KDDI Smart Mobile Safety Manager
FAQ マニュアル

最終更新日　2019 年 4 月 25 日

Document ver1.15

（Web サイト ver.9.6.0）

変更履歴

日付	ver	変更箇所	変更内容
2016/11/29	1.00	全体	新規作成
2016/12/22	1.01	管理サイト FAQ	管理サイト FAQ 追加
		全体	記載の揺れを統一化
2017/1/26	1.02	全体	「参照」、「以下」等に係る記載揺れの統一
2017/2/24	1.03	全体	参照先の記載を修正
2017/4/20	1.04	Android エージェント FAQ	Android エージェント FAQ 追加
2017/5/23	1.05	管理サイト FAQ	iOS の対応バージョンの記載に係る修正・削除
2017/6/22	1.06	管理サイト FAQ	管理サイト FAQ 追加
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 新規追加
2017/7/10	1.07	管理サイト FAQ	管理サイト FAQ 追加
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 追加
		4G LTE ケータイ エージェント FAQ	4G LTE ケータイエージェントサイト FAQ 追加
2017/8/21	1.08	管理サイト FAQ	管理サイト FAQ 追加
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 追加
2017/8/23	1.09	管理サイト FAQ	管理サイト FAQ 修正
		iOS エージェント FAQ	iOS エージェント FAQ 修正
2017/10/11	1.10	管理サイト FAQ	管理サイト FAQ 修正
		Android エージェント FAQ	iOS エージェント FAQ 修正
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 新規追加
2017/11/10	1.11	管理サイト FAQ	管理サイト FAQ 新規追加、修正
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 新規追加、修正
		4G LTE ケータイ エージェント FAQ	4G LTE ケータイ エージェント FAQ 修正
2018/1/12	1.12	管理サイト FAQ	管理サイト FAQ 修正
		Android エージェント FAQ	Android エージェント FAQ 修正
		iOS エージェント FAQ	iOS エージェント FAQ 修正
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 修正
		全体	「アプリ」を「アプリケーション」に記載統一
2018/4/5	1.13	管理サイト FAQ	管理サイト FAQ 修正
		iOS エージェント FAQ	iOS エージェント FAQ 修正

日付	ver	変更箇所	変更内容
		4G LTE ケータイ 管理サイト FAQ	4G LTE ケータイ管理サイト FAQ 修正
2018/12/13	1.14	全体	参照先マニュアルを新デザインマニュアルに修正 管理サイトの表示メニューなどを新デザインの画面に統一
2019/4/17	1.15	全体	文言の統一
		管理サイト FAQ	QA103～QA111 追加
		Android エージェント FAQ	QA10 追加
		iOS エージェント FAQ	QA7 追加
		4G LTE ケータイ 管理サイト FAQ	QA31～QA37 追加

1 はじめに

本マニュアルは、FAQ として、よくある質問と回答を記載します。

2 よくある質問と回答

2.1 管理サイト FAQ

Q1　管理サイトが開けません。

A1　1. インターネットに接続できていますか。
管理サイトを使用するにはインターネットへ接続できている必要があります。
ご利用のパソコンがインターネットに接続できているかご確認ください。

2. ご使用のパソコンが動作環境を満たしていますか。
本製品の動作環境は、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「KDDI Smart Mobile Safety Manager とは」ー「管理サイト動作環境」

Q2　入力するログイン情報がわかりません。

A2　KDDI 法人お客さまセンターにお問い合わせください。

Q3　「ログイン状態を保持」にチェックを入れたが、自動的にログインされません。

A3　自動的にログインする期間は「ログイン状態に保持」にチェックを入れてから 14 日間です。14 日間を過ぎると、再度入力が必要となります。また、1 度ログアウトすると、自動的にログインする機能は無効となります。再度、ログイン情報を入力し、ログインを行ってください。

Q4　ユーザーが新規に登録できません。

A4　ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証は行なえません。
お申し込みライセンス数は、ダッシュボードの契約情報で確認できます。

Q5　機器を紛失してしまったので、至急リモートロックしたいです。

A5　以下の手順に従って、リモートロックを行ってください。

≪4G LTE ケータイの場合≫

1. ［機器］からロックする機器を選択します。
2. 画面右の［所有者の機器］より［ロックする］をクリックします。詳細は、以下を参照してください。

『Apple Business Manager(ABM) 運用マニュアル』の「機器にロックをかける」

≪iPhone／iPad の場合≫

1. ［機器］→［一覧］からロックする機器を選択します。
2. 「操作」の「リモートロック」をクリックし、ロックする設定を行ってください。
3. ［実行］をクリックします。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「機器」－「一覧」－「機器の操作」－「（操作－iOS）リモートロック」

≪Android 端末の場合≫

1. ［機器］→［一覧］からロックする機器を選択します。
2. 「操作」の「リモートロック」をクリックし、ロックする設定を行ってください。
3. ［実行］をクリックします。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「機器」－「一覧」－「機器の操作」－「（操作－Android）リモートロック」

≪Windows の場合≫

1. ［機器］→［一覧］からロックする機器を選択します。
2. 「操作」の「リモートロック」をクリックし、ロックする設定を行ってください。
3. ［実行］をクリックします。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「機器」－「一覧」－「機器の操作」－「（操作－Windows）リモートロック」

Q6　Android 端末の対応機種を知りたいです。

A6　『+Setting Safety Manager 動作状況』を参照してください。

画面右下に表示されている マニュアル をクリックし、マニュアルページよりご覧ください。

Q7　インポート時に「413 Request Entity Too Large」というエラー画面が表示されました。

A7　インポートファイルのサイズがオーバーしています。

インポートできるファイルサイズは 10MB までです。ファイルサイズを 10MB 以下にし、インポートし直してください。

Q8　連絡先配信機能は、何の項目をキーにしてAndroid端末の電話帳に登録していますか。

A8　以下の項目をキーにしています。

・姓

・名

・電話番号

以上の項目がすべて同じデータが既にAndroid端末に存在する場合はそのデータを登録することはできません。

Q9　連絡先配信機能で、連絡先の変更や削除はできますか。

A9　基本プランの場合、連絡先の変更や削除はできません。

4G LTE ケータイプランの場合、共有アドレス帳機能を利用することにより、連絡先の変更及び削除が実施可能です。

（エージェントアプリのバージョンが　v.7.4.200以前では対応していません。）

Q10　1件の連絡先に複数の電話番号やメールアドレスを登録できますか。

A10　基本プランの場合は、1件の連絡先に登録できる電話番号やメールアドレスは1つまでです。

同じ人の複数の電話番号等を登録する場合は、連絡先を複数設定する必要があります。

4G LTE ケータイプランの場合は、電話番号とメールアドレスは3つまで登録可能です。

（エージェントアプリのバージョンが　v.7.4.200以前では対応していません。）

Q11　すでに設定セットが適用されている管理対象端末に、別の設定セットを適用させるとどうなりますか。

A11　新たに設定したものが上書き適用され、設定内容が変更されます。

ただし、iOSの場合は削除禁止設定にした構成プロファイルをインストールした端末へ、別の削除禁止設定にした構成プロファイル配信すると、手順によって構成プロファイルが消失したり一部機能の上書きが発生します。詳細は以下URLでご確認ください。

https://www.optim.co.jp/promotion/smsm/pdf/profilesettingnotice.pdf

Q12　アプリケーション禁止を行ったら、禁止していないアプリケーションも使用できなくなりました。

A12　アプリケーション禁止を行うと、禁止したアプリケーションの機能を使用するアプリケーションも使用できなくなります。

Q13　カメラの制限を行ってから、使用できなくなったアプリケーションがあります。

A13　OSがAndroid4.0未満の場合は、カメラの制限を行うと、カメラを使用するアプリケーションも使用できなくなります。

Q14　スクリーンロックの設定をかけた後、再度「端末の設定を変更しない」の状態に戻してもロックされてしまいます。

A14　「端末の設定を変更しない」は、端末の今の設定から変更を行いません。以前に設定したものがあればそちらの設定が残ります。「制限なし」にチェックを入れたスクリーンロックの設定セットを作成し設定すると、ロックがかからないようになります。

Q15　iPhone／iPadの構成プロファイルが削除されたことを確認する方法はありますか。

A15　以下、条件をすべて満たす場合は、管理サイトで確認できます。

・構成プロファイルインストール時に、管理サイトのバージョンが4.4以降であった場合

・構成プロファイルの削除時に、管理サーバーとつながっていた場合

構成プロファイルが削除されると、機器-管理の通信日時の末尾に「（管理外）」と付加され、赤字で表示されます。上記条件を満たさない場合は、端末の最終通信時間から判断してください。更新プロファイルが削除された端末とは通信が行われないため、最終通信時間が更新されません。

Q16　ウイルス対策ソフトの保護状態が、管理サイトと端末で異なっています。

A16　1.　以下のいずれかに該当する場合は端末側でのみ「保護されていません」と表示されます。

・リアルタイムスキャンを“無効”とした設定セットを適用している場合

・パターンファイルアップデートを“なし”とした設定セットを適用している場合

・手動検索を一度も実行（要完了）していない場合

2.　以下のいずれかに該当する場合は管理サイト側でのみ「保護されていません」と表示されます。

・「パターンファイル最終更新チェック日時」が「状態取得日時」の15日以上前である場合

・「スキャン最終実行日時」が「状態取得日時」の15日以上前である場合

Q17　機器にどんな設定を割り当てているか確認できますか。

A17　機器ごとの設定画面で適用指示を行った設定セット名の確認ができます。

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「機器」ー「機器の設定」ー各 OS を参照

ただし、指示内容が反映済みかどうかは確認できません。

Q18　誤ったApple Push証明書を登録してしまいました。

A18　再度正しいApple Push証明書をご登録し直してください。

そのときには、Apple Push証明書をご登録されたときに利用いただいたApple IDでログインしてください。

ただし、同期不可検知または管理外検知が表示されている場合には、Q19を参照してください。

Q19　同期不可検知、または管理外検知が表示されてしまいました。

A19　以下の手順に従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が表示されている場合≫

最初に登録したApple IDとは別のApple IDでApple Push証明書を登録している可能性があります。

MDM構成プロファイルを削除し、再認証を行ってください。

DEP端末の場合、再認証を行えないため、端末初期化を行ってください。

≪エージェント同期不可検知日時が表示されている場合≫

エージェントアプリケーションの再認証を行ってください。

Q20　iOS：アプリケーション配信
オリジナルアプリ配信時に必要なマニフェストファイル（plist）について。
アプリケーション作成時に作成したマニフェストファイル（plist）と配信用のマニフェストファイル（plist）の差分があるのでしょうか。

A20　アプリケーション作成時に作成されたマニフェストファイル（plist）を利用して、アプリケーション配信用のマニフェストファイル（plist）を作成しています。
作成した配信用のマニフェストファイル（plist）にはアップロード先のURLを追記しています。
オリジナルアプリ登録画面のマニフェストファイル（plist）には、配信用のマニフェストファイル（plist）を登録いただくことで、オリジナルアプリのアプリケーション配信をご利用いただけます。

Q21　iOS：アプリケーション配信
オリジナルアプリのアプリケーション名をバージョンアップのタイミングで変更したいです。

A21　以下の手順で、オリジナルアプリケーションのバージョンアップのときにアプリケーション名の変更が可能です。手順は二通りあります。

1. 既に配信しているアプリケーション（ipa）およびマニフェストファイル（plist）と、アプリケーション名変更後のアプリケーション（ipa）およびマニフェストファイル（plist）にあるBundle IDを、同一の値に設定してください。
   このBundle IDが、管理画面でマニフェストファイル登録時に表示される「アプリケーションID」と同一のものになります。

≪配信用マニフェストファイルをアップロードして変更する場合≫

2. 1.で設定したアプリケーション名変更後のアプリケーション（ipa）とマニフェストファイル（plist）を［オリジナルアプリ登録］の右上にある［アプリアップロード］からアップロードします。
3. アップロード後、作成された配信用マニフェストファイル（plist）をダウンロードします。
4. 作成していたバージョンアップ前のアプリケーションの設定セットの［編集］をクリックし、「マニフェストファイル」の「アップロード」にチェックを入れ、［参照］で3.でダウンロードしたマニフェストファイルを指定し、保存します。

≪ipaファイルをアップロードして変更する場合≫

2. バージョンアップ前のアプリケーションの設定セットの［編集］をクリックし、「ipaファイル」の「アップロード」にチェックを入れ、［参照］でアプリケーション名を変更したアップデート用のipaファイルを指定し、保存します。

Q22　iOS：アプリケーション配信
アプリケーション配信機能で、最新バージョンのアプリケーションを配信させることはできますか。

A22　アプリケーション配信機能では、「Store IDで指定したアプリケーションを配信する」機能になります。どのバージョンが配信されるかについては、Apple社側の仕様に準じます。

Q23　iOS：アプリケーション配信

オリジナルアプリの配信方法について、マニフェストファイル（plist）なしで配信できますか。

A23　マニフェストファイル（plist）なしで配信できます。

オリジナルアプリ登録で、「ipaファイルをアップロード」を選択することで、同封されているマニフェストファイルを自動で登録することができます。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」－「オリジナルアプリ登録」

Q24　iOS：アプリケーション配信

“マニフェストファイル「XXXX.plist」は不正です”と表示されましたがどうしたらよいでしょうか。

A24　マニフェストファイルの以下の値のいずれかが正しくない可能性があります。

値の見直しを行ってください。

・bundle-identifier

・bundle-version

・title

Q25　iOS：VPP

VPP配信に失敗します（MCMDMErrorDomain:12064）。

A25　VPPアプリの配信に失敗する原因によって、対応が異なります。該当の手順に従って対応してください。

≪iTunes Storeアカウントハッシュが異なっている場合≫

VPPアプリの配信ができない原因として、iOS機器とユーザーのiTunes Storeアカウントハッシュが異なっている可能性があります。

iOS機器に設定されているApple IDが、VPP招待時に利用したApple IDと異なる場合、VPPアプリの配信ができません。

iTunes Storeアカウントハッシュの確認方法はそれぞれ以下になります。

1. iOS機器の確認方法
   （1）［機器］→［一覧］画面→対象のiOS機器→ ⓘ を選択
   （2）「情報」の［他の情報を見る］→［デバイス］をクリックし、「その他の情報」パネルの「iTunes Storeアカウントハッシュ」を確認
2. ユーザーの確認方法
   （1）［ユーザー］→［一覧］画面から対象のユーザーを選択
   （2）［VPP設定］を選択し、「参加済みのiTunes Storeアカウントハッシュ」を確認

iTunes Storeアカウントハッシュが異なっている場合、ユーザーのVPP設定画面に［参加依頼再実行］ボタンが表示されます。ボタンをクリックしたあと、端末側で参加依頼に同意していただいたあとに、VPPアプリの配信を再度お試しください。

