

■ 目次

[管理サイト](#)[Androidエージェント](#)[iOSエージェント](#)[Windowsエージェント](#)[サービス企業用サイト](#)[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

■ 管理サイト

Q.1 管理サイトが開けません。

- **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。
- **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「オフィスまるごとサポートデバイスマネジメントとは」 - 「管理サイトの動作環境」

Q.2 入力するログイン情報がわかりません。

- **サービス企業にお問い合わせください。**

Q.3 「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。

- **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。



Q.4 ユーザーが新規に登録できません。

- **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。
お申し込みライセンス数は、トップページの契約情報で確認できます。


Q.5 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。

- **以下の手順に従って、ロックしてください。**


«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」
- 全機器一括リモートロックを行いたい場合は、[サイトマップ] → 「Android - 使用制限」の [リモートロック] →  から設定セットを作成し割り当てを行ってください。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「サイトマップ」 - 「Androidリモートロック」
 - 設定セットとリモート操作画面からの指示が競合した場合は後者が優先されます。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「機器」 - 「一覧」 - 「機器の操作」 - 「(操作-Android) リモートロック」

«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」

«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」

Q.6 Android端末の対応機種を知りたいです。

- 『Androidエージェント対応端末表』を参照してください。
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。

Q.7 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。

- **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。

Q.8 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。

- **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すでにAndroid端末に存在する場合、そのデータの登録はできません。

Q.9 連絡先配信機能で、連絡先の変更や削除はできますか。

- **連絡先の変更や削除はできません。**

Q.10 本製品の連絡先配信で、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。

- **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などを登録する場合は、連絡先を複数設定する必要があります。

Q.11 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。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- **あとから設定した設定セットを適用します。**
端末に別の設定セットがすでに適用されている場合、上書きされます。

Q.12 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。

- **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。**

Q.13 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。

- **OSがAndroid 4.0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。**

Q.14 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。

- **「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。

Q.15 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。

- **以下の場合、管理サイトで確認できます。**

- 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)」または「(同期不可)」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。
構成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。

Q.16 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。

- **以下のいずれかに該当する場合は端末側でのみ「保存されていません」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

- **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

Q.17 設定セット、設定テンプレートの編集、削除ができません。

- **設定セット、設定テンプレート名の先頭に[S]がついているものは、サービス企業で作成したものであり、編集、削除はできません。**
また、その設定テンプレートをデフォルトに設定もできません。

Q.18 機器にどんな設定を割り当てているか確認できますか。

- **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」-「機器の設定」-「(設定-Android) 設定の割り当て」、 「(設定-iOS) 設定の割り当て」、 「(設定-Windows) 設定セットの割り当て」

ただし、指示内容が反映済みかどうかは確認できません。

Q.19 ユーザーのデータをインポートしようとしたが、読み込みエラーになってしまいました。

- **Windows標準のメモ帳でCSVファイルを編集すると、読み込みエラーになる場合があります。**
CSVフォーマットに準拠する必要があるため、Microsoft Excel 2003/2007/2010で編集してください。
また、CSV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「機器」-「CSVで追加」-「インポート用のCSVファイルの構造」

Q.20 Apple Push証明書を更新するときに、どのApple Push証明書を更新したらいいかわかりません。

- **更新作業は『Apple Push証明書年次更新マニュアル』で詳細をご案内しています。**
「Apple Push 証明書を更新する」-「Apple Push 証明書をダウンロードする」の手順【1】で表示される「トピック」の値を必ずメモしておいてください。
メモした「トピック」の値と一致するApple Push証明書を手順【8】で更新してください。

Q.21 端末と同期が行われません。

- **端末側で本製品を利用するためのライセンス認証が行われていますか。**
ライセンス認証は各エージェントマニュアルの以下を参照して行ってください。

- Android…ライセンス認証を行う
- iOS…ライセンス認証(プロファイルのインストール)を行う
- Windows…エージェントをインストールする

Q.22 サイレントインストールが行われません。

- **「管理対象アプリとして配信する場合は、チェックを入れます。**
「ここにチェックが入っており、端末が監視対象端末の場合は、アプリケーションはサイレントインストールされます。」と記載されていますが、App Storeに掲載されているアプリケーションについては、Apple IDとパスワードを入力する必要があります。複数のApp Store掲載アプリケーションを設定した場合は、1回のApple IDとパスワード入力ですべてインストールが行えます。

- 省データモードが有効になっている場合は、サイレントインストールを利用できません。インストールするには、表示されるポップアップに同意する必要があります。
- 『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」

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.23 誤ったApple Push証明書を登録してしまいました。

- **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時に利用いただいた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、次の質問を参照してください。

Q.24 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。

- **同期不可検知の種類によって、対応が異なります。該当の手順に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、または管理外検知が表示された場合≫
再認証以外に復旧方法はありませので、再度認証を行ってください。

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

Q.25 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。

- **アプリケーション作成時のマニフェストファイル (plist) を利用して、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。

Q.26 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。

- **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社側の仕様準じます。

Q.27 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。

- **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」 - 「アプリケーション」 - 「オリジナルアプリ登録」


Q.28 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。

- **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

Q.29 iOS : Appとブック

「Appとブック」アプリケーションの配信に失敗します (MCMDMErrorDomain:12064)。

- **「Appとブック」アプリケーション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≫
「Appとブック」アプリケーション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、Appとブック招待時に利用したApple IDと異なる場合、「Appとブック」アプリケーション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。
 - **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
 - **ユーザーの確認方法**
 1. [ユーザー] → [一覧] →対象のユーザーを選択
 2. [「Appとブック」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「Appとブック」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後、端末側で参加依頼に同意していただいた後に、「Appとブック」アプリケーションの配信を再度お試しください。
 - ≪Appとブック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、Appとブック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、「Appとブック」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] →対象のユーザーを選択
 2. [「Appとブック」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。

Q.30 iOS : Appとブック

「Appとブック」アプリケーションの配信で、「MCMDMErrorDomain:12026」が発生します。

- **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にして電源ONにする) してください。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.31 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。

- **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があります。**

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。

Q.32 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。

- **複数の構成プロファイルを適用させた場合、パスコード・制限など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方が採用されます。

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」

Q.33 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

- **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。**

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]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。

Q.34 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

- **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 > 任意の成約を含める

Q.35 iOS : アプリケーション配信

アプリケーション配信で、ポータル表示をON、機器でアプリケーション配信設定を設定済みになっている状態で、端末側のポータル内に「配信アプリケーション一覧」の項目が表示されません。

- **以下の場合、表示されません。**

- 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。

Q.36 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。

- **2つの設定を用意することにより実現できます。**

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できます。

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。

Q.37 iOS : アプリケーション配信

管理アプリケーションとしてアプリケーション配信を行っていますが、SIMを考案した影響により、配信済みの管理アプリケーションがアンインストールされるなどの影響はありませんか。

- **SIMを交換した場合でも、配信済みのアプリケーションには影響がありません。**

Q.38 iOS : アプリケーション配信

MDM構成プロファイルの同期を行ったら「このアプリケーションは○○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った契機ですか。 ※○○は管理サイトに登録している企業名です。

- **以下の状況のときに表示されます。**

手動でインストールしたアプリケーションを、あとからオフィスまるごとサポートデバイスマネジメントで「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、強制的にオフィスまるごとサポートデバイスマネジメントから配信した状態になります。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.39 iOS : Apple Push証明書

Apple Push証明書を削除してしまい、新しいApple Push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Apple Push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。

- **管理サイトからApple Push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。

Q.40 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。

- **ブラウザによっては、表示がおかしくなることがあるようです。**
何度か再読み込み、または更新を試していただくと改善されますので、お試しください。
- **現在ご利用中のブラウザとは別のブラウザをご利用いただくと改善される場合があります。**

Q.41 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。

- **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。

Q.42 iOS : Apple Push証明書

登録済みとは別のApple Push証明書を適用後、100台中、85台が管理外になりました。
再度正常なApple Push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。

- **管理外になった原因は異なるトピック値のApple Push証明書がアップロードされたことで、同期ができなくなったことが検知されたためです。**
同じトピック値のApple Push証明書で更新し直した場合は、管理サイトから各端末に同期指示を送ることで再び管理対象に戻せます。

Q.43 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Apple Push証明書が見当たらないのですがどうすればよいですか。

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

Q.44 iOS : Apple Push証明書

「機器「○○」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。 ※○○には管理サイトで登録している機器名が表示されます。

- **Apple Push証明書の登録を新しいApple IDでやり直した可能性があります。**
対処としては、端末で再認証を行っていただく必要があります。
また、登録前のApple Push証明書を更新していただき、登録しなおす方法をお勧めしますが、そのときも再認証を行っていただく必要があります。

Q.45 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。

- **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。

Q.46 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。

- **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にしておく必要があります。**

Q.47 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。

- **機器自体に「ウイルス対策」のパッケージにチェックが入っていないかと思しますので、そちらにチェックを入れてください。**
管理サイトの「機器」から対象の端末を選択し、「パッケージ」をご確認ください。

Q.48 Android : Android N 対応

Android端末のAndroid 7.0へアップデートしたときに、Device Owner Mode未使用で利用するとこれまでとどのような違いが生じますか。

- **Device Owner Modeを未使用の場合、Android 7未満までと違い、以下の制限・利用ができなくなります。**
 - 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
 - スクリーンロックパスワード変更ができなくなります。

