプリについて検索を行います。🔍 をタップすると検索欄が表示されます。 🔍 検索するアプリ名を入… キャンセル 前方一致検索のみとなります。
3	［同期］	グループ内の Safety Manager App Catalog の情報を同期します。

6.2.5 全体検索を行う

【1】［全体検索］をタップします。

検索は前方一致のみです。

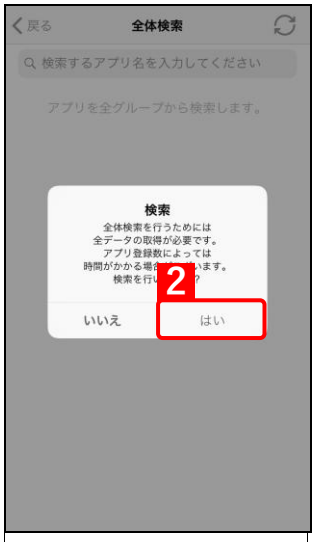
初回検索時は、手順【2】へ進んでください。



【2】［はい］をタップします。

検索前にすべてのアプリの情報を取得します。時間がかかる場合がありますのでご注意ください。

初回検索時のみ表示されます。



【3】情報取得の進捗状況が表示されます。情報取得完了後、検索を行うことができます。

6.2.6 Safety Manager App Catalog からアプリをインストールする

【1】任意のアプリをタップします。

⇒アプリの詳細が表示されます。

情報取得完了後、検索を行うことができます。

アプリの配信方法にしたがって、(A) アイコンが表示されます。

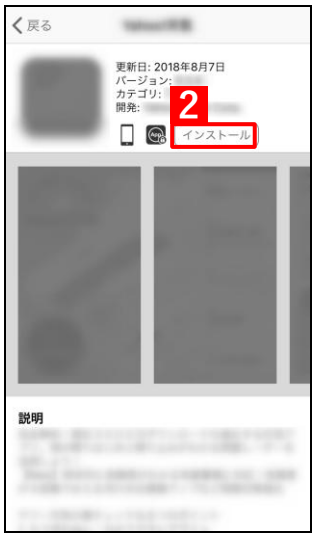
・App Store（ ）：App Store 登録されているアプリ。
・App とブック：「App とブック」ライセンス購入済アプリ。
・インハウス：In-House アプリ。
・管理対象（ ）：管理対象アプリ。

省データモードを設定している iOS 13.1 以上の端末に管理対象アプリを配信した場合は、サイレントインストールは行われません。端末のホーム画面にグレーアウトした「待機中」アイコンが表示されます。アイコンをタップしてインストールを行ってください。

【2】［インストール］をタップします。

⇒［インストール］から［更新待ち］に表示が変わります。

アプリのインストール状況を確認するには［同期］をタップします。
インストールが完了すると、［インストール済み］と表示されます。



6.2.7 Safety Manager App Catalog からアプリを更新する

Safety Manager App Catalog からインストールしたアプリのアップデート方法は、アプリの種類や状態によって以下の 3 通りあります。

●非管理対象のアプリをアップデートする

●管理対象のアプリをアップデートする

●強制アップデートする

6.2.7.1 非管理対象のアプリをアップデートする

非管理対象のアプリは、ボタン名が［再インストール］と表示されます。バージョンアップが必要な場合は、［再インストール］から手動でアップデートを行います。

【1】［再インストール］をタップします。

【2】バージョンアップ対象アプリの場合は、［アップデート］が表示されます。

⇒［アップデート］をタップします。

バージョンアップがない場合は、［開く］が表示されます。

6.2.7.2 管理対象のアプリをアップデートする

管理対象のアプリは、ボタン名が［アップデート］と表示されます。バージョンアップが必要な場合は、［アップデート］から自動でアップデートを行います。

【1】［アップデート］をタップすると、アップデートが開始されます。

6.2.7.3 強制アップデートする

以下の場合、強制アップデートができます。

●ステータスボタンが「インストール済み」または「更新待ち」の場合

●App Store アプリ、B2B アプリ、「App とブック」アプリのいずれかの場合

●管理対象アプリポリシーの「バージョンアップ要求を許可する」が有効の場合

『管理サイト リファレンスマニュアル』の「設定－iOS」－「アプリケーション」－「管理対象アプリポリシー」

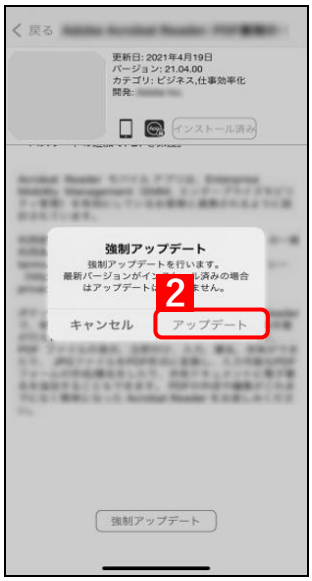
App Store に最新バージョンがリリースされているアプリの表示が「インストール済み」の場合は、［強制アップデート］でアップデートを行ってください。

App Store を「App とブック」からインストールしている場合は、「App とブック」ライセンスが割り当たっている状態で、強制アップデートを行ってください。

【1】アプリの詳細を表示します。一番下までスクロールして［強制アップデート］をタップします。

端末にインストールされている App Store アプリが、既に最新バージョンの場合は［強制アップデート］をタップしてもアップデートされません。

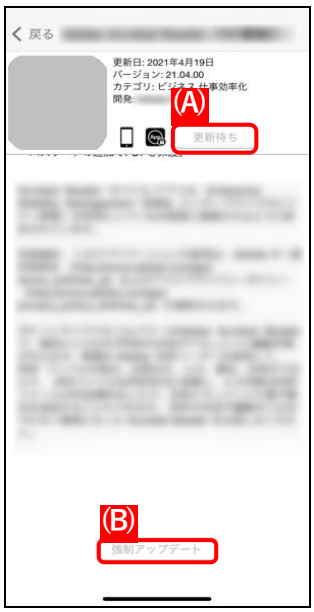
【2】強制アップデートの確認が表示されます。［アップデート］をタップします。



【3】アップデートをしています。しばらくお待ちください。

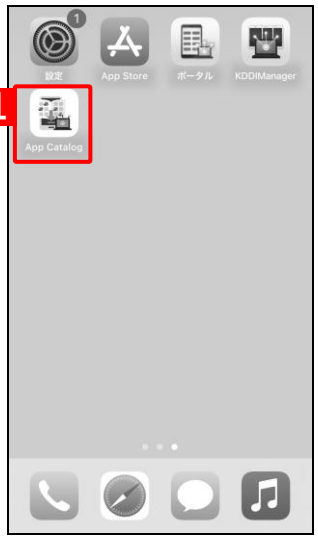
【4】アップデートが完了しました。

強制アップデートが成功すると、ステータスボタンが（A）［更新待ち］になり、（B）［強制アップデート］が非活性になります。一定時間経過すると、再び活性化されます。



6.2.8 Safety Manager App Catalog をアンインストールする

【1】アイコン（App Catalog）を長押します。



【2】［App を削除］をタップします。

⇒確認画面が表示されます。

【3】［App を削除］をタップします。

⇒アンインストールされ、アイコンも削除されます。