≪VPPへの参加依頼が正常に終了していない場合≫

管理画面のログに「MCMDMErrorDomain:12064」のエラーコードが表示された場合の原因として、VPPへの参加依頼が正常に終了していない可能性があります。

以下の手順で、VPP設定の「参加依頼のステータス」をご確認ください。

1. ［ユーザー］→［一覧］画面から対象のユーザーを選択
2. ［VPP設定］を選択し、「参加依頼のステータス」を確認
3. 参加依頼の手続きが終了していると「参加済み」が表示され、終了していないと「参加依頼中」が表示されます。

Q26　iOS：VPP

VPP配信で、「MCMDMErrorDomain:12026」が発生します。

A26　本エラーが発生した場合、以下をお試しください。

1. 配信対象のアプリケーションが100MBを超えている可能性があります。サイズが100MBを超えるものを配信する場合は、Wi-Fi環境へ接続してください。
2. 対象のiOS機器を再起動（電源OFFして電源ONにする）してください。

Q27　iOS：構成プロファイル

App Storeからアプリケーションがインストールできません。

A27　非監視対象の端末で、App Storeからアプリケーションがインストールできない場合、構成プロファイルの以下の設定値を確認することで解決する場合があります。

・「許可されるコンテンツレーティング/App」の項目

こちらが、「Appを許可しない」という設定になっていると入手できるアプリケーションのレーティングに該当し、インストールができなくなります。

Q28　iOS：構成プロファイル

構成プロファイルのWebフィルタリング機能とSMSMの設定テンプレートにあるWebフィルタリング機能の違いは何でしょうか。

A28　構成プロファイル内の「Webフィルタリング」に関しては、Safariに対する制限機能になります。

設定テンプレート内の「Webフィルタリング」に関しては、+browser Safety Managerに対しての制限機能になります。

Q29　iOS：構成プロファイル

複数の構成プロファイルを適用させたときに競合が発生した場合、端末ではどのような挙動になりますか。

A29　複数の構成プロファイルを適用させた場合、パスコード・制限等のセキュリティに関する設定項目はすべてマージされます。設定が異なる項目については、セキュリティがより厳しいほうが採用されます。

例）

構成プロファイルA：

・Appのインストールを許可「しない」

・カメラの使用を許可「する」

構成プロファイルB：

・Appのインストールを許可「する」

・カメラの使用を許可「しない」

例題のような内容の「構成プロファイルA」と「構成プロファイルB」を配信する場合、適用後の機器側の状態は、以下のようになります。

・Appのインストールを許可「しない」

・カメラの使用を許可「しない」

Q30　iOS：構成プロファイル

構成プロファイルのインストールに失敗します。（※監視対象と非監視対象による設定項目の差分がある場合）

A30　構成プロファイルの設定項目により、配信可能となる端末が監視対象の端末と、非監視対象の端末と分かれる場合がありますので、ご注意ください。

構成プロファイルの設定項目には、監視対象の端末にのみ適用できる項目が存在します。

（監視対象端末のみ適用可能な項目の詳細は、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「設定ーiOS」ー「構成プロファイル」ー「構成プロファイルアップロード」

監視対象の端末にのみ適用可能な項目にチェックを入れた状態で、非監視対象の端末に配信しようとすると、構成プロファイルのインストールに失敗します。

ただし、［制限］タブ内のペイロードについては、監視対象端末のみが対象の項目を非監視対象端末に配信しても、設定が無効なだけで構成プロファイルのインストール自体は成功します。

Q31　iOS：構成プロファイル

構成プロファイルのインストールに失敗します。（※矛盾する設定を含んでいる場合）

A31　構成プロファイルの設定項目内で相反する設定を含んでいる構成プロファイルを配信するとインストールに失敗します。

例えば、以下の設定をした場合に発生します。

・制限タブ ＞パスコード変更を許可しない

・パスコードタブ ＞ 任意の制約を含める

Q32　iOS：アプリケーション配信

ポータル内でアプリケーション一覧が表示されません。

A32　1. ポータル表示、アプリケーション配信設定をしていますか。

2. 設定していても、以下に当てはまる場合は表示されませんのでご注意ください。

・対象のアプリケーションが、B2Bアプリケーションの場合、表示されません。

・管理サイトのアプリケーション一覧で、対象アプリケーションの管理が有効になっている場合、自動でアプリケーションがインストールされるため、ポータルの配信アプリケーション一覧には表示されません。

Q33　iOS：アプリケーション配信
アプリケーションのバージョンアップを個別（端末ごと）に配信する方法はありますか。

A33　バージョンアップを行うポリシーが設定された「アプリケーション配信」設定と、ポリシーの設定されていない「アプリケーション配信」設定を用意し、端末ごとに切り替えることで実現可能です。

1. アプリケーション配信で、設定A「バージョンアップする」と設定B「バージョンアップしない」を作成します。
2. 設定Aには、「自動的にバージョンアップする」の設定されているポリシーを設定します。
3. 設定Bには、「自動的にバージョンアップしない」の設定されているポリシーを設定します。
4. バージョンアップを行いたい機器には設定Aを、バージョンアップをさせたくない機器には設定Bを設定します。

Q34　iOS：アプリケーション配信
SIMを差し替えた場合、どのような影響がありますか。

A34　設定はSIMではなく端末（IMEI等）に紐づいているため、SIMを差し替えても端末に反映している設定には影響ありません。

Q35　iOS：アプリケーション配信
エージェントアプリをタップしたら「このアプリケーションは〇〇が管理されています」というようなポップアップが表示されるのですがどういう契機ですか。
※〇〇は管理サイトに登録している企業名です。

A35　手動でインストールしたアプリケーションを、あとからSMSMから「管理」にチェックを付けた状態で配信した場合に、ポップアップが表示します。

以下の2点にご注意ください。

1. 監視対象モードでない端末の場合のみ表示されます。
2. 監視対象モードの端末の場合、ポップアップは表示されず、強制的にSMSMから配信した状態になります。

Q36　iOS：アプリケーション配信
OSのバージョンアップを管理サイトから行えますか。

A36　管理サイトからOSのバージョンアップは行なえません。

Q37　iOS：Apple Push証明書
Apple Push証明書を削除してしまい、新しい証明書をセットしました。
その後、同期がとれなくなったので、元に戻し、元の証明書を更新しました。
それでも同期不可という表示になり、端末との同期もとれないのですがどうしたらよいでしょうか。

A37　管理サイトから証明書が削除され、1日経過してしまうと同期不可になってしまいます。
そのため、同期不可の状態を改善するには端末を再認証していただく必要があります。

Q38　iOS：Apple Push証明書

Apple Push証明書を発行しようとしたらApple側のサイトの表示がおかしいです。

A38　利用するブラウザによって表示が変わるようです。

ブラウザによって改善することがありますので、お試しください。

※InternetExplorer、GoogleChromeでは利用に影響があることがあります

Q39　iOS：Apple Push証明書

Apple IDが分からなくなったため、別のApple IDで新しいApple Push証明書を作成し適用させたいのですが、どういう影響がありますか。

A39　登録されているすべてのiOS端末で再認証をしていただく必要があります。

更新時には、更新前に利用したApple IDおよびApple Push証明書をご利用いただくことをお勧めします。

Q40　iOS：Apple Push証明書

登録済みとは別のApple Push証明書を適用後、一部の端末が管理外になりました。

再度、登録済みと同じApple IDで取得した証明書に差し替えを行い、トピック値は同じになりましたが、管理外のままでした。

どうしたらよいでしょうか。

A40　管理外になった原因は異なるトピック値の証明書がアップロードされたことにより、同期ができなくなったことが検知されたためになります。同じトピック値の証明書に更新した場合、端末から手動同期を行うと再び管理の状態になります。

Q41　iOS：Apple Push証明書

Apple IDのサイトで、「MDMプロファイルトピック」と同一のUID値の証明書が見当たらないのですがどうすればよいですか。

A41　Apple IDのログイン情報が異なっていると思われます。Apple IDの確認をお願いいたします。

Q42　iOS：Apple Push証明書

「機器「〇〇」のMDM構成プロファイルについて同期ができなくなりました。機器の再認証を行ってください。」という、ログが表示されましたがどうしたらよいですか。

※〇〇には管理サイトで登録している機器名が表示されます。

A42　以下の理由が考えられます。

1. Apple Push証明書の更新に失敗した。

   ※証明書を削除した、誤ったApple IDで登録した場合を含みます。

2. 端末側で、MDM構成プロファイルを削除した。

Q43　Android：アプリケーション配信

閉域網利用の環境下で、アプリケーション配信でアップデートを行ったところ、一部の端末ができなかったのですが、何が原因でしょうか。

A43　閉域網環境下でご利用の場合、端末で以下の設定が行われていないと、アプリケーション配信が行われない場合があります。

1. Androidの設定を選択します。
2. 一覧からGoogleを選択します。
3. セキュリティの項目を選択します。
4. アプリケーションの確認を選択します。
5. 各項目のスイッチをOFFに設定します。
   ※OSや端末毎に設定手順が変わる可能性があります。

Q44　Android：ウイルス対策オプション

ウイルス対策ソフトをアップデートしようとしています。
端末で提供元不明アプリの許可を設定しないとアップデートできませんか。

A44　オプション提供のウイルス対策ソフトをアップデートする場合、端末の提供元不明アプリの設定をONにしていただく必要があります。

Q45　Android：ウイルス対策オプション

管理サイトではウイルス対策の設定を作成したのですが、ウイルス対策のインストールが通知されず、App Managerに表示されないのですがどうしたらよいですか。

A45　機器に「ウイルス対策」のパッケージが適用されていない可能性があります。
以下の手順でご確認ください。

1. 管理サイト「機器」より対象の機器を選択します。
2. 「パッケージ」を選択し、［編集］をクリックして「ウイルス対策」にチェックを入れます。

Q46　Device Owner Modeを使用しない場合、どういったデメリットがありますか。

A46　Android 7以降でDevice Owner Modeに対応しています。
Device Owner Modeを未使用の場合、以下の制限・利用ができなくなります。

1. 利用者によるエージェントアンインストールができるようになります。
   （アンインストール抑止ができません）
2. スクリーンロックパスワード変更ができなくなります。

Q47　iOS：Apple Push 証明書

更新前と違う Apple ID で証明書更新後、正しい Apple ID で再度証明書を更新したのですが、管理サイトを見ると、同期不可となっている機器があります。どうしたら解消されるのでしょうか。

A47　更新前と異なる証明書を管理サイトへセットし、時間が経過すると以前使用していた証明書に紐付いていた端末は、同期不可となります。
解消するには端末側で再認証をしていただく必要があります。

Q48　iOS：構成プロファイル

構成プロファイル配信後に、iOS 端末側で Wallet が起動できなくなりました。回避方法を教えてください。

A48　Apple 社の仕様により、Passbook から Wallet と名称変更されていることが影響してます。

構成プロファイルの制限設定にある「ロック画面で Passbook 通知を許可」という項目を禁止すると、「ロック画面での Wallet 通知を許可」を禁止することになり、その結果、iOS 端末側で Wallet が起動できなくなります。

Wallet が起動できなくなる事象を回避するためには管理サイトの構成プロファイルの制限設定にある「ロック画面での Passbook 通知を許可」にチェックを入れてください。

Q49　iOS：アプリケーション配信

管理サイトの機器ログに、MCMDMErrorDomain:12040 というエラーログが表示された場合はどうしたらよいでしょうか。

A49　該当の端末が、「iTunes Store と App Store」に Apple ID でサインインされていないため、アプリケーション配信が機能せずこのエラーが発生します。

端末側の「iTunes Store と App Store」へのサインイン状況をご確認ください。

Q50　iOS：Web フィルタリング

基本機能にある Web フィルタリングとオプションの Web フィルタリングの違いを教えてください。

A50　iOS 端末で利用できる基本機能の Web フィルタリングとオプションの Web フィルタリングには、以下の違いがあります。

≪基本機能の Web フィルタリング機能≫

利用前提：端末を監視対象モードにしていただく必要があります。
ブラウザは Safari を利用していただく必要があります。

機能：URL 指定によるホワイトリスト、ブラックリストの設定が可能です。

≪オプションの Web フィルタリング機能≫

Web フィルタリング機能が利用できるオプションは以下の二つがあり、それぞれで以下のようになっております。

1. インターネット接続管理

利用前提：ブラウザは専用の「+browser Safety Manager」を利用していただく必要があります。
また、エージェントアプリ「KDDI Smart Mobile Safety Manager」をインストールしていただく必要があります。

機能：URL によるホワイトリスト、ブラックリストの設定が可能です。

2. Web フィルター

利用前提：ブラウザは専用の「+browser Safety Manager」を利用していただく必要があります。
また、エージェントアプリ「KDDI Smart Mobile Safety Manager」をインストールしていただく必要があります。

機能：URL 指定によるホワイトリスト、ブラックリストの設定のほかに、カテゴリ指定によるホワイトリスト、ブラックリストの設定が可能です。

Q51　Android：Android N 対応

Android のバージョンを 7 にアップグレードすると「動作が停止しました。」という現象が起きてしまいますが、どうしたらよいでしょうか。

A51　エージェントアプリのバージョンが「8.1.202.0」未満の場合は Android 7 に対応していないため、動作が停止、または終了してしまいます。

Android 7 にバージョンアップし、エージェントアプリのバージョンが「8.1.202.0」未満で「動作が停止しました。」と表示が出てしまう場合には、エージェントアプリの再インストールをお願いいたします。