Q.49 iOS : Apple Push証明書

更新前と違うApple IDでApple Push証明書の更新後、正しいApple IDで再度Apple Push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。

- **更新前と異なるApple Push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Apple Push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。

Q.50 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。

- **該当の端末がApple IDで「iTunes StoreとApp Store」にサインインされていないため、発生していると思われます。**
アプリケーション配信機能では、このログが表示されている場合は、端末にApple IDでサインインされていないと動作いたしません。
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。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.51 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。

- **エージェントアプリのバージョンが「8.1」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」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。

Q.52 Android : アプリケーション配信、ウイルス対策機能

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、インストールができません。ダウンロードまでは正常に終わるのですが、インストールはできない状態ではどうしたらよいでしょうか。


- **「スキャンできませんでした」というエラーは、「Lookout for au」というセキュリティソフトが表示しています。**
回避策として端末の通知画面からインストールしてください。
ウイルス対策オプションのウイルス対策アプリの場合は、App Managerを利用してインストールをお願いいたします。

Q.53 iOS : Exchange設定

iOS端末へ配信したExchange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。

- **Apple社側の不具合が原因となります。**
iOS 10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一度削除し、再設定してください。

「機器ごとに行う場合の削除手順」

1. 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. 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] メールのみで仕様”の列の値を削除して保存する
4. 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

Q.54 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。

- **設定によりできます。**
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できる設定ですと端末上でWebクリップが削除できます。
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クリップを削除不可にするためには、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、大本の構成プロファイルを変更しただけの場合は、端末に設定が反映されないため、ご注意ください。

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


1. 管理サイトの「設定」→ [構成プロファイル] → [構成プロファイルアップロード] から対象を選択→ [その他] → [Webクリップ設定] をクリックする
2. [編集] をクリックする
3. 内容を変更せずに保存実行する

Q.55 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、「Appとブック」アプリケーション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。どうしたらよいでしょうか。

- **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

Q.56 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App Store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。

- **状況により異なります。**
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、運用方法に沿った端末設定、アプリケーション配信の方法をご利用ください。

「Apple IDの入力が不要な条件」

以下のすべての条件を満たしていること。
ただし、「Appとブック」利用で機器にライセンスを割り当てて配信している場合は、条件を満たしていても、Apple ID入力は不要となる。

1. Apple IDのログインを事前に行っている
2. App Storeの利用規約が更新されていない
3. 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

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)


株式会社オプティム
(c)東日本電信電話株式会社

Q.57 iOS : アプリケーション配信

iOS 10以上のiPhone SE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。オフィスまるごとサポートデバイスマネジメント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。

- **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

Q.58 iOS : Appとブック

「Appとブック」アプリケーションを配布した後、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。

- **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
 - App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

Q.59 iOS : Appとブック

「Appとブック」アプリケーションを配布した後、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。

- **オフィスまるごとサポートデバイスマネジメントでは、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オフィスまるごとサポートデバイスマネジメントから自動的に配信が行われないようにできます。

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
 - App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

Q.60 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。

- **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。

Q.61 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。

- **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」 - 「アプリケーション」 - 「アプリケーション配信」

Q.62 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。

- **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確認をお願いいたします。

1. [機器] → [一覧] クリックする
2. 対象端末を選択 →  をクリックする
3. 「情報」の[アプリケーション] をクリックする
4. 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

Q.63 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。

- **オフィスまるごとサポートデバイスマネジメントでは、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。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧


最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.64 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。

● 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。

Q.65 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、あらた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。

● 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、同期のたび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場合、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。

Q.66 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。

● 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. [x] 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

Q.67 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。

● 設定によりできます。

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」

Q.68 iOS : Apple Push証明書

Apple Push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。

● 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。

- Apple ID自体は変更しないでください。
- Apple ID自体を変更してApple Push証明書を更新すると、それまでに認証した機器への同期ができなくなります。

Q.69 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。

● 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. Google 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

Q.70 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。

● Android 6.0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。

Q.71 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。

● 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。

Q.72 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Google 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。

● Google 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、Google 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。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.73 iOS : ADE

管理サイトのADE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。

● Apple社のApple Business Manager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、ADE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（Apple Business Manager）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ADE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ADEトークンをアップロードしてください。

- 以下のマニュアルを参照し、更新作業を行う
 - 『Apple Business Manager (ABM) マニュアル (利用方法・年次更新手順)』の「Automated Device Enrollment (ADE)」 - 「ADEトークンの年次更新」
- 管理サイトの「設定」→「iOS」→「ADE」→「ADE機器管理」をクリックする
- 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
 - 表示されない場合は、「ADEと同期」をクリックしてください
 - 登録したADEトークンを削除しないようご注意ください

Q.74 iOS : ADE

ADE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。

● 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。

- 管理サイトの「設定」→「iOS」→「ADE」→「ADE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「ADE定義プロファイル」を作成する
- 「機器」→「一覧」→一覧より対象を選択→→「設定」の「設定の割り当て」→「ADE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
- 対象端末の初期化を行う
- 初期化が終了し、非監視対象モードになる

Q.75 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の変更はできますか。

● 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。担当営業にお問い合わせください。

Q.76 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。

● 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。

すでにアプリケーション配信を実施し、その後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。

- 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
- 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
- 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
- 端末に、アプリケーションDのみ配信される

Q.77 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。

● Apple社の仕様になります。

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、オフィスまるごとサポートデバイスマネジメントではなく、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。

Q.78 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。

● 以下のようになっていると、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。

- 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。
- 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。

Q.79 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。

● 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。

Q.80 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。

● 再び、同期を行えるようにするためには、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。

- 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構成プロファイルについて」 - 「MDM構成プロファイルをアンインストールする」
- 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「ライセンス認証を行う」、「ADEを利用してライセンス認証を行う」
 - ADE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する手順となります。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.81 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。

- **管理サイトからAndroidのアプリケーション配信が行われた場合、端末側では同期のタイミングでアプリケーション配信が行われます。**
手順は以下のようになります。
 1. 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が表示されます。端末利用者はポップアップ画面で [OK] を押してください。
 2. 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。
 3. 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ときの端末の手順については、以下を参照してください。
 - 『Androidクライアント リファレンスマニュアル』の「管理サイトからの指示による動作」 - 「アプリが配信された場合（従来版エージェント）」
 - アプリケーション配信設定については、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 - Android」 - 「アプリケーション」 - 「アプリケーション配信」
 - Google 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。

Q.82 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。

- **アプリケーション禁止で禁止したアイコンを非表示にはできません。**

Q.83 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。

- **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] をクリックする

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。

Q.84 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。

- **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 Modelになっている。

Q.85 Android : スクリーンロック

スクリーンロックが実行されたときに、画面にメッセージを出せますか。

- **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。**

Q.86 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ださい。


- **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（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。

Q.87 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ください。

- **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。**
この状態のときには、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。

Q.88 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ください。

- **以下の手順で確認できます。**
iOS : アクティベーションコード
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。

Q.89 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。

- **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。

Q.90 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。

- **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てられていなかった可能性があります。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.91 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。

- **端末側の操作で再度認証していただく必要があります。**
 - 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。
 - Android（従来版）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。
 - Android（ストア版）の場合
端末の初期化以外の方法では、再び管理下に設定することは出来ません。
詳細は、「Androidキッティングマニュアル」7 端末の所有者を変更する を参照ください。

Q.92 管理者のユーザーIDの変更するにはどうしたらよいでしょうか。

- **[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。

Q.93 iOS : ADE

ADE端末を追加登録したときに、オフィスまるごとサポートデバイスマネジメント側に反映されません。どうしたらよいでしょうか。

- **以下の手順をお試しください。**
お客様環境の管理サイトの「ADEトークン登録」画面で、「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≫
「ADE機器再読込」をクリックしていただき、「ADE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ビジネスマネージャーサイト」より、再度ADEトークンを取得します。
その後、オフィスまるごとサポートデバイスマネジメントの「ADEトークン登録」へアップロードを行い、「ADE機器再読込」をクリックして、ご確認ください。


1. 以下のマニュアルを参照し、更新作業を行う
 - 『Apple Business Manager (ABM) マニュアル (利用方法・年次更新手順)』の「Automated Device Enrollment (ADE) 」 - 「ADEトークンの年次更新」
2. 管理サイトの [設定] → [iOS] → [ADE] → [ADE機器管理] 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。
 - 表示されない場合は、[ADEと同期] をクリックしてください。
 - 登録したADEトークンを削除しないようご注意ください。

Q.94 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。

- **Appleの仕様となり申し訳ございません。**
Appleの仕様により、MDM（オフィスまるごとサポートデバイスマネジメント）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

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
 - 「マップ」アプリケーションのStoreIDは「915056765」
 - 「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

Q.95 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。

- **影響はありません。**
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。

Q.96 リモートワイブはキャンセルできますか。

- **リモートワイブのキャンセルはできません。**

Q.97 iOS : Appとブック

「Appとブック」アプリケーションの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ください。
「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)」

- **「Appとブック」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。

Q.98 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ください。

- **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つ設定する必要があります。

FAQ一覧

例)
"https://mdm.sdm.ntt-east.net"
"http://mdm.sdm.ntt-east.net"

■ 目次

[管理サイト](#)