Q52　アプリケーション配信で配信したアプリケーションをインストール中に「スキャンできませんでした」というエラーが表示され、ダウンロードまでは問題ありませんがインストールができません。

A52　エラーは、「Lookout for au」というセキュリティソフトによるものです。

回避策として、ダウンロード後に表示される、端末の通知画面からインストールを実施してください。

SMSM で提供しているアプリケーション（ウイルス対策オプションにより配信されるウイルス対策アプリ、インターネット接続管理オプションや Web フィルターオプションにより配信される +browser safety manager アプリ等）は App Manager を利用してインストールを実施してください。

Q53　iOS：Exchange 設定

iOS 端末へ配信した Exchenge アカウント設定のパスワードも変更したが、反映されていません。

どうしたらよいでしょうか。

A53　Apple 社側の不具合により、iOS10 以上の場合、パスワードを更新したプロファイルを配信するとパスワードが消えてしまう事象が発生します。

回避策ですが、現在行っている Exchange 設定を以下の手順で再設定してください。

≪機器ごとに行う場合の削除手順≫

1. SMSM管理サイトの［機器］→［一覧］からExchange設定を行っている端末→ ⓘ を選択する
2. 「設定」の「他の設定を見る」→［Exchange（ActiveSync）設定］をクリックする
3. ［削除］をクリックする
4. 確認画面で［OK］をクリックする
5. 同期を行う

≪機器インポートを使い複数機器同時で行う場合の削除手順≫

1. SMSM管理サイトの［機器］→［CSVで編集］に移動する
2. 「1. CSVファイルを準備します」の ［ダウンロード］をクリックする
3. ダウンロードしたCSVファイルの“［S:iOS:Exchange］Exchange ActiveSync ホスト”から“［S:iOS:Exchange］メールのみで使用”の列の値を削除して保存する
4. SMSM管理サイトの［機器］→［CSVで編集］にある「2. CSVファイルをアップロードします」の［ファイルを選択］をクリックし、編集したCSVファイルを選択する
5. ［アップロード］ボタンをクリックする
6. 同期を行う

Q54　iOS：Web クリップ

削除してしまった Web クリップアイコンを元に戻したいのですが、どうしたらよいでしょうか。

A54　Apple Configurator で作成された Web クリップを管理サイトにアップロードしてご利用されている場合、その Web クリップの構成プロファイルが削除可能な設定ですと端末上で Web クリップが削除可能となります。管理サイトの構成プロファイルアップロード画面で Web クリップを作成、もしくはアップロード後一度編集いただいた場合は端末内にある、配信された Web クリップアイコンは削除できません。

Apple Configurator を使用して作成した Web クリップを再度端末に表示させるためには、以下の手順で対象の構成プロファイルの編集を行ってから、対象端末の構成プロファイルの設定を変更し、同期を行ってください。対象端末のみ設定変更を実施せず、大元の構成プロファイルを変更しただけの場合は、全端末に設定が反映されるため、ご注意ください。

Web クリップをインストールさせるためには上記 ID を変更させる必要がありますので、以下の手順を実施してください。

≪Apple Configurator で作成した Web クリップを削除不可にする方法≫

1. 構成プロファイルアップロード画面で、対象の Web クリップ設定を開く
2. 編集ボタン押下
3. 内容を変更せずに保存実行

Q55　iOS：ホーム画面レイアウト

ホーム画面レイアウトを利用したのですが、プリインストールされているアプリケーションに関しては設定した配置になります。

しかし、VPP 配信などでインストールされたアプリケーションに関しては指定の位置にならずアイコン位置が固定されません。

A55　アプリケーション ID に、対象のアプリケーションのアプリケーション ID（bundleID）を入力する必要があります、アプリケーションのアプリケーション ID は、管理サイトから以下の方法でご確認いただけます。

≪端末のアプリケーション一覧から確認する方法≫

1. 管理サイトの［機器］→［一覧］→レイアウトを行うアプリケーションがインストールされている端末を選択する
2. 「情報」の［アプリケーション］をクリックする
3. 「アプリケーション ID」が表示される

≪アプリケーションレポート機能を利用する方法≫

1. 管理サイトの［機器］→［CSV をダウンロード］→［アプリケーションレポート］を選択する
2. 抽出条件で、iOS の「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）」にチェックを入れ、［レポート作成］をクリックする
3. レポート作成の完了後、対象のアプリケーションの「［I］パッケージ名/アプリケーション ID」の値に「アプリケーション ID」が表示される

Q56　iOS：アプリケーション配信

iOS 端末でアプリケーション配信を行うとき、利用者様の端末に Apple ID のサインイン情報を求められることがあります。

配信を行おうとしているアプリケーションは AppStore で配信されている無料の App です。

利用者の端末で ID、パスワードが求められない場合と求められる場合の違いは何になりますでしょうか。

A56　アプリケーション配信をご利用のとき、Apple ID が求められる場合と求められない場合については端末の設定状況や、配信方法によって変わります。

以下の条件になりますので、運用方針に沿った端末設定、アプリケーション配信の方法をご利用ください。

※ただし、App Store の利用規約が変更になった場合は条件に係わらず、Apple ID の入力が求められます。

≪Apple ID の入力が必要な場合≫

（1）端末の設定

設定 > iTunes Store と App Store > パスワードの設定

または

設定 > 一般 > 機能制限 > パスワードの設定

にある、「無料ダウンロード」の「パスワードを要求」が ON

a） 端末が非監視対象モード

（2）アプリケーション配信の方法

1） 配信アプリを非管理対象に設定している

a） VPP を利用しないで配信する

b） VPP をユーザー割り当てにより配信する

≪Apple ID の入力が不要な場合≫

1）端末の設定

設定 > iTunes Store と App Store > パスワードの設定

または

設定 > 一般 > 機能制限 > パスワードの設定

にある、「無料ダウンロード」の「パスワードを要求」が OFF

a） 端末が監視対象モード

（2）アプリケーション配信の方法

1） 配信アプリが管理対象に設定されている

a） VPP 利用でデバイスにライセンスを割り当てて配信する方法

b） VPP 利用でユーザーにライセンスを割り当て配信する方法

Q57　iOS：アプリケーション配信

iOS 10 以上の iPhoneSE 端末で誤ってシステムアプリ（メール/Store ID：108187098）を削除しました。
SMSM でアプリケーション配信をしたところ、エラーが表示され、再インストールできませんでした。
「App のインストールを許可：しない」の制限をかけている状態で、どうすればシステムアプリを配信できるでしょうか。

A57　すべてのプリインストールアプリ共通で Apple の仕様により、MDM からの配信はサポートしていません。
削除したプリインストールアプリを戻す方法は、非管理対象としての配信方法になります。

現在の iOS の仕様ではプリインストールアプリ（最初から端末にインストールされているアプリケーション）を「App のインストールを許可：しない」の条件で再インストールする方法はございません。
「App のインストールを許可：しない」の構成プロファイルをはずしてから、以下の方法でインストールをお試しください。

1. 管理サイトにログインする
2. ［設定］→［iOS］→［アプリケーション］をクリックする
3. ［アプリケーション配信］をクリックする
4. 以下の設定を作成/保存を実行する
   ・App Store アプリケーション一覧で作成する
   ・StoreID を入力する
   ・管理：チェックを付けない
   ・ポリシー：未選択
5. ［機器］→［一覧］→対象機器を選択→「設定」の［設定の割り当て］をクリックする
6. 上記で作成したアプリケーション配信の設定セットを選択し、［保存］をクリックする
7. 同期を実行する
8. 端末側で、ポータルを開き、アプリケーションをインストールするボタンを選択する
9. インストールボタンを選択する
10. App Store アプリが起動するため、インストールボタンを選択する
    ※端末によってはクラウドマークの場合もございます。
11. アプリケーションのインストールが完了する

Q58　iOS：VPP

VPP アプリを配布した後、アプリケーションの最新版を全端末へ配布し、更新させたい場合の手順を教えてください。

A58　以下の手順でアプリケーション配信の設定を行うことで、対象のアプリケーションの最新版を自動的に配信できます。

1. アプリケーション配信（アップデート）を作成する
2. 「管理対象アプリポリシー」を作成、以下の項目をチェックする
   ・VPP ライセンスを利用する
   ・自動的にバージョンアップする
3. ［管理］を有効にして、1.で作成したアプリケーション配信へ 2.のポリシーを割り当てる

Q59　iOS：VPP

VPP アプリを配布した後、アプリケーションの新バージョンがリリースされても、購入済みの古いバージョンを継続で利用したい場合に、アップデートさせない手順を教えてください。

A59　SMSM では、アプリケーションのアップデートをさせなくする機能はありません。

以下の手順でアプリケーション配信の設定を行うことで、対象のアプリケーションの最新版が公開されても SMSM から自動的に配信が行わないようにすることはできます。

1. アプリケーション配信（非アップデート）を作成する
2. 「管理対象アプリポリシー」を作成、以下の項目をチェックする
   ・VPP ライセンスを利用する
3. 2.で作成した「管理対象アプリポリシー」で、以下の項目はチェックを入れない
   ・自動的にバージョンアップする
4. ［管理］を有効にして、1.で作成したアプリケーション配信へ 2.のポリシーを割り当てる

Q60　iOS：アプリケーション一覧

インストールされているアプリケーションがアプリケーション一覧から消える事象が発生します。
原因を教えてください。

A60　アプリケーション配信により対象のアプリケーションがバージョンアップ中やインストール中、停止中の場合、アプリケーション一覧から消えてしまいます。

Apple 社の仕様により、アプリケーションがバージョンアップ中やインストール中、停止中の場合、iOS 端末から該当アプリケーションの情報が取得できなくなるため、一時的にアプリケーション一覧に表示されなくなります。

バージョンアップが完了後に同期が行われますと、再度、アプリケーション一覧に表示されるようになります。

Q61　Android：アプリケーション配信

インハウスアプリ（自社製アプリ）を配信したいのですが、配信はできますか。

A61　アプリケーション配信でファイル指定をしていただくことによってインハウスアプリ（自社製アプリ）を配信できます。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 - Android」ー「アプリケーション」ー「アプリケーション配信」

Q62　Android：アプリケーション配信、アプリケーション禁止

アプリケーション配信やアプリケーション禁止で対象のアプリケーションのパッケージ名とバージョン番号を確認する方法はありますか。

A62　アプリケーションのパッケージ名とバージョン番号はアプリケーションの開発元に確認していただくなど、お客様側でご確認いただく必要があります。

配信前に確認用の端末をご用意いただける場合、以下の手順で管理サイトから対象のアプリケーションのパッケージ名とバージョン番号を確認できます。

※配信前に確認用の端末をご用意いただけない場合、アプリケーションの開発元へご確認をお願いいたします。

1. ［機器］タブをクリックする
2. 対象端末を選択する
3. ［アプリ］タブをクリックする
4. 対象のアプリケーションの［詳細］をクリックする
5. パッケージ名やバージョン番号などのアプリケーション情報が表示される

Q63　iOS：構成プロファイル

音声コントロールの制限はできますか。

A63　SMSM では、音声コントロールの制限はできません。

※Apple Configurator からも音声コントロールは制限できません。

Q64　iOS：構成プロファイル

端末利用者による Apple ID の変更の制御はできますか。

A64　以下の手順を行うことにより Apple ID 変更不可の設定ができます。

1. 端末で固定化したい Apple ID でログインを行う
2. 管理サイトで［設定］→［構成プロファイル］→［構成プロファイルアップロード］から新規プロファイルを作成する
3. 「iOS 制限設定」タブを開き、「アカウント設定の変更を許可（監視対象のみ）」のチェックを外した制限を作成する
4. ［設定］→［構成プロファイル］→［構成プロファイル］で新規に作成し上記で作成した構成プロファイルを設定するか、既存の構成プロファイルに上記で作成した構成プロファイルを追加する
5. ［機器］→［一覧］→一覧より対象を選択→「設定」の［設定の割り当て］→「構成プロファイル」の［編集］から端末に構成プロファイルを割り当てる
6. 同期する

※端末で Apple ID のログインを行う前に、上記構成プロファイルを割り当てた場合、ログインができなくなりますので、ご注意ください。

Q65　iOS：アプリケーション配信

アプリケーション配信で、配信したアプリケーションを端末利用者が削除すると、改めてインストールするまで、インストールを促すポップアップが表示され続けますか。

A65　アプリケーション配信対象のアプリケーションが、端末にインストールされていない場合、同期の度にインストールを促すポップアップが表示されます。

ただし、サイレントインストールの条件を満たしていると、ポップアップは表示されずにインストールが実行されます。

Q66　iOS：アプリケーション配信

アプリケーション配信で配信したアプリケーションが端末上で待機中となりインストールできなくなりました。どうしたらよいでしょうか。

A66　以下の手順で、インストールを行っているアプリケーションを削除し、再度配信を実施してください。

1. 端末の「待機中」となっているアイコンを長押しする
2. ［×］をタップし、アプリケーションを削除する
3. 端末を同期し、再度配信を実施する

Q67　iOS：アプリケーション配信

管理側からアプリケーションを配信、削除できるようにしたいのですが、できますか。

A67　アプリケーション配信で、対象のアプリケーション配信設定の「管理」の「有効」にチェックを入れていただくことにより管理側からのアプリケーション配信ができるようになります。

また、アプリケーション配信設定で「管理」の「有効」にチェックが入っているアプリケーションの場合、機器に割り当てられているアプリケーション配信の設定を外すと、その後の同期のタイミングで端末より削除されます。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」－「アプリケーション」－「アプリケーション配信」

Q68　iOS：Apple Push 証明書

ApplePush 証明書で利用している Apple ID のメールアドレスを変更してもよいでしょうか。

A68　Apple ID の連絡先のメールアドレスを変更していただいても問題ございません。

Q69　Android：認証

エージェント認証後、ユーザー登録を行いたいが白い画面が表示されたまま止まってしまいます。どうしたらよいでしょうか。

A69　WebView を最新バージョンに更新すると改善します。以下の手順で、WebView をアップデートしてください。

1. Play ストアを起動する
   ※Google アカウントでログインする必要があります。
   Google アカウントが未登録の場合は、登録してください。
2. メニューから［マイアプリ&ゲーム］を選択する
3. 一覧から［Android システムの WebView］を選択する
4. ［更新］を選択する

Q70　Android：認証

Android 端末のライセンス認証時に表示される利用権限の要求の設定はスキップできないでしょうか。

A70　Android 6.x 以降は、OS の仕様により利用権限の要求が表示されるようになっております。

権限には、「必須権限」のものと、「任意権限」があります。

このうち、「必須権限」の項目については、設定が必須になり、権限設定をしていただかないと認証が完了しません。

この設定の操作はスキップできません。必ず、端末側で設定していただくようお願いいたします。

Q71　Android：認証

Android 端末のライセンス認証時に表示される利用権限の要求の電話権限についての各項目は、設定しないとどのような影響がありますか。

A71　電話権限の「未設定」をタップして表示される「アプリ情報」の「許可」にある各項目は、以下の機能で利用しています。

・カメラ：ライセンス認証の QR コード認証で利用します。

・ストレージ：ファイルのダウンロード先として利用します。

・位置情報：位置情報機能・Zone Management の機能で利用します。

・連絡帳：連絡先配信・設定バックアップ・復元機能で利用します。

・電話：端末識別情報取得のため利用します。こちらのみ、有効化が必須になります。

Q72　Android：アプリケーション禁止

アプリケーション禁止の設定項目に Play ストアを指定した場合、アプリケーションのアップデートは実施されるのでしょうか。

A72　Play ストアを禁止した場合、Play ストアを経由するアプリケーションのアップデートは、Play ストアアプリの設定により、次のように動作が異なります。

≪アプリケーション側で「自動アップデート」が有効の場合≫

　アプリケーション禁止で禁止していても、アップデートされます。

≪アプリケーション側で「自動アップデート」が無効の場合≫

　アプリケーション禁止で禁止している場合、アップデートされません。

Q73　iOS：DEP

管理サイトの DEP サーバートークン登録画面のアカウント情報が消えています。どうしたらよいでしょうか。

A73　Apple 社の Device Enrollment Program の利用規約が更新されている可能性があります。
これ以降、新しい利用規約に「同意」していない場合、DEP トークンのアカウント情報が取得できません。
Apple 社側のサイト（Device Enrollment Program）へログインし、利用規約の更新に伴う同意を実行されているかご確認ください。
同意しても DEP トークン登録画面のアカウント情報が表示されない場合は、以下の手順で、再度管理サイトに DEP トークンをアップロードしてください。

1. 以下のマニュアルを参照し、更新作業を行う

   『DEP サーバートークン年次更新マニュアル』

2. 管理サイトの［設定］→［iOS］→［DEP］→［DEP 危機管理］をクリックする
3. 機器が表示されることを確認する

※すべての端末を取得しますので、お時間がかかる場合がございます
※表示されない場合、［DEP サービスと同期］をクリックしてください
※登録した DEP サーバートークンを削除しないようご注意ください

Q74　iOS：DEP

DEP を利用して iOS 端末を非監視対象モードにしたいのですが、できますか。

A74　以下の手順で、監視対象モードから非監視対象モードに変更できます。

1. 管理サイトの［設定］→［iOS］→［DEP］→［DEP 定義ファイル］で、「監視対象モードに設定する」のチェックを外した「DEP 定義プロファイル」を作成する
2. ［機器］→［一覧］→一覧より対象を選択→「設定」の［設定の割り当て］→「DEP 定義プロファイル」の［編集］から端末に構成プロファイルを割り当てる
3. 対象端末の初期化を行う
4. 初期化が終了し、非監視対象モードになる

Q75　iOS：アプリケーション配信

アプリケーション配信利用時に端末のポップアップ表示に表示する企業名を変更はできますか。

A75　アプリケーション配信のポップアップ画面で表示している企業名を変更する場合は、変更申込書でのお申し込みが必要です。KDDI の担当営業にお問い合わせください。

Q76　iOS：アプリケーション配信

アプリケーション配信で配信を実施したあとに、配信設定を変えた場合、重複しているアプリケーションはどのようになりますか。

A76　すでにアプリケーション配信を実施し、その後に別の配信設定に変更したときに重複しているアプリケーションがあった場合は、重複しているアプリケーションの再インストールは行われません。

以下のような動作になります。

1. 端末 N にアプリケーション配信の「ポリシーX」にアプリケーション A、アプリケーション B、アプリケーション C を設定し、配信する
2. 端末 N に、アプリケーション A、アプリケーション B、アプリケーション C が配信される
3. 端末 N にアプリケーション配信で「ポリシーY」にアプリケーション A、アプリケーション B、アプリケーション C、アプリケーション D を設定し、配信する
4. 端末に、アプリケーション D のみ配信される

Q77　iOS：アプリケーション配信

アプリケーション配信中に端末の画面で対象のアプリケーションが「待機中」と表示される場合と、表示されない場合は何が違うのでしょうか。

A77　アプリケーション配信で配信したアプリケーションのインストール処理は、SMSM ではなく、iOS による作業であり、Apple 社の仕様によります。そのため、「待機中」の表示条件については回答できません。

Q78　iOS：アプリケーション配信

アプリケーション配信を実行してアイコンがインストール中になっていたのですがアイコンが消えました。なぜでしょうか。

A78　以下の設定になっていると、アプリケーションが配信できず、アイコンが消えてしまいます。

1. 構成プロファイルの「制限」タブにある「App のインストールを許可」の設定が「しない」になっている。
2. 1.の状態で、さらに、構成プロファイルの「制限」タブにある「App」にある「App の使用制限（監視対象のみ）」の項目が「一部の App のみを許可」になっており、配信対象のアプリケーションが登録されていない。

アプリケーション配信を利用する場合は、「App のインストールを許可」を「する」にしていただき、「App の使用制限（監視対象のみ）」の項目が「一部の App のみを許可」の場合には、配信対象のアプリケーションを登録してください。

Q79　iOS：同期

iOS 端末が管理サイトで「管理」→「通信日時 MDM（構成プロファイル）」の表示が赤字で「同期不可」となっています。どうすれば機器の同期ができますか。

A79　無通信時に MDM 構成プロファイルが削除されるなどして、APNs により同期できないことが検知された場合に、「管理」→「通信日時 MDM（構成プロファイル）」に赤字で「同期不可」が表示されます。

再び同期を行えるようにするためには、以下の手順に従って、端末側で MDM 構成プロファイルの再インストール・再認証を行っていただく必要があります。

1. 端末側の MDM 構成プロファイルのアンインストールを行う。詳細は、以下を参照してください。

『iOS クライアント リファレンスマニュアル』の「MDM 構成プロファイルのアンインストール」

2. 端末側に MDM 構成プロファイルのインストール（ライセンス認証）を行う。詳細は、以下を参照してください。

『iOS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

※DEP の設定で「端末から MDM 構成プロファイルの削除を禁止」している場合は、初期化によって MDM 構成プロファイルを削除していただく手順となります。

Q80　iOS：同期

iOS の定期同期の間隔は 8 時間とのことですが、この間隔の調整はできますか。

A80　iOS 端末と管理サイト間の定期同期の間隔の変更はできません。

Q81　Android：アプリケーション配信

アプリケーション配信でどのようにアプリケーションを配信できますか。

A81　Android のアプリケーション配信の方法はアプリケーション配信設定や端末などにより以下の方法がございます。

≪自動でアプリケーションをインストールする場合≫

（a）前提条件

・au 端末であること

・Android 6 以上であること

・アプリケーション配信設定で、対象のアプリケーションの apk ファイルをアップロードすること

（b）アプリケーション配信実施時の動作

・同期のタイミングでアプリケーション配信を実行しますが、端末利用者の操作なしでインストールできます。

≪端末側操作によりインストールする場合≫

（a）前提条件

・≪自動でアプリケーションをインストールする場合≫の前提条件以外であること

（b）アプリケーション配信実施時の動作

・同期のタイミングでアプリケーション配信を実行します。

・管理サイトのアプリケーション配信設定で「ポップアップ」にチェックがある場合は、端末側にポップアップ画面で表示します。

端末利用者はポップアップ画面で［OK］を押してください。

・画面の上から下へスライドすると、ダウンロード通知画面が表示されるので、通知をタップします。

・画面の内容に従って、インストールを行ってください。

※アプリケーション配信が実行された時の端末の手順についての詳細は、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「アプリケーションが配信された場合」

※アプリケーション配信設定についての詳細は、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 - Android」－「アプリケーション」－「アプリケーション配信」

※Play ストアでのアプリケーション配信の場合は、異なりますので、ご注意ください。

Q82　Android：アプリケーション禁止

アプリケーション禁止を設定したら起動禁止できますが、禁止したアプリケーションのアイコンを非表示にできないのでしょうか。

A82　アプリケーション禁止で禁止したアイコンを非表示にすることはできません。

Q83　Android：アプリケーション禁止

設定にも禁止制限をかけているのですが､TOP 画面の上をスライドすると GPS を OFF にできてしまいます。何か制御する方法はありますか。

A83　端末の上部をスライドさせて表示される画面（通知センター、ステータスバーなど）の各項目につきましては制御が行えません。

GPS の ON/OFF の検知の場合は、管理サイトで、次の手順で「通知設定」を設定すると管理者が検知通知を受け取れるようになります。

1. ［設定］→［サービス環境設定］→［通知設定］をクリックする
2. 「ログメール通知」の［編集］をクリックする
3. 以下を設定する
   - ・メール通知タイミング：「随時」に設定
   - ・メール通知対象ログ：位置情報設定の変更
   - ・メール送信先（カスタム）：管理者以外のメールアドレスへ送りたい場合に設定
4. ［保存］を選択する

こちらを設定していただくことによって、同期により GPS 設定の変更が管理サイトへ通知された後、数分後に対象のメールアドレスへ変更された旨の通知メールが届くようになります。

Q84　Android：スクリーンロック

Android 7 にアップデートしたあと、スクリーンロックパスワードの変更を実施しましたが、変更後のパスワードを入力してもロック解除ができません。どうしたらよいでしょうか。

A84　Android 7.0 以降の OS でスクリーンロックを利用する場合、以下の 2 つの条件が満たされている必要があります。条件が満たされていない場合、管理サイトからスクリーンロックパスワードの変更を実施しても変更できません。

- ・エージェントのバージョンが 8.1.202.0 以上である。
- ・端末が Device Owner Mode になっている。Device Owner Mode 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』

Q85　Android：スクリーンロック

スクリーンロックが実行された時に、画面にメッセージを出せますか。

A85　スクリーンロックの画面にメッセージの表示はできません。

Q86　iOS：構成プロファイル

構成プロファイルアップロードで設定できるWebフィルタリングを利用できる条件を教えてくれませんか。

A86　構成プロファイルを使ってWebフィルタリングを制限する場合、端末を監視対象モードにする必要があります。

また、構成プロファイルから設定するWebフィルタリング設定の対象ブラウザは、Safariに限らず、WebViewを実装しているサードパーティ製のブラウザー（Google Chrome、FireFoxなど）も制限対象となります。

※構成プロファイルを利用しない場合は専用ブラウザーにのみ適用されます。ご利用には「インターネット接続管理」、または「Webフィルター」オプションのご契約が必要です。

Q87　iOS：構成プロファイル

「構成プロファイル「ｘｘｘｘ」のインストールが一時的に延期されました。」というログが表示される原因について教えてほしい。

A87　端末がスリープ状態かつロックがかかっている状態の場合に本ログが表示されます。

この状態の時には、iOSの仕様により、端末に構成プロファイルはインストールされず、待機する形となります。インストールを実行させるためには、端末を起動いただき、ロックを解除していただく必要があります

Q88　エージェントのアクティベーションコードの記載場所を教えてほしい。

A88　管理サイトの［機器］→［一覧］→一覧より対象を選択→「情報」の［エージェント］をクリックすると、アクティベーションコードを確認できます。

Q89　機器名に電話番号が含まれていますが、電話番号を変えると自動で変更されますか。

A89　機器名は自動で変更されません。

電話番号を変更した場合は、管理サイトで機器名を変更してください。

「管理情報」の「電話番号」は更新されます。

Q90　機器名に電話番号ではなく IMEI が入っている機器がありますが、どうしてでしょうか。

A90　認証時に端末から電話番号が取得できなかった場合に、IMEI が機器名につきます。

SIM が挿入されていなかったか、SIM に電話番号が割り当たっていなかった可能性があります。

Q91　管理サイトから機器を削除してしまいました。

再度管理下に戻すには、どうしたらよいでしょうか。

A91　端末側の操作で再度認証していただく必要があります。

（1）　iOS の場合

MDM 構成プロファイルを上書きインストールし、再度認証を行ってください。

（2）Android の場合

エージェントアプリを起動し、ライセンス解除を行い、解除後、再度認証を行ってください。

ライセンス解除時にパスワードを求められる場合は、管理サイトの Android の「エージェント共通管理」にある項目「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」を参照ください。

Q92　管理者のユーザーID の変更をするにはどうしたらよいでしょうか。

A92　［ユーザー］→［一覧］→一覧より対象を選択→「管理情報」の［編集］から「ユーザーID」を変更できます。

変更したあとに、［保存］をクリックして変更を適用します。

Q93　iOS：DEP

DEP 端末を追加登録したときに SMSM 側に反映されません。どうしたらよいでしょうか。

A93　お客様環境の管理サイトの「DEP サーバートークン登録」画面につきまして、「アカウント情報」に「アカウント情報が取得できませんでした」と表示されているかご確認ください。

≪表示されていない場合≫

「DEP 機器再読込」をクリックしていただき、「DEP 機器管理」画面の確認をお願いいたします。

※反映にはお時間がかかる場合がございます

≪表示されている場合≫

以下の方法で、一度「Apple デプロイメントプログラムサイト」より、再度 DEP サーバートークンを取得していただき、SMSM の「DEP サーバートークン登録」へアップロードを行い、「DEP 機器再読込」をクリックして、ご確認ください。