[Androidエージェント](#)

[iOSエージェント](#)

[Windowsエージェント](#)

[サービス企業用サイト](#)

[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.99 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。

- **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。**
 - **Android 7.0以上の場合**
Device Owner Mode、またはAndroid Enterpriseで利用いただく必要があります。
Device Owner Mode、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。
 - **「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。

Q.100 「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。

- **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「制限なし」にするだけでは、端末のパスワードポリシーを解除できません。

Q.101 iOS : ADE

ADE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。

- **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。


Q.102 iOS : ADE

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

- **ADEとオフィスまるごとサポートデバイスマネジメントサーバーの同期が行われていない可能性があります。**
ADEトークン登録を実施後、再度お試しください。
◀ADE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
 - 『Apple Business Manager (ABM) マニュアル (利用方法・年次更新手順)』の「Automated Device Enrollment (ADE)」 - 「ADEトークンの年次更新」
 2. 管理サイトの「設定」→ [iOS] → [ADE] → [ADE機器管理] 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、「ADEと同期」をクリックしてください
 - 登録したADEトークンを削除しないようご注意ください


Q.103 iOS : 機器情報

端末の監視対象モードの設定が、有効か無効かを確認する方法はありますか。

- **以下の手順で、確認できます。**
◀管理サイトでの確認手順▶
 1. [機器] → [一覧] → 対象機器を選択 →  → 「情報」の [デバイス] をクリックする
 2. 「監視対象」を確認する
◀iOS端末での確認手順▶
 1. 設定アプリをタップする
 2. 設定アプリの最上部的表示を確認する
 - 有効の場合は、「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。」と表示されています。
 - OSのバージョンによっては、文言が異なることがあります。
 - 監視対象の iPhone、iPad、iPod touch を使う場合は、以下を参照してください。
 - <https://support.apple.com/ja-jp/HT202837>


Q.104 管理 サイト : 機器情報

管理サイトで端末のシリアル番号を確認する方法はありますか。

- **以下の手順で、シリアル番号を確認できます。**
 1. [機器] → [一覧] → 対象機器を選択 →  → 「情報」の [デバイス] をクリックする
 2. 「基本」の「シリアル番号」を確認する
 - Android端末では、機種によってはシリアル番号が取得できない場合があります。詳細は以下を参照してください。
 - 『Androidエージェント対応端末表』

Q.105 管理 サイト : 機器情報

機器にユーザーが紐付いているか、確認する方法はありますか。

- **以下の手順で、機器に紐付いているユーザーを確認できます。**
 1. [機器] → [一覧] → 対象機器を選択 →  をクリックする
 2. 「ユーザー」を確認する
 - 機器にユーザーが紐付いていない場合は、「(なし)」と表示されます。

Q.106 iOS : 構成プロファイル

端末ユーザーが、「iPhoneを探す」の設定を変更できないようにする方法はありますか。

- **以下の手順で「構成プロファイルアップロード」を指定すると、端末ユーザーが設定を変更することはできません。**
 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] → [iOS制限設定] → [機能の制限] をクリックする
 2. [新規作成] または [編集] をクリックする
 3. 「アカウント設定の変更を許可 (監視対象のみ)」のチェックを外す
 4. [保存] をクリックする
 - 本機能は監視対象の端末でのみ利用できます。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧


最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.107 管理 サイト：機器情報

管理サイトの機器画面に表示される各端末の「機器名」を編集する方法はありますか。


● 以下の手順で、「機器名」を変更できます。

1. [機器] → [一覧] → 対象機器を選択 →  → [管理情報の編集] をクリックする
2. 「機器名」を変更する
3. [保存] をクリックする
 - CSVのアップロードでも機器名を編集することができます。詳細については、以下を参照してください。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「CSVで編集」
- 端末側から変更することはできません。

Q.108 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をする方法はありますか。

● 以下の手順で、配信済みオリジナルアプリのアップデートができます。

1. [設定] → [iOS] → [アプリケーション] → [オリジナルアプリ登録] をクリックする
2. 新しいバージョンのアプリ設定を新規で作成する
 - アプリケーションIDが同一のものは、3つまで作成できます。
3. [設定] → [iOS] → [アプリケーション] → [オリジナルアプリ登録] → 該当の設定を選択する
4. 「オリジナルアプリ一覧」の  をクリックする
5. 「2.」で作成した設定を追加する
6. [保存] をクリックする
7. 端末に設定を適用して、同期を行う
 - アップデート時の留意事項などについては、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」 - 「オリジナルアプリ登録」

Q.109 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、DM Browserなどの任意のブラウザで使用できますか。

● 使用できません。Safari向けの機能です。

Q.110 iOS：ADE

ADE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。どうしたら解消されますか。

● ネットワークの接続状態に問題がないか確認のうえ、管理サイトで生成・紐付けした機器情報の同期を行ってください。

- 解消しない場合は、端末の初期化と再アクティベートを行ってください。

Q.111 Android：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、発生する原因を教えてください。

● Googleポリシー変更に伴いオフィスまるごとサポートデバイスマネジメント ver.9.3.104.0以降から、オフィスまるごとサポートデバイスマネジメントのデバイス管理者権限を端末操作で変更できます。

端末操作者が端末から[設定] → [セキュリティ] → [端末管理アプリ] の「オフィスまるごとサポートデバイスマネジメント」のチェックを外すと、デバイスマネジメント エージェントのデバイス管理者権限が無効になり、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管理者は、端末操作者にデバイス管理者権限を再度有効に設定するよう促し、今後は無効に設定しないよう喚起してください。「デバイス管理者権限」が無効に設定されている場合は、以下の機能が利用できません。


- スクリーンロックポリシー（強制されず自由に変更できる）
- カメラ禁止機能（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）
 - リモートロックは、OS標準のスクリーンロックが利用できなくなります。独自リモートロックは「デバイス管理者権限」が無効に設定している場合でも利用できます。
- Androidエージェントのアンインストール抑止機能
- Android 7以降では、オフィスまるごとサポートデバイスマネジメント ver.9.3.104.0以前からDevice Owner Modeを利用しないと、アンインストールができません。
- 「デバイス管理者権限」が無効時にアンインストールを行うと、管理サイトにアンインストール失敗のログが表示されます。

Q.112 Android：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はありますか。

● 以下の手順で、Device Owner Modeのセキュリティ設定の両方を行ってください。

- 従来版の認証方法では、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を利用してください。

1. [設定] → [Android] → [Device Owner Mode] → [セキュリティ設定] をクリックする
2.  をクリックして、新規で作成する
3. 「設定名」を入力する
4. 「ステータスバー」の「無効にする」にチェックを入れる
5. [保存] をクリックする
6. 端末に設定を適用して、同期を行う

Q.113 Android：連絡先

配信済みの連絡先の内容を変更して再度配信すると、変更内容が反映されません。

● 配信済みの連絡先に対し、更新や削除を行うことはできません。

連絡先を配信したときに、すでに「姓」「名」「電話番号」が一致している連絡先がある場合は、連絡先を配信することはできません。「姓」「名」「電話番号」の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。

Q.114 Android：Android Enterprise

Android Enterprise導入時に、Googleアカウントを新規で作成して登録を行うと「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が、どうしたらよいですか。

● Googleアカウント作成時に入力した生年月日が、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。

以下の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。

1. <https://support.google.com/accounts/answer/1350409?hl=ja>

Q.115 Android：ウイルス対策

ウイルス対策「モバイルウイルス対策」の契約をしていますが、管理サイトで該当の設定項目がありません。原因を教えてください。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント


サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- **本製品で提供しているウイルス対策ソフト「モバイルウイルス対策」を利用する場合は、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です。**
以下の手順で、パッケージを割り当てます。

1. [機器] → [-一覧] → 対象機器を選択 →  → 「設定」の[他の設定を見る] → [パッケージ] クリックする
2. [編集] クリックする
3. オプションパッケージの「ウイルス対策ソフト」にチェックを入れる
4. [保存] クリックする

- オプションパッケージの割り当て、およびウイルス対策ソフトの詳細については、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「機器」 - 「一覧」 - 「機器の設定」 - 「(設定 - Android) パッケージ」
- 『管理サイト リファレンスマニュアル』の「機器」 - 「一覧」 - 「機器の情報」 - 「(情報 - Android) ウィルス対策ソフト」

Q.116 iOS : 構成プロファイル

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


- **iOS 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には、以下の設定が必要です。**

- iOS 11.3未満でも発生する場合は、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、以下の設定を行う。**

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] → [iOS制限設定] → [機能の制限] をクリックする
2. [新規作成] または [編集] をクリックする
3. 「管理対象外出力先で管理対象ソースからの書類を許可」のチェックを外す
4. [保存] クリックする

- **MDMで配信する連絡帳の読み込みを行う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] をクリックする
2.  をクリックして、新規で作成する
3. 「オリジナルアプリ一覧」または「App Storeアプリ一覧」に管理対象にしたいアプリケーションを入力する
4. 「管理」の有効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、必ず配信済みの管理対象アプリも含めた設定を作成してください。設定に含まれていないアプリは、配信時にアンインストールされます。
 - 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」の有効にチェックを入れてください。
5. 端末に設定を適用して、同期を行う
6. 端末側へ同期されると、「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。」というポップアップ画面が表示される
7. [管理] をタップする