≪手順≫

1. 以下のマニュアルを参照し、更新作業を行う

 『DEP サーバートークン年次更新マニュアル』

2. 管理サイトの［設定］→［iOS］→［DEP］→［DEP 危機管理］をクリックする
3. 機器が表示されることを確認する

※すべての端末を取得しますので、お時間がかかることがございます。

※表示されない場合、［DEP サービスと同期］をクリックしてください。

※登録した DEP サーバートークンを削除しないようご注意ください。

Q94　iOS：アプリケーション配信
プリインストールのアプリケーションを削除してしまいました。アプリケーション配信で配信できますか。

A94　Apple の仕様により、MDM（SMSM）からの配信はサポートしていないため、手動で App Store からインストールしていただくか、非管理対象としての配信であればできます。
非管理対象としての配信手順は、以下の方法でインストールをお試しください。
※プリインストールアプリ：最初から端末にインストールされているアプリケーション

≪手順≫

1. 管理サイトにログインする
2. ［設定］→［iOS］→［アプリケーション］をクリックする
3. ［アプリケーション配信］をクリックする
4. ［アプリケーション配信］をクリックする
   ※「マップ」アプリケーションの StoreID は「915056765」になります。
   - 「App Store アプリ一覧」の「Store ID」に「915056765」を新規に追加
   - 管理：チェックを付けない
   - ポリシー：未選択
5. ［機器］→［一覧］→対象機器を選択→「設定」の［設定の割り当て］をクリックする
6. 上記で作成したアプリケーション配信の設定セットを選択し、［保存］をクリックする
7. 同期を実行する
8. 端末側で、ポータルを開き、アプリケーションをインストールするボタンを選択する
9. インストールボタンを選択する
10. App Store アプリが起動するため、インストールボタンを選択する
    ※端末によってはクラウドマークの場合もございます。
11. アプリケーションのインストールが完了する

Q95　管理サイトで機器名を変更すると、端末側などに影響はありますか。

A95　管理サイトで「機器名」を変更しても、対象の端末自体の名前は変更されません。また、ポップアップなどの通知もありません。

端末側でポータルを表示している場合は、ポータル内で表示される「機器名」が変更されます。
iOS 端末でエージェントアプリをインストールしている場合は、エージェントアプリ内で表示される「機器名」が変更されます。

管理サイトで機器名を変更すると、管理サイトのログで「機器名」を使って検索する場合、過去のログにある「機器名」の名称は変わらないため、新旧両方の「機器名」で検索が必要になります。

Q96　リモートワイプはキャンセルできますか。

A96　リモートワイプをキャンセルすることはできません。

Q97　iOS：VPP

VPP のアプリケーション配信を行ったところ、以下のエラーが出たが、原因と回避策を教えてほしい。

「機器「xxx」への参加依頼が失敗しました: MDM 要求が無効です。（MCMDMErrorDomain:12008）」

A97　VPP のユーザー指定配信時に出力されるログになります。

［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］で該当機器に割り当たっている構成プロファイルの「Apple Configurator および iTunes からの App のインストールを許可」が"しない"となっていると思われます。解決するためには、「Apple Configurator および iTunes からの App のインストールを許可」を一時的に"する"にしていただくことでアプリケーションの配信ができます。アプリケーション配信後、必要に応じて、「App のインストールを許可」を再度"しない"に設定してください。

Q98　iOS：構成プロファイル

構成プロファイルの「アダルトコンテンツを制限」を利用中に特定のアドレスが見れなくなる原因と回避策を教えてほしい。

A98　構成プロファイルの「アダルトコンテンツを制限」につきましては Apple 社の仕様となり、非公開情報のため原因は不明です。

構成プロファイルの Web フィルタリング設定で、例外設定として「許可する URL」に"見れなくなった特定のアドレスを登録すれば表示できます。

https のアドレスも許可したい場合は、以下のように 2 つ設定する必要がございます。

例："https://ausl.smartmanager.jp"

"http://ausl.smartmanager.jp"

Q99　Android：スクリーンロック

スクリーンロックパスワード変更を実施したときに動作しない場合があるのはなぜでしょうか。

A99　リモート操作でスクリーンロックパスワード変更を実施しても、パスワード変更が反映されない場合は、以下の２点があります。

（1）Android 7.0 以上の場合

デバイスオーナーモード、または Android Enterprise で利用いただく必要があります。

デバイスオーナーモード、または Android Enterprise でない場合、リモート操作でスクリーンロックパスワード変更ができません。

（2）「パスワードポリシー」を満たしていない場合

管理サイトの［スクリーンロック］設定で、「パスワードポリシー」を指定している場合、条件を満たすパスワードを設定する必要があります。

［スクリーンロック］の設定にある「パスワードポリシー」をご確認のうえ、スクリーンロックパスワード変更を実施してください。

Q100 「スクリーンロック」の設定を解除し、端末で自由に設定できるようにしたい。どうすればよいでしょうか。

A100 端末に割り当たっている［スクリーンロック］の設定を「設定なし」にするだけでは、端末のパスワードポリシーを解除することができません。
解除したい場合は、［スクリーンロック］の設定で「パスワードポリシー」を「制限なし」の設定を作成し、端末に適用してください。

※端末に割り当たっている［スクリーンロック］の設定を「設定なし」にするだけでは、端末のパスワードポリシーを解除することができません。
「設定なし」にした場合に端末側の設定がどのようになるかについては、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「付録」－「(設定なし)」とした場合の各種設定の挙動」

Q101 iOS：DEP
DEP 定義プロファイルを設定した機器で iPhone／iPad の初期設定をしたが、エラーとなり進まない。どうしたらよいでしょうか。

A101 端末を初期化後、再度初期設定を行ってください。

≪初期設定手順≫
初期設定で新しい iPhone として登録し、ホーム画面まで進められる場合は初期設定完了後に「設定」から端末の初期化を行ってください。
初期設定で新しい iPhone として登録し、ホーム画面まで進められない場合は、iPhone を USB ケーブルで Mac と接続して iTunes を起動して初期化してください。

Q102 iOS：DEP
デバイスに DEP 定義プロファイルを割り当て、DEP 機器管理で同期しても表示されない機器があります。

A102 DEP サーバーと SMSM サーバーの通信がうまくいっていない可能性があります。
DEP サーバートークン登録を実施後、再度お試しください。

≪DEP サーバートークン登録手順≫
1. 以下のマニュアルを参照し、更新作業を行う


『DEP サーバートークン年次更新マニュアル』

2. 管理サイトの［設定］→［iOS］→［DEP］→［DEP 危機管理］をクリックする
3. 機器が表示されることを確認する

※すべての端末を取得しますので、お時間がかかる場合がございます
※表示されない場合、［DEP サービスと同期］をクリックしてください
※登録した DEP サーバートークンを削除しないようご注意ください

Q103 iOS：機器情報

使用している端末が監視対象モード有効か無効を確認する方法を教えてください。

A103 以下の手順で監視対象モードの有効/無効をご確認ください。

＜管理サイト確認手順＞

①[機器]をクリックします。

②該当機器を選択します。

③情報欄の[デバイス]をクリックします。

④「監視対象」にて確認可能です。

＜端末側の確認手順＞

①設定アプリをタップします。

②設定アプリの最上部にて以下の文言が記載されていれば有効の状態です。

※OS バージョンにより文言が異なる可能性がございます。

==========

この「(機種名)」は「(構成プロファイルの組織名)」によって監視および管理されています。

==========

【監視対象の iPhone、iPad、iPod touch を使う】[https://support.apple.com/ja-jp/HT202837]

Q104 管理サイト：機器情報

管理サイトで端末のシリアル番号の確認方法を教えてください。

A104 以下の手順で端末のシリアル番号をご確認ください。

基本プラン

＜管理サイト確認手順＞

①[機器]をクリックします。

②該当機器を選択します。

③情報欄の[デバイス]をクリックします。

④「基本」の「シリアル番号」にて確認可能です。

※Android 端末の場合、機種によってはシリアル番号が取得できない場合がございます。

Q105 管理サイト：機器情報

機器にユーザーが紐づいているかの確認方法を教えてください。

A105 以下の手順で機器に設定されているユーザーをご確認ください。

基本プラン

＜管理サイト確認手順＞

①[機器]をクリックします。

②該当機器を選択します。

③上部の「ユーザー」にて確認可能です

※設定されていない場合は「(なし)」と記載されます。

Q106 iOS：構成プロファイル

「iPhone を探す」の設定を端末ユーザーが変更できないようにする方法を教えてください。

A106 構成プロファイルアップロードにて以下の項目を指定することで制限可能です。

※本機能は監視対象端末にのみ利用可能な機能です。

＜設定項目＞

[構成プロファイルアップロード]＞[iOS 制限設定]＞[機能の制限]

項目名：アカウント設定の変更を許可(監視対象のみ)　しない

Q107 管理サイト：機器情報

SMSM 管理者画面＞[機器]　にて表示される各端末の「機器名」の編集方法を教えてください。

A107 以下の手順で「機器名」を変更してください。

基本プラン

■手順

①[機器]をクリックします。

②該当機器を選択します。

③[管理情報の編集]をクリックします。

④「機器名」を変更したら[保存]をクリックします。

※端末側から変更することはできません。

※デバイスマネジメントパック版では、機器名の変更は行えません。

Q108 iOS：オリジナルアプリ登録

配信済みオリジナルアプリのバージョンアップ方法を教えてください。

A108 以下の手順に従って、オリジナルアプリのアップデートを行ってください。

■手順

①管理サイト [オリジナルアプリ登録]＞[新規作成] にて新しいバージョンのアプリ設定を作成、保存

※アプリケーション ID が同一のものは 3 つまで作成可能です。

②[アプリケーション配信設定]＞[該当の設定を選択]（古いバージョンが入った設定を選択します）

③オリジナルアプリ一覧 欄にて[+]を押し、手順「①」にて作成したバージョン

（バージョンアップする内容）のアプリを追加、保存

④端末に設定を適用し、同期

なお、マニュアルにアップデート時の留意事項等の記載がございますので併せてご参考ください。

【管理サイト リファレンス マニュアル】8.5.3 オリジナルアプリ登録

[https://www.optim.co.jp/promotion/smsm/pdf/ManagementSite_Reference.pdf]

Q109 iOS：Web クリップ

構成プロファイルアップロードの「Web クリップ」で配信した Web クリップは

+browser Safety Manager 等、任意のブラウザで使用できますか。

A109 使用できません。Safari 向けの機能でございます。

Q110 iOS：DEP

DEP のアクティベーション時に「iPhone を構成中会社名：最終構成を待っています」の状態で止まってしまいます。どうしたらよいですか。

A110 ネットワークの接続状態に問題がないかを確認のうえ

管理サイトにて生成・紐づけされた機器情報より同期を行ってください。

それでも解消しない場合は、初期化を行っていただき再アクティベートを行ってください。

Q111 Andoroid：デバイス管理者権限

「『機器(機器名)』の操作者がデバイス管理者権限を無効にしました。」という通知が来ました。

通知が発生する原因を教えてください。

A111 Google ポリシー変更に伴い KDDI Safety Manager ver.9.3.104.0 以降、

SMSM のデバイス管理者設定を端末操作にて変更可能とする対応を行いました。

端末操作にて、[設定] >[セキュリティ]>[端末管理アプリ] の「KDDI Safety Manager」のチェックを外し無効とした際に

該当のログが出力され管理者に通知が送信されます。

該当の通知を受信した際には操作者に変更しないよう喚起していただき、端末のデバイス管理者設定を再度有効に戻してください。

なお、「デバイス管理者権限」が無効化されている状態の場合、次のような機能が利用不可になります。

●スクリーンロックポリシーが強制されず、自由に変更可能になります。

●カメラ禁止機能が利用出来ません(Android 4.0 以降のみ)。

●リモート操作(リモートロック、スクリーンロックパスワード変更、リモートワイプ）が利用出来ません。

※リモートロックは OS 標準のスクリーンロックをご利用頂けなくなるもので
独自リモートロック画面は「デバイス管理者権限」が無効化されていてもご利用頂くことが可能です。

●Android エージェントのアンインストール抑止機能が利用出来ません。

※Android 7 以降では、Device Owner Mode を利用しない限りはこれまでもアンインストール抑止不可です。

※「デバイス管理者権限」が無効の時に上記操作を行うと、管理サイトに失敗した旨のログが表示されます。

Q112 Andoroid：位置情報

Android 端末の位置情報を変更させないようにする方法を教えてください。

A112 以下の手順で Secure Shield の設定および Device Owner Mode のセキュリティ設定の両方を行ってください。
なお、従来版の認証方法の場合は位置情報の変更を制御することはできません。
Device Owner Mode および Android Enterprise をご利用ください。

＜Secure Shield の設定手順＞
※事前に Secure Shield 対応端末であるかをご確認ください。
【Android エージェント対応端末表】[https://www.optim.co.jp/promotion/smsm/pdf/SupportedDevices.pdf]
①[設定]をクリックします。
②[Android]をクリックします。
③「セキュリティ」をクリックします。
④[Secure Shield]にて[＋]ボタンをクリックします。
⑤設定名を記入し、[有効]欄にチェックを入れます。
⑥[設定位置情報サービス]欄にチェックを入れて保存します。
⑦端末に適用します。

＜Device Owner Mode のセキュリティ設定手順＞
①[設定]をクリックします。
②[Android]をクリックします。
③[Device Owner Mode]をクリックします。
④[セキュリティ設定]にて[＋]ボタンをクリックします。
⑤設定名を記入し、「ステータスバー」欄で[無効にする]にチェックを入れ保存します。
⑥端末に適用します。

Q113 Andoroid：連絡先

配信済みの連絡先の内容を変更して再度配信した場合に変更内容が反映されません。どうしたらよいですか。

A113 配信済みの連絡先に対し、更新・削除を行うことは出来ません。
配信時「姓」「名」「電話番号」が一致している連絡先がある場合
管理サイトにて配信しようとしている連絡先は配信対象外となります。
※いずれかが一致していない場合は、新たな連絡先として生成されます。

Q114 Andoroid：Android Enterprise

Android Enterprise 導入の際に、Google アカウント登録を新規作成から行おうとしたところ「リンクを保護者のアカウントにリンクする」というページに遷移してしまいました。どうしたらよいですか。

A114 Google アカウント作成時に入力いただいた生年月日が、Google 社のアカウント所有条件を満たしていないと「リンクを保護者のアカウントにリンクする」というページに遷移します。
下記 Google 社のサイトをご確認のうえ、条件を満たす設定に修正してください。

【Google アカウントヘルプ】「Google アカウントの年齢条件」
[https://support.google.com/accounts/answer/1350409?hl=ja]

Q115 Android：ウイルス対策

ウイルス対策を申し込んだのに管理サイトでウイルス対策を設定できる項目がないです。考えられる原因を教えてください。

A115 本製品で提供しているウイルス対策ソフト「KDDI Smart Mobile Safety Manager AntiVirus」をご利用になる場合は、

ご利用になる Android 機器に対してオプションパッケージの割り当てが必要となります。

[機器]＞[一覧]＞該当機器選択＞[設定]＞[他の設定を見る]＞[パッケージ] にて[編集]を押していただき

ウイルス対策ソフトのパッケージにチェックを入れ保存してください。

【管理サイトリファレンスマニュアル】4.1.8.3 （設定－Android）パッケージ

[https://www.optim.co.jp/promotion/smsm/pdf/ManagementSite_Reference.pdf]

【管理サイトリファレンスマニュアル】4.1.10.7 （情報－Android）ウイルス対策ソフト

[https://www.optim.co.jp/promotion/smsm/pdf/ManagementSite_Reference.pdf]

Q116 iOS：構成プロファイル

iOS 端末で利用中の電話アプリで、連絡帳の参照ができなくなりました。どうしたらよいですか。

A116 iOS のバージョン 11.3 以降では、ＭＤＭで配信した連絡帳を電話アプリで参照するためには以下の設定が必要になります。

※iOS11.3 未満でも発生する以下の設定をお試しください。

●構成プロファイルの制限設定で以下の設定を行います。

①[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] → [設定名] > [制限設定]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」を「許可しない」に設定する。

●ＭＤＭで配信する連絡帳を読み込む側のアプリケーションを管理対象アプリとして設定します。

①[設定] → [iOS] → [アプリケーション] → [アプリケーション配信]で、設定を作成し、

管理対象にしたいアプリケーションを入力する。

その際、[管理]にチェックを入れる

※他に管理対象アプリを配信している場合は、新規作成の際に

手順「①」の設定に既存アプリの設定が含まれていないと、配信時にアンインストールされます。

必ず配信済みの管理対象アプリの設定を含めて作成してください。

※既存の設定に追加(変更)する場合は、管理対象にしたいアプリケーションを追加し、[管理]にチェックを入れてください。

②端末に「①」で作成した設定を割り当て、同期する

③端末側へ同期が届くと、端末側でポップアップ画面が表示される

「App 管理の変更企業コードに App "管理対象にしたアプリ名"の管理を許可しますか？

App データは管理対象になります。」

と表示されるので、[管理]を押下する

2.2 Android エージェント FAQ

Q1　エージェントがインストールできません。

A1　以下をご確認ください。

1. インターネットに接続できていますか。
2. 誤った URL や QR コードを読み込んでいませんか。
3. Lookout for au が動作を妨げている可能性がありますので、一度 Lookout for au を無効化してインストールを行ってください。
   ※アプリケーションの無効化手順：「設定」→「アプリ」→「Lookout for au」→「無効にする」
   エージェントインストール後、再度有効にしてご利用頂けます。
4. 動作環境を満たしていますか。
   エージェントの動作環境は、以下を参照してください。

『Android キッティングマニュアル』の「はじめに」－「エージェント動作環境」

Q2　エージェントのライセンス認証が行えません。

A2　以下をご確認ください。

1. インターネットに接続できていますか。
2. 企業コードや認証コードが間違っていませんか。
3. ライセンス認証前に、Web フィルタリングの設定を行っていませんか。
4. お申込みライセンス数が超えていませんか。
   お申し込みライセンス数は、管理サイトのダッシュボードにある利用状況、もしくは契約数で確認できます。

Q3　エージェントは起動しているが管理サイトに表示されません。

A3　1. エージェントのライセンス認証は行っていますか。
   エージェントの機能を使用するためには、ライセンス認証を行う必要があります。
   エージェントを起動させ、ライセンス認証を行ってください。
   ライセンス認証の手順は、以下を参照してください。

『Android キッティングマニュアル』の「エージェントのキッティング」－「ライセンス認証を行う」

2. インターネットに接続できていますか。
   管理サイトへ反映させるためにはインターネットへ接続できている必要があります。
   ご使用の Android 端末がインターネットに接続できているかご確認ください。

Q4　エージェントのライセンス解除を行いたいのですが、パスワードの入力を求められます。何を入力すればよいですか。

A4　エージェントの利用を停止する場合には、予め管理者が設定している場合は、ライセンス解除をするとき、パスワード入力が必要になります。
エージェントのライセンス解除をしたい場合は、パスワードについて設定をした管理者へお問い合わせください。

Q5　KDDI Smart Mobile Safety Manager AntiVirusを利用したいです。

A5　「KDDI Smart Mobile Safety Manager AntiVirus」を使用するには「ウイルス対策オプション」のご契約が必要です。

「KDDI Smart Mobile Safety Manager」をインストール後、以下の手順で管理サイト操作及びアプリケーションのインストールを行ってください。

1. 「ウイルス対策機能」より詳細設定を行います。詳細は、以下をご参照ください。

   『管理サイト リファレンスマニュアル』の「設定－Android」－「ウイルス対策機能」

2. 1 で設定した内容を機器に反映させます。詳細は、以下をご参照ください。

   『管理サイト リファレンスマニュアル』の「機器」－「一覧」－「機器の設定」－「（設定－Android）パッケージ」

3. 機器への配信設定を行います。

   「KDDI Smart Mobile Safety Manager AntiVirus」は機器登録されている機種すべてに配布されるのではなく、個別に配信設定を行う必要があります。詳細は、以下をご参照ください。

   『管理サイト リファレンスマニュアル』の「機器」－「一覧」－「機器の設定」－「（設定－Android）設定の割り当て」

4. 同期して、端末へ設定を反映します。
5. 端末に「KDDI Smart Mobile Safety Manager AntiVirus」をインストールします。詳細は、以下をご参照ください。

   『Android クライアント リファレンスマニュアル』の「ウイルス対策機能」－「インストールする」

Q6　KDDI Smart Mobile Safety Manager AntiVirusがインストールできません。

A6　ご使用の Android 端末が動作環境を満たしていますか。

KDDI Smart Mobile Safety Manager AntiVirus の動作環境は、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「Android クライアントについて」－「ウイルス対策機能動作環境」

Q7　機種変更をしました。同じ設定を反映させるのに、どのような手順が必要ですか。

A7　「KDDI Smart Mobile Safety Manager」の設定は、SIM（電話番号）ではなく機器の固有情報（IMEI 等）に紐づき設定しているため、機種変更後の機種への設定が必要です。

また、端末側でライセンス解除やリセットを行っても管理サイトに［機器］情報が残り、請求対象となってしまいますので、管理サイトで機種変更前の機器情報を削除する必要があります。

以下の手順で機種変更後の端末に設定を反映してください。

1. マニュアルサイト掲載の『クイックスタートマニュアル』を参照し、エージェントアプリのインストール、ライセンス認証を行ってください。
2. 機種変更前の端末に設定していた設定内容を、機種変更後の端末に反映してください。
3. 古い機器情報を管理サイトから削除してください。
4. 機種変更前の端末を別の用途で利用する場合は、エージェントアプリのライセンス解除及びアンインストールを行ってください。iOS の場合は、MDM 構成プロファイルも削除してください。

Q8　Android 端末の言語を英語に変更したのに、エージェントの言語が変更されません。

A8　一部の画面ではすぐに言語が変更されません。Android 端末を再起動してください。

Q9　Android 7.0 以降の端末で、ライセンス認証ができません。

A9　エージェントを最新版にアップデートする前に Android のバージョンを 7.0 へ上げてしまった場合は、正しくライセンス認証ができません。
先に OS を Android 7.0 にアップデートしてしまった場合は、以下の手順に従って、エージェントを再インストールしてください。

≪Device Owner Mode を利用せず管理する場合≫
初回にエージェントをインストールしたときと同じ URL にアクセスし、エージェントの APK を再度ダウンロードしてください。

≪Device Owner Mode を利用して管理する場合≫
端末初期化後に Device Owner Mode を設定してから、エージェントを再度インストールしてください。
Device Owner Mode については、以下を照してください。

 『Android キッティングマニュアル』

Q10　SMSM の従来版エージェントとストア版エージェントを両方インストールしてしまいました。片方をアンインストールする方法を教えてください。

A10　以下の手順に従って操作を行ってください。

＜Android Enterprise で認証していない端末でストア版アプリを認証した場合＞

①ストア版エージェントを起動して[終了]をタップします。

起動したアプリがストア版か従来版かの確認方法につきましては、

アプリ起動後トップ画面の左下にあるバージョン値の「()」内をご確認ください。

※「(Store)」と記載されている場合はストア版アプリでございます。

※パスワードを聞かれる場合は、管理サイトのエージェント共通管理をご確認ください。

《パスワード確認手順》

[設定]＞[管理アプリの通信と動作]＞[エージェント共通管理]の

「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」項目

②「①」を実施した後に[アンインストール]をタップします。

※この時もパスワードを聞かれる場合は上記のパスワードを入力します。

③従来版エージェントを起動し[ライセンス解除]をタップします。

※パスワードは「①」と同様のパスワードになります。

④「③」を実施した後に[ライセンス認証]をタップして通常通りライセンス認証作業を実施します。

ライセンス認証作業につきましてはマニュアルをご参照ください。

【Android キッティングマニュアル】[https://www.optim.co.jp/promotion/smsm/pdf/Android_Kitting.pdf]

＜Android Enterprise で認証している端末で従来版を認証した場合＞

※注意※操作には端末の初期化が伴います。

①ストア版エージェントを起動して[終了]をタップします。

※パスワード聞かれた場合は、管理サイトのエージェント共通管理をご確認ください。

《パスワード確認手順》

[設定]＞[管理アプリの通信と動作]＞[エージェント共通管理]の

「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」項目

②[端末初期化]をタップし端末を初期化します。

③再度 Android Enterprise のキッティング手順に沿ってキッティングを行ってください。

【Android キッティングマニュアル】[https://www.optim.co.jp/promotion/smsm/pdf/Android_Kitting.pdf]

なお、ストア版エージェントは v.9.5.111.0 以降、

Device Owner Mode で認証していない端末ではライセンス認証はできないよう仕様変更しております。

2.3 iOS エージェント FAQ

Q1　ライセンス認証が行えません。

A1　1. インターネットに接続できていますか。
ライセンス認証を行うにはインターネットへ接続できている必要があります。
ご使用の iPhone／iPad がインターネットに接続できているかご確認ください。

2. Apple Push 証明書の登録は行いましたか。
ライセンス認証を行うには、Apple Push 証明書の登録が必要です。
登録方法の詳細は、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』

3. 企業コードや認証コードが間違っていませんか。
入力した企業コードや認証コードが正しくないとライセンス認証を完了できません。
入力した企業コード、または認証コードをもう一度確認してください。

4. ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証は行えません。
お申し込みのライセンス数については管理者にお問い合わせください。

5. Jailbreak された機器ではありませんか。
Jailbreak（iOS 端末を不正に改造）された機器では、ライセンス認証が完了しない可能性があります。
管理者にお問い合わせください。

6. ライセンス認証前に Web フィルタリング設定を行っていませんか。
iOS 9.0 及び 9.1 の場合、ライセンス認証前に Web フィルタリング設定をした場合、本製品の構成プロファイルがインストールできなくなるため、認証画面が次に進まず、ライセンス認証が完了しませんのでご注意ください。

Q2　MDM 構成プロファイルへの設定は行ったが管理サイトに表示されません。

A2　インターネットに接続できていますか。
管理サイトへ反映させるためにはインターネットへ接続できている必要があります。
ご使用の iPhone／iPad がインターネットに接続できているかご確認ください。

Q3　MDM 構成プロファイルのインストール中に途中でキャンセルをしてしまいました。

A3　再度、最初から MDM 構成プロファイルのインストールを行ってください。
MDM 構成プロファイルのインストール方法は、以下を参照してください。


『iOS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

Q4　MDM 構成プロファイルのインストール中に「サーバ証明書は無効です。」というメッセージが表示されました。

A4　iPhone／iPad の日時設定が正しく設定されていない場合があります。iPhone／iPad の日時設定を正しく設定し直してください。

Q5　MDM 構成プロファイルを誤って削除してしまいました。

A5　再度、iPhone／iPad の認証を行ってください。詳細は、以下を参照してください。

『iOS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

Q6　再度ライセンス認証を行いたい場合には。

A6　再度、ライセンス認証を行ってください。詳細は、以下を参照してください。

『iOS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

Q7　機種変更を行う場合のライセンス認証手順はどうしたらよいでしょうか。

A7　「KDDI Smart Mobile Safety Manager」の設定は、SIM（電話番号）ではなく機器の固有情報（IMEI 等）に紐づき設定しているため、機種変更後の機種への設定が必要です。
また、端末側でライセンス解除やリセットを行っても管理サイトに［機器］情報が残り、請求対象となってしまいますので、管理サイトで機種変更前の機器情報を削除する必要があります。