Q.117 iOS : OSアップデート

管理サイトからOSアップデートを実行しても、iOS端末がアップデートされません。どうしたらよいですか。

- **機器のログ、もしくは端末の状況を確認してください。**

未知のエラーが発生した場合、およびiOS端末が以下の状態の場合は、アップデートできないことがあります。

- ダウンロードまたはインストールに必要なディスク容量が不足している
- ダウンロードまたはインストールに必要なバッテリー残量が少ない
- ダウンロード可能なWi-Fiネットワーク接続状態ではない(モバイル通信など)
- 通話のためインストールが中断された

Q.118 iOS : 構成プロファイル

App Storeを非表示にする方法を教えてください。

- **以下の手順で構成プロファイルの制限を設定することで、App Storeを非表示にできます。**

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] → [iOS制限設定] → [新規作成] または [編集] をクリックする
2. 「Apple Configurator 2 および iTunes からの App のインストールを許可」または「App Store からの App のインストールを許可(監視対象のみ)」のチェックを外す
 - 「App StoreからのApp のインストールを許可(監視対象のみ)」は、監視対象かつiOS 9.0以降の端末のみ設定できます。
3. [保存] クリックする
4. 端末に設定を適用して、同期を行う

- 構成プロファイルの制限設定については、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」 - 「[iOS制限設定] タブ」 - 「画面 (機能の制限)」

Q.119 iOS : 構成プロファイル

iOS端末で利用できるアプリケーションの一部を制限する方法を教えてください。

- **以下の手順で構成プロファイルの制限を設定することで、利用できるアプリケーションの一部を制限できます。**

- 監視対象端末のみ設定できます。

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] → [iOS制限設定] → ([新規作成] → [Appの制限]) または ([Appの制限] → [編集]) をクリックする
2. 「Appの使用を制限(監視対象のみ)」をドロップダウンリストから以下のどちらかを選択する
 - ・許可するアプリケーションを指定する場合は「一部のAppのみを許可」
 - ・禁止するアプリケーションを指定する場合は「一部のAppのみを許可しない」
3. 「アプリケーションID (Bundle Identifier)」に対象のアプリケーションIDを入力する
4. 端末に設定を適用して、同期を行う

- 構成プロファイルの制限設定については、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」 - 「[iOS制限設定] タブ」 - 「画面 (Appの制限)」

«アプリケーションIDの確認方法»

- **すでに端末にインストールしている場合**

1. 端末の設定から [機器] → [対象機器] → [詳細] → [情報] → [アプリケーション] をタップする
2. 対象アプリケーションの右端の [詳細] をタップする

- **端末にインストールしていない場合**

1. 「iTunesプレビュー」サイトを起動する
2. 該当のアプリケーションを検索する
3. 該当アプリケーションのページURLの「id」以降の数字を確認する
4. 「http://itunes.apple.com/lookup?country=JP&id=」の末尾に手順3で確認した数字を入れて、Webで検索する
5. ダウンロードしたテキストファイルを開いて、アプリケーションIDを確認する
 - 「bundleId」がアプリケーションIDになります。

- アプリケーションIDの調べかたの詳細については、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」 - 「アプリケーション検知」 - 「アプリケーションIDの調べかた」

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.120 iOS : DM Browser

iOS端末にユーザーが手動でお気に入り登録したWebページが、DM Browserを再起動するとお気に入りから消えてしまいます。どうしたらよいですか。





- **Webフィルタリングの設定で、以下の場合は、端末からお気に入り登録すると消えてしまいます。**
URLを確認して、以下に該当しないように、Webフィルタリングの設定を変更してください。
 - ・「許可するURLを指定する」に設定していて、許可していないWebページは、お気に入りから削除されます。
 - ・「禁止するURLを指定する」に設定していて、禁止にしているWebページは、お気に入りから削除されます。
 - Webフィルタリングの詳細については、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」-「インターネット」-「Webフィルタリング」

Q.121 Android : DM Browser

Android端末でDM Browserをデフォルトブラウザにする方法を教えてください。

- **以下の手順で、DM Browserをデフォルトブラウザにできます。**
 - **Android端末で設定する場合**
 - **デフォルトブラウザを選択していない場合**
 1. ブラウザーのアプリケーションをタップする
 2. デフォルトブラウザ選択のダイアログで「DM Browser」を選択する
 3. [常時を選択] する
 - Android 12 以上は、デフォルトブラウザ選択のダイアログは表示されません。「[Chrome]」などを、すでにデフォルトブラウザにしている場合」の手順で、デフォルトブラウザにしてください。
 - **「Chrome」などを、すでにデフォルトブラウザにしている場合**
 1. [設定] → [アプリ] → [歯車マーク] → ブラウザーのアプリケーションで、「DM Browser」を選択する
 - **管理サイトで設定する場合**

アプリケーション非表示の設定で、「DM Browser」以外のブラウザのアプリケーションを制限します。以下の2つの条件が満たされている必要があります。

 - ・ Androidエージェントのバージョンがverver9.5.101.0以上のストア版である
 - ・ Device Owner Modeが有効である
 1. [設定] → [Android] → [Device Owner Mode] → [アプリケーション非表示] をクリックする
 2.  をクリックして、新規で作成する
 3. 「設定名」を入力する
 4. [保存] をクリックする
 5. 「対象アプリケーション」の  をクリックする
 6. 制限するブラウザの「アプリケーション名」と「パッケージ名」を入力する
 -  をクリックして、複数登録できます。
 7.  をクリックする
 8. 端末に設定を適用して、同期を行う
 - 設定するアプリケーションにより、OSの動作に支障をきたす場合があります。
 - アプリケーション非表示の詳細については、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-Android」-「Device Owner Mode」-「アプリケーション非表示」

Q.122 Android : アプリケーション禁止

電話がかかってきたとき端末に着信画面が表示されません。原因を教えてください。

- **以下の場合は、電話がかかってきたとき端末に着信画面が表示されません。**
 - ・ 「アプリケーション禁止」の設定で、関連アプリケーションを禁止している
 - ・ 端末の設定で、電話がかかってきたときの着信画面が表示されないようにしている
 - **確認手順**
 1. 該当端末に電話をかける
 - ⇒ 端末に「〇〇（禁止アプリケーション名）がアプリケーション禁止によって禁止されました」とポップアップが表示されたら、着信に関連するアプリケーションが「アプリケーション禁止」によって禁止されています。
 2. 「アプリケーション禁止」の設定で、ポップアップに表示されているアプリケーション名を許可する
 - 「アプリケーション禁止」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-Android」-「アプリケーション」-「アプリケーション禁止」
 3. 端末に同期する
 4. 再度、手順1を実行して、端末に着信画面が表示されることを確認する
- 上記の手順で、端末に着信画面が表示されない場合は、端末側の通知設定を確認してください。
- 「アプリケーション禁止」設定と端末の通知設定に問題がなく、着信画面が表示されない場合は、Device Owner Mode利用時の障害が発生している可能性があります。パートナー通知を確認してください。

Q.123 Android : Android Enterprise

Android Enterpriseで配信したアプリケーションを自動バージョンアップさせる条件を教えてください。

- **Managed Google Playストアで、公開したアプリケーションおよび限定公開アプリは、以下の条件を満たすと自動アップデートします。**
 - ・ managed Google Playストアにアプリケーションの最新バージョンを公開している
 - ・ 限定公開アプリは、managed Google PlayストアにAPKファイルの最新バージョンをアップロードしている
 - ・ アプリケーション配信の設定で該当アプリケーションを「指定アプリのみインストール可能」で登録していて、「強制インストール」にチェックが入っている
 - ・ Google Playストア上で「ネットワークの指定なし」または「Wi-Fi経由のみ」を設定している
 - アップデートの挙動は、Googleの仕様です。
 - OSバージョン、Google Playストアのバージョンにより表示が異なる場合があります。

Q.124 Android : Android Enterprise

Android Enterpriseを利用している端末で、プリインストールアプリのアップデートを行う設定方法を教えてください。

- **管理サイトで設定する必要はありません。**
プリインストールアプリは、以下の条件を満たしているとアップデートします。
 - ・ managed Google Playストアにアプリケーションの最新バージョンが公開している
 - アップデートの挙動は、Googleの仕様です。
 - OSバージョン、Google Playストアのバージョンにより表示が異なる場合があります。
 - プリインストールしているオリジナルアプリが、managed Google Playストアに公開していない場合は、アップデートできません。

Q.125 Android : Android Enterprise

Android端末にWebクリップを配信できますか。

- **Webクリップの配信は、iOSが提供している機能です。**
Androidでは、Android Enterpriseが提供しているウェブアプリを配信する方法があります。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト





用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- iOSのWebクリップとAndroid Enterpriseのウェブアプリが、同じ動作になるか事前に確認してください。

「ウェブアプリの配信手順」

1. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [個別アプリケーション] をクリックする
2.  をクリックして、新規で作成する
3. 「アプリ設定名」を入力する
4. [アプリを選択する] をクリックする
5. [ウェブアプリ] をクリックする
6.  をクリックして、新規で作成する
7. 「タイトル」と「URL」を入力する
8. [作成] をクリックする
9. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [アプリケーション配信] をクリックする
10.  をクリックして、新規で作成する
11. 「配信設定名」を入力する
12. 「指定のアプリのみインストール可能」を選択する
13.  をクリックして、手順1~8で作成した設定を「アプリ個別設定」に選択する
 - 強制インストールしたい場合は、「強制インストール」にチェックを入れる
14. [保存] をクリックする
15. [ユーザー] → [一覧] → 対象のユーザーを選択する
16. [その他] → [設定] → [編集] をクリックする
17. 手順9~14で作成した設定を「Android Enterpriseアプリ配信設定」に選択する
18. [保存] をクリックする
19. 端末に設定を適用して、同期を行う

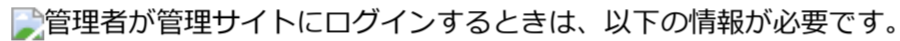
Q.126 iOS : ホーム画面レイアウト

iOS端末のホーム画面でアプリケーションの移動ができません。原因を教えてください。

- **ホーム画面レイアウトの設定を端末に適用していると、端末のホーム画面でアプリケーションの移動ができません。**
端末のホーム画面でアプリケーションの移動をしたい場合は、ホーム画面レイアウトの設定を変更します。
 - 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」-「便利機能」-「ホーム画面レイアウト（監視対象のみ）」

Q.127 管理サイト : ユーザー

管理者のログイン情報を変更する方法を教えてください。

- **以下の手順で、管理者ユーザーの情報を変更できます。**
-  管理者が管理サイトにログインするときは、以下の情報が必要です。
- 企業コード
 - ユーザーIDもしくはメールアドレス
 - パスワード
1. [ユーザー] → [一覧] → 対象のユーザーを選択する
 2. 「管理情報」の [編集] をクリックする
 - ユーザーID、メールアドレス、パスワードを確認します。
 3. 「名前」、「ユーザーID」もしくは「メールアドレス」を変更する
 4. [保存] をクリックする
 5. 「パスワード」の [編集] をクリックする
 6. 「新規パスワード」「新規パスワード(再入力)」を入力する
 7. [保存] をクリックする

Q.128 管理サイト : 同期

端末の時刻が大幅にずれている場合は、同期などに問題はありませんか。

- **端末の時刻が大幅にずれていると、同期ができずオフィスまるごとサポートデバイスマネジメントの基本的な機能に影響がでます。**
オフィスまるごとサポートデバイスマネジメントエージェントと管理サーバーは、SSL通信を行っており、時刻が大幅にずれていると、同期ができません。
そのためリモートロックやリモートワイプを含め全般的に設定の変更を受付できなくなります。
また、位置情報や各種ログの送信ができません。


Q.129 iOS : 構成プロファイル : 同期

構成プロファイルのコンテンツフィルタ設定で、「アダルトコンテンツを制限」に設定したら、アダルトコンテンツに分類されないWebページも制限されました。対処法を教えてください。

- **アダルトコンテンツに分類しないWebページのURLを「許可されたURL」に登録してください。**
 - コンテンツフィルタ設定の詳細については、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」-「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/コンテンツフィルタ設定」-「画面（フィルタ・タイプ：アダルトコンテンツを制限）」


Q.130 Android : Android Enterprise

Android Enterpriseでアプリケーション配信をしても、端末にアプリケーションがインストールされません。Google Playストアをタップすると、Managed Google Playストア画面にならず、ログインを求められます。原因を教えてください。

- **Android Enterpriseの連携が完了していない可能性があります。**
以下の手順で、「Android Enterpriseユーザー」が「連携済」か確認してください。
1. [機器] → [一覧] を表示します
 2. 対象のAndroid端末の機器名または「詳細」の  をクリックする
 3. 「情報」の [デバイス] をクリックする
 4. 「Android Enterprise」パネルの「Android Enterpriseユーザー」が「連携済」と表示している
 - 「(Unknown)」と表示している場合は、以下を確認してください。
 - 端末がAndroid Enterpriseを利用できる方法でキッキングしているか
 - 端末にユーザーが紐づいているか
 - 紐づいていない場合は、[機器] → [一覧] 画面→対象のAndroid機器を選択して、[>] → [管理情報の編集] で、ユーザーを選択してください。
 - 端末が組織に紐づいている場合は、組織をユーザーに紐づけてから、ユーザーを端末に紐づけてください。
 - 詳細については、以下を参照してください。
 - 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」-「アプリを強制インストールする」-「組織（ユーザー）にアプリケーション配信設定を割り当てる」、「端末にユーザーを割り当てる」
 - Android端末の [設定] → [アカウント] で、「仕事用アカウント」以外のアカウントをログインしている場合もAndroid Enterpriseの利用ができません。

Q.131 iOS : ADE

ADE機器をオフィスまるごとサポートデバイスマネジメントの登録機器から削除するにはどうしたらよいですか。

- **以下の手順で、機器を削除してください。**
1. [機器] → [一覧] を表示します
 2. 対象のADE機器の機器名または「詳細」の  をクリックする

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント


Windowsエージェント



サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

3. 設定の [設定の割り当て] をクリックする
4. [ADE定義プロファイル] [編集] をクリックする
5. 「(設定なし)」を選択して、[保存] をクリックする
6. [同期] をクリックする
7.  をクリックする
8. [この機器を削除する] をクリックする
9. ABMのサイトにログインして、「デバイスの割り当て」をクリックする
10. 「1.デバイスの選択」で、端末のシリアル番号を登録する
11. 「2.操作の選択」の「デバイスの割り当て解除」で、以下のどちらかを選択する

- ・デバイスの割り当て解除
 該当の企業への割り当てを解除します。
- ・デバイスの所有を解除
 ADE端末の登録情報を削除します
 - 「デバイスの所有を解除」すると、ABMからシリアルを登録して、再割り当てができなくなります。再度、ADE機器にする場合は、Apple Configurator2でADE化してください。

Q.132 管理サイト：認証手順 ライセンス認証解除のパスワードの確認方法を教えてください。

● 以下の手順で、確認してください。

1. [設定] → [Android] または [Windows] → [アプリの通信と動作] をクリックする
2. 「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」に表示しているパスワードを確認する
3. 詳細については、以下を参照してください。
4. 『管理サイト リファレンスマニュアル』の「設定 - Android」 - 「管理アプリの通信と動作」
5. 『管理サイト リファレンスマニュアル』の「設定 - Windows」 - 「管理アプリの通信と動作」

Q.133 iOS：MDM構成プロファイル：同期 通信日時（MDM構成プロファイル）が更新されず、同期ができません。どうしたらよいですか。

● 以下の方法を1から順に試してください。

- ・ 該当機器がインターネット接続可能な状態で行ってください。
1. 端末を再起動する
 2. 端末のポータルから同期を行う
 - 「サービス環境設定」でポータルを表示状態にしている場合»
 - ・ 端末のホーム画面に表示されているポータルから同期を行う
 - 「サービス環境設定」でポータルを非表示にしている かつ iOSエージェントをご利用の場合»
 - ・ 端末でエージェントを起動し、左上のメニューボタン「≡」からポータルを開き、同期を行う
 - 「サービス環境設定」でポータルを非表示にしている かつ iOSエージェントを利用していない場合»
 - ・ こちらの方法は行えません
 3. 管理サイトから同期を行う
 4. 再認証（再キッティング）を行う
 - 対象機器がADE端末の場合は、初期化を伴います。

Q.134 管理サイト：解約 MDMを解約したいです。解約時に管理サイト側、端末側で何か操作が必要でしょうか。

● はい。解約前に以下の操作を行ってください。

- 端末からエージェントおよび構成プロファイルをアンインストールする
- Android端末の場合»
【従来版エージェント】
1. アプリ [デバイス管理 エージェント] を起動する
 2. [ライセンス解除] をタップする
 - パスワードを求められる場合は、管理サイトの以下の項目を確認してください。
[設定] → [Android] → [管理アプリの通信と動作] 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」欄
 3. [アンインストール] をタップする
- 【ストア版エージェント】
- ・ ストア版エージェントではライセンス解除およびアンインストールはできません。以下の手順で初期化を行ってください。
1. アプリ [デバイス管理 エージェント] を起動する
 2. [終了] をタップする
 - パスワードを求められる場合は、管理サイトの以下の項目を確認してください。
[設定] → [Android] → [管理アプリの通信と動作] 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」欄
 3. [端末初期化] をタップする
- iOS端末の場合»
【ADE利用なし】
1. [設定] → [一般] → [デバイス管理] → [デバイス管理 エージェント] をタップする
 2. [削除] をタップする
 - 構成プロファイルを「削除禁止」で配信している場合は [削除] ボタンからの削除ができません。 [削除] ボタンがない場合は、設定アプリから端末の初期化を行ってください。
 3. ホーム画面から [Device Management] を長押しして「×」をタップする
 - エージェントアプリをインストールしていない場合は手順3は不要です。
- 【ADE利用あり】
1. [設定] → [一般] → [デバイス管理] → [デバイス管理 エージェント] をタップする
 2. [削除] をタップする
 - 構成プロファイルを「削除禁止」で配信している場合は [削除] ボタンからの削除ができません。 [削除] ボタンがない場合は、設定アプリから端末の初期化を行ってください。
 3. ホーム画面から [Device Management] を長押しして「×」をタップする
 - エージェントアプリをインストールしていない場合は手順3は不要です。
 4. 管理サイトの [機器] → 該当機器を選択 → [設定の割り当て] → [ADE定義プロファイル] にて設定しているADE定義プロファイルを外し [保存] をクリックする
 5. [設定] → [iOS] → [ADE] → [ADE機器管理] にて [ADEと同期] をクリックする
- 管理サイトから機器を削除する
- 基本プランの場合»
1. [機器] → [一覧] をクリックする
 2. エージェントおよび構成プロファイルをアンインストールした機器の左にあるチェックボックスにチェックを入れる
 3. 「削除」の下にある [実行] をクリックする