以下の手順で機種変更後の端末に設定を反映してください。
エージェントのインストールは、エージェントをご利用になる場合のみ行ってください。

1. ライセンス認証（MDM 構成プロファイルのインストール）を行う。詳細は、以下を参照してください。

『iOS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

2. エージェント認証を行う。詳細は、以下を参照してください。

『iOS キッティングマニュアル』の「エージェント認証」－「エージェント認証を行う」

Q8　共有アドレス帳
4GLTE ケータイ向けで利用できる共有アドレス帳は、iOS でも利用できますか。

A8　共有アドレス帳は、4GLTE ケータイ向けの機能となります。
iOS ではお使いいただけません。

Q9　エージェント認証

エージェント認証で、アクティベーションコードの入力を省略したい。

A9　ポータルを利用してエージェントの認証作業をするとアクティベーションコードを手で入力しなくても自動で認証することができます。

（1） エージェントをインストールします。

エージェントをインストール済みの場合は、スキップしてください。

1. ポータルをタップ
2. ポータル画面で、［エージェントを認証する］をタップ
3. ［App Store からインストール］をタップ
4. App Store に移動します。のポップアップが表示されるので、［OK］をタップ
5. App Store で開きますか？のポップアップが表示されるので、［開く］をタップ
6. App Store のエージェントのページへ移動するため、［インストール］をタップ

インストール完了後、一度、端末のホーム画面に戻ってください。

（2） エージェント認証を行います。

1. ポータルをタップ
2. ポータル画面で、［エージェントを認証する］をタップ
3. ポータル画面で、［起動して認証］をタップ
4. 「KDDI Manager で開きますか？」のポップアップが表示されるので、［開く］をタップ
5. 「認証中」の表示後、位置情報、通知について［許可］をタップすると完了

Q10　iOS エージェントで認証しないと使えない機能はありますか。

A10　エージェントのインストール・認証を行われないと
ご利用いただけない機能につきましては下記のとおりです。

●位置情報測位・送信
●Jailbreak 検知
●メッセージ通知　※オプション機能になります

2.4 Mac エージェント FAQ

Q1　ライセンス認証が行えません。

A1　1. インターネットに接続できていますか。
ライセンス認証を行うにはインターネットへ接続できている必要があります。
ご使用の Mac OS 端末がインターネットに接続できているかご確認ください。

2. 企業コードや認証コードが間違っていませんか。
入力した企業コードや認証コードが正しくないとライセンス認証を完了することができません。
入力した企業コード、または認証コードをもう一度確認してください。

3. ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証を行うことはできません。
お申し込みのライセンス数については管理者にお問い合わせください。

4. Safari の設定を確認してください。
Safari の設定で Cookie を受け入れない状態になっていると、ライセンス認証は行なえません。
Safari メニューで［環境設定…］をクリックし、［セキュリティ］タブの［Cookie の受け入れ］で［常に受け入れる］を選択します。

Q2　プロファイルへの設定は行ったが管理サイトに表示されません。

A2　インターネットに接続できていますか。
管理サイトへ反映させるためにはインターネットへ接続できている必要があります。
ご使用の Mac 端末がインターネットに接続できているかご確認ください。

Q3　プロファイルのインストール中に途中でキャンセルをしてしまいました。

A3　再度、最初からプロファイルのインストールを行ってください。
プロファイルのインストール方法は、以下を参照してください。

『Mac OS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

Q4　プロファイルのインストール中に「サーバ証明書は無効です。」というメッセージが表示されました。

A4　Mac の日時設定が正しく設定されていない場合があります。Mac の日時設定を正しく設定し直してください。

Q5　プロファイルを誤って削除してしまいました。

A5　再度、Mac の登録を行ってください。詳細は、以下を参照してください。

『Mac OS キッティングマニュアル』の「ライセンス認証」－「ライセンス認証（プロファイルのインストール）を行う」

Q6　再度ライセンス認証を行いたい場合には。

A6　再度、ライセンス認証を行ってください。以下を参照してください。

『Mac OS キッティングマニュアル』の「ライセンス認証」ー「ライセンス認証（プロファイルのインストール）を行う」

Q7　サーバに配置された Apple Push 証明書と端末側の証明書が同一であることを確認したい時にはどうすればいいですか。

A7　管理サイト側の Apple Push 証明書のトピック値を確認します。
Mac 端末側では、［Apple アイコン］→［この Mac について］→［詳しい情報］→［システムレポート］→［ソフトウェア］欄のプロファイルを選択し、対象のプロファイル内のトピック値を確認します。
上記 2 つのトピック値が同一であるか確認してください。

2.5 Windows エージェント FAQ

Q1　エージェントがインストールできません。

A1　ご使用の Windows 機器が動作環境を満たしていますか。
本製品の動作環境は、以下を参照してください。


『Windows キッティングマニュアル』の「Windows クライアントについて」－「動作環境」

Q2　エージェントのライセンス認証が行えません。

A2　1. インターネットに接続できていますか。
ライセンス認証を行うにはインターネットへ接続できている必要があります。
ご使用の Windows 機器がインターネットに接続できているかご確認ください。

2. 企業コードや認証コードが間違っていませんか。
入力した企業コードや認証コードが正しくないとライセンス認証を完了することができません。
入力した企業コード、または認証コードをもう一度確認してください。

3. ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証は行なえません。
お申し込みのライセンス数については管理者へお問い合わせください。

Q3　エージェントは起動しているが Windows 機器の管理･運用が行われていません。

A3　1. エージェントは管理サイトと通信できていますか。
Windows 機器の管理･運用を行うためにはエージェントが管理サイトと通信する必要があります。
エージェントと管理サイトの通信状態はタスクトレイアイコンで確認することができます。
以下のマニュアルを参照し、エージェントが管理サイトと通信できているかご確認ください。


『Windows クライアント リファレンスマニュアル』の「画面の見かた」－「タスクトレイアイコンの説明」

2. エージェントのライセンス認証は行っていますか。
エージェントの機能を使用するためには、ライセンス認証を行う必要があります。
ライセンス認証の方法は、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「エージェントの利用停止」－「ライセンス認証」－「ライセンス認証を行う」

Q4　パスワードの入力を求められます。

A4　エージェントの一時停止、エージェントのアンインストール、ライセンス認証解除など、エージェントの使用を停止する場合にはパスワードの入力が必要な場合があります。管理者へお問い合わせください。

Q5　ライセンス認証の解除が行えません。

A5　エージェントは起動していますか。

ライセンス認証の解除を行うためにはエージェントが起動している必要があります。

以下のマニュアルを参照し、エージェントを起動させてからライセンス認証の解除を行ってください。

『Windows クライアント リファレンスマニュアル』の「エージェントの利用停止」－「一時的に停止する」－「再度エージェントを起動する」

Q6　エージェントの操作マニュアルを閲覧したいです。

A6　画面右下に表示されている 

をクリックし、マニュアルページよりご覧ください。

2.6 Windows 10 Mobile エージェント FAQ

Q1 ライセンス認証が行えません。

A1 1. ご使用の Windows 10 Mobile 機器が動作環境を満たしていますか。
本製品の動作環境は、以下を参照してください。

『Windows 10 Mobile キッティングマニュアル』の「Windows 10 Mobile クライアントについて」－「動作環境」

2. インターネットに接続できていますか。
ライセンス認証を行うにはインターネットへ接続できている必要があります。
ご使用の Windows 10 Mobile 機器がインターネットに接続できているかご確認ください。

3. 企業コードや認証コードが間違っていませんか。
入力した企業コードや認証コードが正しくないとライセンス認証を完了することができません。
入力した企業コード、または認証コードをもう一度確認してください。

4. ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証は行えません。
お申し込みのライセンス数については管理者へお問い合わせください。

Q2 起動しているが Windows 10 Mobile 機器の管理･運用が行われていません。

A2 1. 管理サイトと通信できていますか。
Windows 10 Mobile 機器の管理･運用を行うためには、管理サイトと通信する必要があります。

2. ライセンス認証は行っていますか。
Windows 10 Mobile 機器を使用するためには、ライセンス認証を行う必要があります。
ライセンス認証の方法は、以下を参照してください。

『Windows 10 Mobile キッティングマニュアル』の「基本操作」－「認証を行う」

Q3 パスワードの入力を求められます。

A3 リモートロックの解除をする等、パスワードの入力が必要な場合があります。管理者へお問い合わせください。

Q4 ライセンス認証の解除が行えません。

A4 Windows 10 Mobile 機器は起動していますか。
ライセンス認証の解除を行うためには、Windows 10 Mobile 機器が起動している必要があります。

Q5 操作マニュアルを閲覧したいです。

A5 画面右下に表示されている 

をクリックし、マニュアルページよりご覧ください。

2.7 サービス企業用サイト FAQ

Q1　サービス企業用サイトが開けません。

A1　1. インターネットに接続できていますか。
サービス企業用サイトを使用するにはインターネットへ接続できている必要があります。
ご使用のパソコンがインターネットに接続できているかご確認ください。

2. ご使用のパソコンが動作環境を満たしていますか。
サービス企業用サイトの動作環境は、以下を参照してください。


『サービス企業用サイト ユーザーマニュアル』の「はじめに」－「サービス企業用サイト動作環境」

Q2　「ログイン状態を保持」にチェックを入れたが、自動的にログインされません。

A2　自動的にログインする期間は「ログイン状態を保持」にチェックを入れてから 14 日間です。14 日間を過ぎると、再度入力が必要となります。また、1 度ログアウトすると、自動的にログインする機能は無効となります。再度、ログイン情報を入力し、ログインを行ってください。

Q3　インポート時に「413 Request Entity Too Large」というエラー画面が表示されました。

A3　インポートファイルのサイズがオーバーしています。
※インポートできるファイルサイズは 10MB までです。ファイルサイズを 10MB 以下にし、インポートし直してください。

2.8 4G LTE ケータイ 管理サイト FAQ

Q1	アプリケーション禁止 管理サイトから各端末へ初期化が出来ない様に制限をかける事は可能でしょうか。
A1	端末の初期化を禁止する機能はございません。

Q2	アプリケーション禁止 ブラウザーでインターネットを使わせたくないです。
A2	4G LTE ケータイプランの場合、アプリケーション禁止でブラウザの起動を禁止することが可能です。 以下のアプリケーション名とパッケージ名を利用してください。 アプリケーション名：ブラウザ パッケージ名：com.android.browser

Q3	アプリケーション禁止 アプリケーション禁止を設定しても禁止できないアプリケーションがあります。
A3	Web ベースのアプリケーションの場合、アプリケーション禁止だけでは禁止できない場合があります。 Web ベースのアプリケーションは、バックグラウンドで URL を利用しています。 そのため、完全に禁止するには、「Web フィルタリング」機能を使用してアプリケーション内で遷移先の URL を禁止 URL に指定していただく必要があります。

Q4	共有アドレス帳 既に配信しているアドレス帳（A）に、更新（追加削除など）したアドレス帳（B）を送信すると、上書きされずに追加登録され、アドレスデータの重複が生じるのですがどうしたらよいですか。
A4	詳しい手順については以下の回避方法をご確認ください。 4G LTE ケータイ共有アドレス帳重複の回避方法 https://www.optim.co.jp/promotion/smsm/pdf/FPHowToAvoidContactDuplication.pdf

Q5	共有アドレス帳 端末で登録した連絡先を共有アドレス帳配信を行い変更を加えることが出来ますでしょうか。
A5	端末で登録された連絡先を変更操作することが出来ません。

Q6	共有アドレス帳 配信した共有アドレス帳のグループの項目に「KDDI Smart Manager」と表示される連絡先と、表示がない連絡先の違いは何ですか。
A6	エージェントのバージョンが 7.4.240.0 未満の場合に発生いたします。 連絡先の初回配信のデータの場合、グループの項目に「KDDI Smart Manager」が表示されます。その後、端末側で以下の手順で、連絡先の削除を行ったあとに同期を行うと、グループの項目が空欄表示になります。 ［端末の設定］→［その他の設定］→［アプリ］→［すべて］→［電話帳ストレージ］→［データを消去］

Q7	共有アドレス帳 共有アドレス帳で配信された後にグループ分けを利用者側で行うことは可能ですか。
A7	2017 年 10 月 13 日よりグループ No.としてナンバーでグループ配信が可能となりました。 エージェントのバージョンが 7.4.240.0 未満の場合は、共有アドレス帳で配信したデータのグループ設定の編集は行えません。 エージェントのバージョンが 7.4.240.0 以上の場合は、配信したグループ名は、端末側で編集は可能ですが、管理サイトへは反映されません。
Q8	共有アドレス帳 共有アドレス帳の配信されたことを確認するにはどうしたらよいですか。
A8	管理サイト上で共有アドレス帳を修正し配信した場合、管理・機器ログ画面で、以下のログを確認できます。 「機器「（機器名）」のエージェントが共有アドレス帳の設定を行いました。」
Q9	共有アドレス帳 共有アドレス帳ポリシーの設定画面で連絡先データの一部を削除するため、CSV 編集後ファイルをインポート･取り込みしましたが、連絡先削除した内容が反映されません。
A9	CSV ファイルで、削除したい対象データの「削除（削除する:1）」欄に 1 を入力していただいたかご確認をお願いいたします。
Q10	共有アドレス帳 CSV インポートについて､1 つの CSV の中に携帯と内線情報など電話番号を 3 つまで入れているのですが、インポートすると 1 つしか登録ができません。
A10	エージェントバージョンが 7.4.220.0 未満を利用している場合に､共有アドレス帳機能をご利用された場合、連絡先 1 件に対する電話番号の登録は 1 つのみになります。 共有アドレス帳機能をご利用になる場合は、エージェントバージョンをご確認いただき、最新のバージョンにアップデートしてからご利用ください。

Q11　共有アドレス帳

管理サイトから共有アドレス帳配信を行っていますが、「グループ」に「KDDI Smart Manager」の表記がない端末がありましたが、なぜですか。

A11　エージェントのバージョンが 7.4.240.0 未満の場合に発生いたします。

アドレス帳のグループに「KDDI Smart Manager」が表示される条件については、端末の操作手順により表示がある場合と表示がない場合があります。

1. ［電話帳］で中央ボタンで連絡先を選択した場合、グループ名が表示されます。
2. ［電話帳］で［メニュー］-［編集］を選択した場合、グループ名が表示されません。
3. 下記操作を行った場合は、グループ名が表示されません。
   端末の設定→その他の設定→アプリ→すべて→電話帳ストレージ→データを消去にアップデートしてからご利用ください。

Q12　共有アドレス帳

共有アドレス帳を配布した場合、アドレス帳のグループに「KDDI Safety Manager」と表示されますが、 アドレス帳のグループ表示を実施しても「KDDI Safety Manager」のグループが出てきません。