Q.135 管理サイト：通信量 管理サイトで端末の通信量を確認することはできますか。

● 管理サイトで端末の通信量を確認することはできません。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.136 iOS : ADE

ADE状態が"削除済"であり、ステータスが"除外"となっている端末を再度MDMで管理したいのですが、どうしたらいいですか。

- **除外解除およびADE定義プロファイルの割り当てを行うことで、再度MDMにて管理が可能となります。**
除外解除の手順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)』の「Automated Device Enrollment (ADE)」 - 「ADE端末のADEの利用を解除・再開する」 - 「ADEの利用を再開する」

Q.137 管理サイト：機器

管理サイトにて電話番号の情報が表示されません。原因と対処法を教えてください。

- **SIMカードが挿入されていないまたは、端末がSIMカードを認識していない可能性があります。SIMカードの状態をご確認ください。**
管理サイトの仕様では、端末にSIMが挿入されているとき、SIMの持っている電話番号情報を取得して、該当項目へ表示します。SIMを挿入していない状態または、端末がSIMカードを認識していない状態で電話番号情報を取得すると、電話番号の項目は空欄となります。

Q.138 iOS : アプリケーションレポート

アプリの名称がApp Store上とアプリケーションレポート上で異なっている原因を教えてください。

- **表記が異なる原因は、App Store上で表示されるアプリ名称と、アプリケーションが保持しているアプリ名称が別物であり、提供者によるアプリ名称の設定が異なるためとなります。**
管理サイトで取得しているアプリ名称は、アプリケーションが保持しているアプリ名であるため、App Store上にあるアプリ名称とは同一ではありません。
App Store上のアプリ名称は提供者が任意で設定が可能なため、アプリ名称が必ずしもアプリケーションレポートのアプリ名称と、同一もしくは正式名称とならない場合がございます。

Q.139 管理サイト：機器レポート

端末のUDIDを一括で確認する方法を教えてください。

- **以下の手順にてご確認ください。**
 1. [機器] → [CSVをダウンロード] → [機器レポート] をクリックする
 2. [ios:機器] のチェックボックスにチェックを入れる
 3. [レポート作成] をクリックする
 4. レポート作成完了後に [CSVダウンロード] をクリックする
 5. ダウンロードしたCSVファイルの項目：「[I:iOS]UDID」より確認する

Q.140 iOS : ADE

Apple Configurator 2でADEに接続するとき、入力するMDMサーバのURLを教えてください。

- **「MDMサーバのホスト名またはURL」に、以下のURLを入力してください。**

https://mdm.sdm.ntt-east.net/企業コード/setup/ios/dep_enroll?auth_code=認証コード
 - ・ 企業コード、認証コードは、管理者へお問い合わせください。

Q.141 Wi-Fi

iPhone/iPad利用時、固定IPアドレスでの運用をしています。管理サイトからSSIDを設定する際に、端末毎にIPアドレスを割り当てることはできますか。

- **管理サイトから端末毎にIPアドレスを設定することはできません。**

Q.142 Windows : アプリケーション一覧、アプリケーションレポート







アプリケーション一覧やアプリケーションレポートなどのWindowsアプリケーション機能に表示されないユーザーがいます。

- **ユーザー数が10ユーザーを超えていますか。**
表示されるユーザーは、最大10ユーザーまでです。11人目以降のユーザーは表示されません。
- **端末がアクティブディレクトリに接続できていますか。**
アクティブディレクトリが停止しているなどで端末と接続されていない場合は、ドメインユーザーの情報が送信できないため、管理サイトにユーザーが表示されません。

Q.143 管理サイト：入力項目のカスタマイズ

所属組織以外の端末は非表示にしたいです。各組織のユーザーが、所属する組織下の機器のみ管理できるように設定することはできますか。

- **入力項目のカスタマイズを利用して、組織ごとに管理を行うことができます。**
以下の設定を行うと [組織] タブが非表示となり、他の組織に対する設定の変更・編集・作成はできなくなります。
「ユーザーA」に対して、「組織A」に属さない機器を表示しない手順を例に説明します。

«**確組織作成**»
 1. 管理サイトに管理者権限のある任意のユーザーでログインする
 2. [組織] → [一覧] →  をクリックする
 3. 「組織名」に「組織A」と入力する
 4. [保存] をクリックする
«**入力項目のカスタマイズ作成**»
 1. [ユーザー] → [入力項目のカスタマイズ] →  をクリックする
 2. 「分類名」に「管理対象組織」と入力する
 3. 「グループ」の  をクリックする
 4. 「グループ名」に「組織A-1」と入力する
 5. 「グループ」の [権限] をクリックする
⇒ 「権限」画面が表示される
 6. 「組織」の  をクリックする
 7. メニューリストから「組織A」を選択する
 8. [管理者] を選択する。
 9. 右上の [x] をクリックする
⇒ 「権限」画面が閉じる
 - 「ユーザー所有の機器」「アプリ」は、任意に入力する。
 - 閲覧者、操作者など複数の権限を使い分けたい場合は、手順3  をクリックして、手順4で任意のグループ名を入力し、手順5~9を繰り返し行ってください。
 10. [保存] をクリックする
«**ユーザー作成**»
 1. [ユーザー] → [一覧] →  をクリックする
 2. 以下の項目を設定する
 - ・ 名前：任意（ここでは「ユーザーA」と入力）
 - ・ ユーザーID：任意（ここでは「aaaa」と入力）
 - ・ ユーザー種別：「ログイン (個別に権限を設定)」を選択
 - ・ 組織：「組織A」を選択
 - ・ 管理対象組織：「組織A」を選択（入力項目のカスタマイズで複数のグループを作っている場合は任意のグループを選択する）

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- ・パスワード: 任意 (ここでは「1111」と入力)
 - ・他の項目は任意に入力する
3. [保存] をクリックする

「作成したユーザーでログイン」

1. 管理サイトに「ユーザーA」のログインID (またはメールアドレス) とパスワードを入力してログインする
⇒ログインしたユーザーが所属する組織以外の機器は表示されなくなります。
 - 同様の手順で「ユーザー〇〇」に対する「組織〇〇」を複数作成し、1つの管理サイト内で組織ごとの管理を行うことができます。
- この設定を行って作成したユーザーでログインした場合、すでに作成されている設定セットを端末に適用することはできませんが、設定セットの新規作成、および編集、削除はできません。

Q.144 CSVで削除

「CSVで削除」で削除予定となっている機器を確認する方法はありますか。

- **機器レポートで確認することができます。**
以下を参照して、機器レポートを作成してください。削除予定の機器は、「[I] 削除状況」に「D」が入力されています。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「CSVをダウンロード」 - 「機器レポート」

Q.145 CSVで削除

「CSVで削除」で削除予定となっている機器の削除を取り消す方法はありますか。

- **削除用のCSVファイルで取り消すことができます。**
「CSVで削除」からCSVファイルをダウンロードし、該当する機器の「[S] 削除フラグ」に入力されている「D」を「C」に書き換えて、管理サイトへアップロードしてください。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「CSVで削除」

Q.146 アプリケーションレポート (高速版)

配信したアプリがインストールされていない端末を、管理サイトで確認することはできますか。

- **「アプリケーションレポート (高速版)」で確認することができます。**
以下を参照して、アプリケーションレポートを出力します。
アプリケーションレポートに表示されない端末が、配信したアプリのインストールが行われていない端末です。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「CSVをダウンロード」 - 「アプリケーションレポート (高速版)」
 - 最新の情報を出力するためには、端末と同期を行ってからアプリケーションレポートを出力してください。

Q.147 Windows : セキュリティ

ウイルス対策ソフトとスパイウェア対策ソフトをインストールしているのに、「セキュリティ」画面に表示されません。原因を教えてください。

- **対象のソフトが、ウイルス対策ソフト/スパイウェア対策ソフトとしてWindowsに登録されていないことが原因と考えられます。**
Windowsに登録されていないソフトは、管理サイトでインストールされていないと判断し、表示されません。
以下の手順で、SecurityCenter、およびSecurityCenter2の情報を表示し、Windowsに登録されているか各ソフトの情報を確認してください。情報が表示されなかった場合は、ウイルス対策ソフト/スパイウェア対策ソフトとしてWindows OSに登録されていません。

「ウイルス対策ソフトの確認手順」

1. スタートメニューから、Powershellを起動する
2. コマンド「Get-WmiObject -Namespace root/SecurityCenter AntiVirusProduct」を実行する
3. 続けてコマンド「Get-WmiObject -Namespace root/SecurityCenter2 AntiVirusProduct」を実行する

「スパイウェア対策ソフトの確認手順」

1. スタートメニューから、Powershellを起動する
 2. コマンド「Get-WmiObject -Namespace root/SecurityCenter AntispywareProduct」を実行する
 3. 続けてコマンド「Get-WmiObject -Namespace root/SecurityCenter2 AntispywareProduct」を実行する
- 情報が表示されなかった場合の原因については、ウイルス対策ソフト/スパイウェア対策ソフトの製造、または販売元へお問い合わせください。

Q.148 iOS : 構成プロファイル

「構成プロファイルアップロード」の「パスワードの共有を許可 (監視対象のみ)」項目で、iOS端末のWi-Fiパスワードの共有機能を制限することはできますか。

- **「パスワードの共有を許可 (監視対象のみ)」項目で、Wi-Fiパスワードの共有機能は制限できません。**
「パスワードの共有を許可 (監視対象のみ)」を「しない」に設定したパスワード設定済の端末を、パスワード未設定の端末に近づけてもパスワードは共有されません。
ただし、「パスワードの共有を許可 (監視対象のみ)」を「する」に設定したパスワード設定済の端末を、「しない」に設定したパスワード未設定の端末に近づけた場合は、パスワードが共有されます。
 - 構成プロファイルの詳細については、以下を参照してください。
 - 『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 (機能の制限)」

Q.149 iOS : MDM構成プロファイル

「Appとブック」場所トークンのアップロードを行うと、「このトークンは他のサービスで利用されています。このトークンを利用する場合、他のサービスで行われた設定の影響を受ける可能性があります。」と表示されます。「Appとブック」場所トークンが他のサービスと重複すると、具体的にどのような影響がありますか。

- **複数の端末が同じトークンを使用することになるため、割り当てられるライセンスの使用数、残数、未割り当て数、回収可能数が実際の数値と異なる**などの影響がでる場合があります。そのため、トークンは複数のサービスで同時に使用しないでください。

Q.150 iOS : MDM構成プロファイル

端末側からMDM構成プロファイルを削除したのですが、管理サイトに「管理外」と表示されません。管理サイトで「管理外」と表示されるまでの流れを教えてください。

- **MDM構成プロファイルを削除時に一度、管理サイトと通信を行います。**
端末で構成プロファイルを削除したタイミングで管理サイトと通信が行われ、このタイミングで正常に通信が行われると、管理サイトに「管理外」と表示されます。
このとき、端末がネットワークに繋がっていない、通信が不安定などの原因で、管理サイトと正常な通信が行われなかった場合、「管理外」は表示されません。また、このタイミングを逸すると「管理外」を表示することはできません。
構成プロファイルを削除して「管理外」を確実に表示したい場合は、「リモートワイプ (管理領域)」の使用をおすすめします。
 - リモートワイプ (管理領域) 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「機器」 - 「一覧」 - 「機器の操作」 - 「(操作-iOS) リモートワイプ (管理領域)」

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.151 Android : Android Enterprise

機器ログ「機器[(機器名)]のエージェントがアプリのパーミッション設定を行いました。」が出力される契機を教えてください。

- **機器ログ「機器[(機器名)]のエージェントがアプリのパーミッション設定を行いました。」は、[Android Enterprise]の[アプリケーション配信設定]で以下の変更を行い、同期した契機で出力されます。**
 - ・ 「設定なし」から「全てのアプリをインストール可能」に変更した
 - ・ 「設定なし」から「企業許可アプリのみインストール可能」に変更した
 - ・ 「設定なし」から「指定アプリのみインストール可能」に変更した
 - ・ 「全てのアプリをインストール可能」から「設定なし」に変更した
 - ・ 「指定アプリのみインストール可能」で、アプリの設定を変更した
 - ・ 「企業許可アプリのみインストール可能」から「設定なし」に変更した
 - ・ 「指定アプリのみインストール可能」から「企業許可アプリのみインストール可能」に変更した
 - ・ 「指定アプリのみインストール可能」から「設定なし」に変更した
 - ・ 「企業許可アプリのみインストール可能」から「指定アプリのみインストール可能」に変更した
 - ・ 「指定アプリのみインストール可能」から「全てのアプリをインストール可能」に変更した
 - ・ 「全てのアプリをインストール可能」から「指定アプリのみインストール可能」に変更した
- 設定変更後、個別ランタイムパーミッション設定が成功した場合、失敗した場合にはかわらず、同期したタイミングでログが出力されます。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-Android」-「アプリケーション」-「Android Enterprise/アプリケーション配信」

Q.152 Android Enterprise

企業ドメインメールアドレスでGoogleに登録しているのですが、IDとパスワードを忘れてしまいました。IDとパスワードを確認する方法はありますか。

- **以下のGoogleのサポートページにアクセスし、ページの記載にしたがって確認してください。**
 - ・ <https://support.google.com/a/answer/6335621?sjid=17137903673567032565-AP>

Q.153 Android Enterprise

同じ企業ドメインメールアドレスを複数の企業で使用できますか。

- **同じ企業ドメインメールアドレスを複数の企業で使用することはできません。**
同一の企業ドメインメールアドレスで登録を行っても、利用企業ごとに組織IDが割り当てられます。
 - ・ 割り当てられた組織IDは、管理サイトの [設定] → [サービス環境設定] → [Android Enterprise(企業アカウント登録)] で確認できます。
 - ・ 使用している企業メールアドレスに紐づく利用企業の組織ID一覧は、以下の「Google管理コンソール」で確認できます。
 - https://support.google.com/a/topic/2413312?hl=ja&ref_topic=4388346&sjid=15856793320198241142-AP

Q.154 Android Enterprise

企業ドメインメールアドレスを使った企業登録で管理者を複数設定することはできますか？

- **Google管理コンソールで管理者を複数設定することができます。**
詳細は、以下を参照してください。
 - ・ <https://support.google.com/googleplay/work/answer/14319210?hl=ja#zippy=%2C他の管理者を招待する>

Q.155 Android Enterprise

管理サイトに登録した企業ドメインメールアドレスを忘れてしまいました。確認する方法はありますか。

- **本製品で確認する方法はありません。Googleにお問い合わせください。**
 - ・ <https://support.google.com/a/answer/6335621?sjid=12010277794815423333-AP>

Q.156 Android Enterprise

企業ドメインメールアドレスとはなんですか。

- **法人メールアドレスとも呼ばれ、法人、企業などが仕事で使用するためのメールアドレスです。**
企業などでドメインを購入して独自にアドレスを作成します。

Q.157 Android Enterprise

企業ドメインメールアドレスでの登録とGmailのメールアドレスで登録する場合の違いを教えてください。

- **企業ドメインメールアドレスは新しく追加された登録方法で、Gmailのメールアドレスは従来の登録方法です。**
端末のキッティング手順に違いはありませんが、企業ドメインメールアドレスではGoogleアカウントを事前に用意する必要がなく、企業登録時に入力したメールアドレスで仕事用のGoogleアカウントを自動的に作成することができます。
新規企業登録時には、企業ドメインメールアドレスで登録することをおすすめします。
 - ・ 登録した企業ドメインメールアドレスは管理サイトに表示されないため、お客様ご自身で管理してください。

■ 目次

[管理サイト](#)[Androidエージェント](#)[iOSエージェント](#)[Windowsエージェント](#)[サービス企業用サイト](#)[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

■ Androidエージェント

Q.1 エージェントがインストールできません。

- **ご使用のAndroid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。

- 『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」 - 「エージェントの動作環境」
- 『Androidキッティングマニュアル』の「Android クライアントについて」 - 「動作環境」

Q.2 エージェントのライセンス認証が行えません。

- **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。
- **企業コードや認証コードが間違っていないか。**
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。
- **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過で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、またはオペレーターにお問い合わせください。

Q.3 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。

- **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』

- **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。

Q.4 パスワードの入力を求められます。

- **以下をご確認ください。**
エージェントの利用停止、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、またはオペレーターにお問い合わせください。

Q.5 モバイルウイルス対策はどこからダウンロードすればいいでしょうか。

- **ご契約が必要になります。**
「モバイルウイルス対策」を使用するには「デバイスマネジメント エージェント」のインストールが必要であり、管理サイトより配布操作が必要な場合、デバイスマネジメント エージェントライセンス認証時に自動配布される場合がございます。詳細は以下を参照してください。
- 「デバイスマネジメント エージェント」のインストール方法は『Androidキッティングマニュアル』
- 「モバイルウイルス対策」の配布についての詳細は管理者にお問い合わせください。

Q.6 モバイルウイルス対策がインストールできません。

- **ご使用のAndroid端末が動作環境を満たしていますか。**
以下を参照してご確認ください。
- 『Androidクライアント リファレンスマニュアル』の「関連アプリの使用法」 - 「ウイルス対策機能」 - 「ウイルス対策機能の動作環境」

Q.7 Android 7.0以降の端末で、ライセンス認証ができません。

- **以下の点をご確認ください。**
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 Model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』

Q.8 「エージェントのデータ移行に失敗しました。端末の再起動をしてください。」という通知が表示されました。どのようにしたらよいですか。

- **通知の案内に従い、Android端末を再起動してください。**

Q.9 アプリケーション配信

Android Enterpriseのアプリケーション配信設定で「指定アプリのみインストール可能」から「全てのアプリをインストール可能」に設定を変更した場合、配信したアプリケーションは端末から削除されますか。