A12　エージェントのバージョンが 7.4.240.0 未満の場合に発生いたします。

配信した共有アドレス帳は、「KDDI Safety Manager」というグループ名を設定していますが、端末側で“表示方法”を“グループ順”に設定しても“グループ表示”することはできません。

Q13　共有アドレス帳

ビジネス便利パックから SMSM へ共有アドレス帳を移行する場合など、赤外線通信や SD カードなどで連絡帳データを移行し、その後に管理サイトから既に端末内にある連絡帳データを配信した場合はどのようになるのでしょうか。

A13　アドレスデータが重複します。

SMSM ではアドレスデータで判断しておらず、管理サイトから配信した共有アドレス帳と、それ以外で登録したアドレス帳データとして判断している仕様のためとなります。

Q14　共有アドレス帳

共有アドレス帳は複数作成できますか。複数作成できる場合、何個まで作成できますか。

A14　複数作成することができます。上限は 50 個になります。

Q15　共有アドレス帳

共有アドレス帳を管理画面から適用する以外に端末へ適用する方法はありますか。

A15　管理画面からのみ配信可能です。

Q16　共有アドレス帳

共通アドレス帳を複数パターン（A、B）管理サイトへ登録した場合、A を配信したのち B を同じ端末へ再度配信し直すと、端末側の連絡帳データは A から B に置き換わりますでしょうか。

A16　置き換わります。

Q17　共有アドレス帳

共有アドレス帳配信以外の方法で登録した連絡先を重複させたくない場合、何か方法はありますでしょうか。

A17　共有アドレス帳は 「端末側に共有アドレス帳配信以外の方法で登録したアドレスデータ」を管理していないため、共有アドレス帳と同じ情報の登録があった場合に重複を避ける方法はありません。

Q18　共有アドレス帳

一度配信した共有アドレス帳のデータのアップデートをする手順を教えてください。

A18　以下の手順で、配信中の共有アドレス帳の内容を更新することができます。

1. 配信中の共有アドレス帳ポリシーからファイルをエクスポートする
2. エクスポートしたファイルの内容を編集する
   （a）変更がある場合は変更箇所を修正
   （b）新規登録の場合は追加
   （c）削除の場合は、削除（削除する:1）の列に「1」を記入
3. 編集完了後、元の共有アドレス帳ポリシーに編集済みファイルを再インポートする

以上で、共有アドレス帳のデータの更新が終わり、次回端末同期時に、更新した共有アドレス帳が配信されます。

※共有アドレス帳に登録しているデータは、CSV ファイルの「GUID」の値で管理しています。アドレス帳を更新するときは、エクスポートした CSV ファイルの「GUID」の値は変更しないでください。

Q19　共有アドレス帳

共有アドレス帳を配信後に、端末側で個人で連絡先を登録し、その後共有アドレス帳を再配信した場合に、個人が登録した連絡先は残りますか。

A19　端末側で登録したアドレスは共有アドレス帳配信後にも残ります。

Q20　共有アドレス帳

共有アドレス帳は組織毎に配信が行えますか。

A20　以下の手順で組織をご利用いただくことで配信ができます。

1. 組織を作成する
2. 管理プロファイルを作成し、組織に配信したい共有アドレス帳の設定を割り当てる
3. 1.で作成した組織に 2.で作成した管理プロファイルを割り当てる
4. 1.で作成した組織にグループ化したいユーザーを紐づける
   ・ユーザー画面で、組織に含めたいユーザーを選択し、組織欄で 1.で作成した組織を選択する
5. 4.で組織に紐づけたユーザーと配信対象の機器を紐づける
   ・機器画面で、対象の機器を選択し、所有者で 4.で組織に紐づけたユーザーを選択する

以上を実施した後に同期を行うと、組織に紐づいた機器に、割り当てた共有アドレス帳を配信できます。

Q21	組織 組織ごと（A，B，C）に、管理者権限を割り振ることは可能でしょうか。
A21	4G LTE プランでは、組織ごとに管理者権限の割り振りを行うことが出来ません。

Q22	組織 機器へ組織を一括で割り当てる手順を教えてください。
A22	4G LTE プランで、機器へ組織を一括で割り当てる方法につきましては、SMSM の購入元にお問い合わせください。

Q23	位置情報 GRATINA4G の端末側の位置情報設定を管理サイト側で設定できませんか。
A23	端末側の位置情報に必要な設定を管理サイト側で設定することはできません。

Q24	位置情報 リモートワイプした後に位置情報は取得できますか。
A24	リモートワイプは端末を初期化してしまうため、リモートワイプ後は位置情報が取得できなくなります。

Q25	パスワードポリシー 端末側のパスワード設定を「数字のみ」に強制できますか。
A25	OS の仕様上「数字のみ」のパスワードを強制的に設定要求をすることはできません。

Q26	認証 キッティング時、Wi-Fi 環境下で認証作業を行っても良いでしょうか。
A26	Wi-Fi 環境下で認証作業を行っていただいて問題ございません。 Wi-Fi のみで通信している場合は、管理サイトの ［同期］ボタンをクリックしても同期は実行されません。同期が必要な場合は、エージェントアプリの画面から同期を行ってください。

Q27	認証 認証コードはどこに表記がありますか。
A27	管理サイトログイン後のトップ画面、別画面からはトップタブを押下していただいた画面の下へスクロールしていただき、「認証コード」欄をご確認ください。詳細は、以下を参照してください。  『Apple Business Manager(ABM) 運用マニュアル』の「トップページの使い方」

Q28　認証

ライセンス認証完了時に設定が割り当たるようにしたいのですが、どうしたらよいでしょうか。

A28　以下の手順でライセンス認証完了時に端末に設定を割り当てることができます。

1. 端末でライセンス認証を行う前に、管理サイトでライセンス認証待ち機器を作成する
   ※ライセンス認証待ち機器作成時に、端末と紐づけるため、以下の情報が必要です。
   ・電話番号
2. 管理サイトで制限設定やポリシーなどを作る
3. 2.で作った設定セットを 1.で作ったライセンス認証待ち機器に割り当てる
4. 端末でライセンス認証を行う
   ※1.で作ったライセンス認証待ち機器と紐づく情報に基づいて管理サイト側で端末情報が更新され、3.で端末に割り当てた設定セットが配信され、端末に割り当たります。

Q29　定期バックアップ

定期バックアップの復元コードの確認方法を教えてください。

A29　管理サイト画面の［メニュー］ の［管理・機器ログ］をクリックして表示する管理・機器ログ画面から確認することができます。

キーワード検索できますので、ここで機器名、または復元など入力すると絞り込めます。

定期的にバックアップがある場合は、以下のいずれかのログがあり、「復元コード」部分に復元コードが表示されています。

・「エージェントがバックアップへ復元しました: 復元コード」

・「エージェントが即時バックアップを行いました: 復元コード」

Q30　スクリーンロックパスワード変更をしたときに動作しなくなりました。対応方法を教えてください。

A30　管理者が設定している「パスワードポリシー」の条件を満たしていないときに動作しない場合があります。管理サイトの［パスワードポリシー］の設定条件をご確認のうえ、スクリーンロックパスワード変更を実施してください。

Q31　管理サイト：機器情報

管理サイトで端末のシリアル番号の確認方法を教えてください。

A31　以下の手順で端末のシリアル番号をご確認ください。

4G LTE ケータイプラン

＜管理サイト確認手順＞

①[機器]をクリックします。

②「CSV 一括エクスポート」をクリックします。

③「詳細な機器情報を全て出力する」にチェックを入れます。

④「作成」をクリックします。

⑤エクスポートした CSV ファイルにてシリアル番号が確認できます。

Q32　管理サイト：機器情報

機器にユーザーが紐づいているかの確認方法を教えてください。

A32　以下の手順で機器に設定されているユーザーをご確認ください。

4G LTE ケータイプラン

＜管理サイト確認手順＞

①[機器]をクリックします。

②該当機器を選択します。

③上部の「所有者」にて確認可能です

※設定されていない場合は「(なし)」と記載されます。

Q33　管理サイト：機器情報

SMSM 管理者画面＞[機器]　にて表示される各端末の「機器名」の編集方法を教えてください。

A33　以下の手順で「機器名」を変更してください。

4GLTE ケータイプラン

■手順

①[機器]をクリックします。

②該当機器を選択します。

③[設定を変更する]をクリックします。

④「機器名」を変更したら[保存]をクリックします。

※端末側から変更することはできません。

Q34　FP：共有アドレス帳

共有アドレス帳で配信した連絡先の削除方法を教えてください。

A34　配信済みの連絡先を削除する場合は、以下の手順で操作を行ってください。

■手順

①[メニュー]>[共有アドレス帳]をクリックします。

②対象の設定を選択し、「共有アドレス帳エクスポート」ををクリックします。

③ダウンロードした CSV ファイルを Excel 等で開き編集を行います。

※M 列「削除(削除する:1)」：1 を入力

④[共有アドレス帳インポート]をクリックし、[次へ]ををクリックします。

⑤参照より編集した CSV ファイルを選択し、アップロードします。

⑥問題が無ければ[インポート実行]をクリックします。

⑦[メニュー]>[管理プロファイル]をクリックします。

⑧該当の共有アドレス帳の設定が当たっている管理プロファイルをクリックします。

⑨同期します。

Q35　FP：アプリケーション禁止
４GLTE ケータイで Web アプリケーションを禁止することはできますか。

A35　Web ショートカットアプリケーションはアプリケーション禁止では禁止することが出来ません。
「Web フィルター（オプション）」をご利用いただく方法でのみ禁止が可能です。

「ブラウザ」を禁止する場合は「アプリケーション禁止」で制御可能です。
【プリインストール アプリケーション禁止 可否一覧】
[https://www.optim.co.jp/promotion/smsm/pdf/FPAppslist.pdf]

Q36　FP：アプリケーション禁止
ワンセグを制限する方法を教えてください。

A36　[メニュー]>[アプリケーション禁止] にて制限可能です。
アプリケーション名、パッケージ名については、「プリインストール アプリケーション禁止 可否一覧」の「TV」の項目をご参照ください。

【プリインストール アプリケーション禁止 可否一覧】
[https://www.optim.co.jp/promotion/smsm/pdf/FPAppslist.pdf]

Q37　FP：同期
機種変更後通信日時が更新されていません。解決方法を教えてください。

A37　下記手順にて、管理サイトでご確認いただいている機器が正しい機器かをご確認ください。

■手順
①端末側で[設定]をタップします。
②[その他設定]をタップします。
③[端末情報]をタップします。
④[端末の状態]をタップします。
⑤[SIM のステータス]をタップします。
⑥「電話番号」欄を確認します
⑦管理サイトにて[機器]をクリックします。
⑧「検索条件」のプルダウンから「電話番号」を選択します。
手順「⑥」で確認した値を検索ボックスに入力し[検索]をクリックします。
⑨表示された機器情報の通信日時をご確認ください。

2.9 4G LTE ケータイ エージェント FAQ

Q1 エージェントがインストールできません。

A1 ご使用の 4G LTE ケータイ端末が動作環境を満たしていますか。
エージェントの動作環境は、以下を参照してください。

『ABM サーバートークン年次更新マニュアル』の「エージェント動作環境」

Q2 エージェントのライセンス認証が行えません。

A2 1. インターネットに接続できていますか。
ライセンス認証を行うにはインターネットへ接続できている必要があります。
ご使用の 4G LTE ケータイ端末がインターネットに接続できているかご確認ください。

2. 企業コードや認証コードが間違っていませんか。
入力した企業コードや認証コードが正しくないとライセンス認証を完了することができません。
入力した企業コード、または認証コードをもう一度確認してください。

3. ライセンス数は足りていますか。
お申し込みの内容により、お申し込みのライセンス数を超えてのライセンス認証を行うことはできません。
お申し込みのライセンス数については管理者にお問い合わせください。

Q3 エージェントは起動しているが管理サイトに表示されません。

A3 1. エージェントのライセンス認証は行っていますか。
エージェントの機能を使用するためには、ライセンス認証を行う必要があります。
エージェントを起動させ、ライセンス認証を行ってください。
ライセンス認証の手順は、以下を参照してください。

『ABM サーバートークン年次更新マニュアル』の「ライセンス認証を行う」

2. インターネットに接続できていますか。
管理サイトへ反映させるためにはインターネットへ接続できている必要があります。
ご使用の 4G LTE ケータイ端末がインターネットに接続できているかご確認ください。

Q4 パスワードの入力を求められます。

A4 エージェントの利用を停止する場合には、パスワード入力が必要な場合があります。
エージェントの終了、エージェントのアンインストール、ライセンス認証解除など、エージェントの利用を停止する場合にはパスワードの入力が必要な場合があります。
管理者にお問い合わせください。

Q5　位置情報

位置情報の更新がされないのですが、端末側でどの様な操作をすれば、定期的位置取得が可能となるのでしょうか。

A5　位置情報を取得するためには、端末本体とエージェントアプリ、管理サイトの設定が必要です。

以下をご確認ください。

<管理サイトの設定>

「エージェントによる測位」で、「定期的に測位する」に設定する。

※「エージェント起動時のみ測位する」の場合は端末再起動、エージェントのライセンス認証、OS 仕様によるエージェントが再起動、ユーザ操作によるエージェント再起動時のみ取得します。

<エージェントアプリの設定>

位置情報取得を許可する。

※アプリ起動→メニュー→位置情報→許可する

<端末本体の設定>

1. 「GPS による位置測位」/「ネットワークによる位置測位」のいずれかによる測位を可能にしていること

   ※可能な限り、位置情報設定モードを「高精度」に設定してください。

2. バックグラウンドデータを有効にしていること。

   ※メニュー→設定→無線・ネットワーク→データ使用料→KDDI Safety Manager→バックグラウンドデータを制限するを OFF にする。

3. エコモードなどの省電力モードを無効にしていること。

   ※メニュー→設定→エコ・電池→エコモード　を OFF にする。

詳細な情報については以下の設定注意事項をご確認ください。

位置情報取得の設定注意事項

https://www.optim.co.jp/promotion/smsm/pdf/location_notice.pdf