- **「指定アプリのみインストール可能」から「全てのアプリをインストール可能」に設定を変更しても端末からアプリケーションは削除されません。**
ただし、以下の設定に変更した場合はアプリケーションが削除されます。
- 「指定アプリのみインストール可能」から「設定なし」に変更した場合
- 「指定アプリのみインストール可能」から、対象アプリが含まれていない「指定アプリのみインストール可能」の設定に変更した場合

Q.10 アプリケーション配信

Android Enterpriseで「企業許可アプリのみインストール可能」の設定をしていますが、個別アプリケーションに設定しているアプリケーションが端末側で表示されません。原因を教えてください。

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

● 指定したアプリケーションが企業許可アプリに表示されているかを確認してください。

以下を参照してご確認ください。

- 『Android Enterprise アプリケーション配信 手順書』の「アプリをインストールする」 - 「アプリを強制インストールする」 - 「企業許可アプリを追加する」

Q.11 アプリケーション配信

「アプリ情報の取得に失敗しました。(notFound: No enterprise was found for the given id.)」というエラーが出てアプリケーション配信ができません。原因と対処法を教えてください。

- **【設定】→【サービス環境設定】→【Android Enterprise(企業アカウント登録)】にてGoogleアカウントを削除している、もしくはGoogle Play (<https://play.google.com/work>) で「管理者設定」の「組織の情報」を削除した場合にエラーが発生することを確認しています。** また、企業アカウント登録に使用したGoogleアカウントが凍結された場合にも本エラーが発生する場合があります。こちらはGoogleの仕様で表示されるエラーのためアカウント凍結についての詳細はGoogleにお問い合わせください。

Q.12 アプリケーション配信

「Android Enterpriseのアプリ配信が失敗しました。: 配信対象アプリを確認後、もう一度機器同期を行ってください(notFound: No device was found for the given id.)」のエラーログが出てアプリケーションが配信されません。対処法を教えてください。

- **本エラーログは、キティング後にGoogleとMDM間でのユーザー紐付け処理が完了する前にアプリケーション配信設定が送信された場合に発生します。**
【機器】→該当機器の【詳細】→【デバイス】→【Android Enterprise】欄が「連携済」になっていることを確認のうえ、再度管理サイトから同期を行ってください。
なお、もし【Android Enterprise】欄が「連携済」にならない場合は以下をご確認のうえ、設定が反映されるまでお待ちください。

- 該当機器にユーザーが紐付いているか
⇒【機器】→該当機器の【詳細】の「所属」欄にユーザーが設定されていない場合は、【編集】をクリックし、ユーザーを選択してください。
- 端末側のインターネット接続状況に問題がないか
⇒<https://mdm.sdm.ntt-east.net/login>のページが表示できるかご確認ください。つながらない場合はネットワーク管理者にご確認ください。

Q.13 アプリケーション配信

Android Enterpriseで設定したアプリケーションが配信されません。原因と対処法を教えてください。

- **アプリケーションが配信されない場合は、以下を確認してください。**

- 【機器】→該当機器の【詳細】にて通信日時が更新されているか
⇒通信日時が更新されない場合は、端末側の状態や通信状況を確認してください。
- 組織（ユーザー）にアプリケーション配信設定が正しく割り当てられているか
⇒管理サイトの【組織(ユーザー)】→該当組織(ユーザー)選択→【設定】に設定が割り当てられているかを確認してください。
○ 組織に設定を割り当てている場合は、【ユーザー】→該当ユーザー選択でユーザーが組織に紐付いているかもご確認ください。
- アプリを配信する端末に、ユーザーが正しく割り当てられているか
⇒管理サイトの【機器】→該当機器の【詳細】でユーザーが割り当てられているかを確認してください。
- 「Android Enterpriseユーザー」欄が「連携済」になっているか
⇒【機器】→該当機器を選択→【詳細】→【デバイス】の「Android Enterpriseユーザー」欄を確認してください。
- 企業アカウント登録に使用したGoogleアカウントが凍結されていないか
⇒企業アカウント登録で使用したGoogleアカウントで、Googleのサービスにログインできるかを確認してください。
- 「企業許可アプリ」にアプリが正しく割り当てられているか
⇒管理サイトの【設定】→【Android】→【アプリケーション】→【Android Enterprise】→【企業許可アプリ】にアプリが追加されているか確認し、追加されていない場合はアプリを追加してください。
- 上記の端末側の条件を満たしていてもインストールができない場合は、以下を参照して、アプリケーション配信設定が割り当てられているユーザーの端末に、アプリを一括で配信してください。
○ 『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」 - 「Android Enterprise/アプリケーション配信」 - 「画面（一括配信）」
- アプリケーション配信設定を行った日の翌朝まで待つと配信される場合があります。アプリケーション配信設定の詳細については、以下のマニュアルを参照してください。
○ 『Android Enterpriseアプリケーション配信手順書』

Q.14 アプリケーション配信

Google Playストアの使用を禁止しているとき、アプリケーションの強制インストールはできますか。

- **アプリケーション禁止の「禁止するアプリケーションを指定」でGoogle Playストアを禁止していても、強制インストールはできます。**

Q.15 アプリケーション配信

Android Enterpriseのアプリケーション配信で「すべてのアプリをインストール可能」に設定している状態で、「指定アプリのみインストール可能」の設定をすることはできますか。

- **できません。Android Enterpriseをご利用の場合、一台の端末に対して「すべてのアプリをインストール可能」と「指定アプリのみインストール可能」を両方設定することはできません。**

Q.16 アプリケーション配信

Android Enterpriseでアプリケーション配信をしたら、端末側で「サーバーからの情報の取得中にエラーが発生しました。df-charta-01」というエラーが出ました。対処法を教えてください。

- **管理サイトからアプリケーション配信の指示は出ており、端末側で情報を受け取れていない場合に端末側で本エラーメッセージが発生する場合があります。**
モバイル回線からWi-Fiに変えるなど、端末側のアクセスポイントを変えて再度同期を行ってください。
なお、こちらはGoogle側で表示しているメッセージのため、上記で改善しない場合はGoogleにお問い合わせください。

Q.17 アプリケーション配信

Android Enterpriseで配信したアプリケーションでアプリ内課金をしようとしたら「(アプリケーション名)は停止しました」と表示が出た後アプリが強制終了してしまいました。原因を教えてください。

- **「アプリ内課金あり」のアプリケーションをAndroid Enterpriseで配信した場合、追加機能の購入などはできません。**
本挙動はGoogleの仕様に基づいています。

Q.18 アプリケーション配信

Android Enterpriseのアプリケーション配信を利用して、「Google Play開発者サービス」をアップデートしたいです。指定のバージョンもしくは最新バージョンにアップデートできますか。

- **指定のバージョンへのバージョンアップはできませんが、アプリケーション配信設定にて「指定アプリのみインストール可能」の「強制インストール：する」を指定して配信することで最新バージョンがリリースされたときに自動的に最新バージョンにアップデートすることはできます。**
手順につきましては以下のマニュアルをご参照ください。
- 『Android Enterpriseアプリケーション配信手順書』の「アプリを強制インストールする」

Q.19 アプリケーション配信

Android Enterpriseで配信したアプリケーションをアンインストールされないように制限することはできますか。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- **アプリケーションのアンインストールを禁止する設定はございません。**
しかし、アプリケーション配信設定が当たっていれば同期の度に再配信されます。

Q.20 アプリケーション配信

アプリケーション禁止設定でGoogle Playストアを設定している場合、アプリケーション配信で配信したアプリケーションはアップデートされますか。

- **アプリケーション禁止でGoogle Playストアが禁止されていても、端末側でGoogle Playストア内の「アプリの自動更新」設定を「ネットワークの指定なし」もしくは「Wi-Fi経由のみ」に設定していればアプリケーションはアップデートされます。**

Q.21 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のアップデートを禁止することはできますか。

- **managed Google Playストア上で表示されているアプリケーションのアップデートは禁止できません。**
本挙動はGoogleの仕様に基づいています。

Q.22 アプリケーション配信

アプリケーション配信の設定を別の設定にした場合、差し替え前の設定で配信されたアプリケーションは端末から削除されますか。

- **差し替え後の設定に含まれないアプリケーションは削除されます。**
例えば、配信設定Aに「a」「b」「c」というアプリケーションが設定されており、配信設定Bに「b」「d」「e」というアプリケーションが設定されていた場合、配信設定Aから配信設定Bに差し替えると、アプリケーション「a」「c」は端末から削除され、「b」は削除されません。

Q.23 アプリケーション配信

「指定アプリのみインストール可能」で配信を行った後に「すべてのアプリを許可」に変更した場合、アプリケーションのログイン情報は引き継がれますか。

- **はい。ログイン情報は引き継がれます。**
「指定したアプリのみインストール可能」の設定から「すべてのアプリを許可」に変更しても配信しているアプリケーションに影響はございません。

Q.24 アプリケーション配信

管理者が許可したアプリのみを利用者が自由にインストールすることはできますか。

- **許可アプリのみを自由にインストールすることはできます。**
配信設定を「企業許可アプリのみインストール可能」に設定してください。
 - 『Android Enterpriseアプリケーション配信手順書』の「管理者が承認したアプリのみインストールを許可する」

Q.25 Android Enterprise

端末のロック画面に「この端末は組織によって管理されています」と表示されます。表示されないようにすることはできますか。

- **Device Owner Modeが有効の端末で表示されます。**
本メッセージはGoogleの仕様のため、管理サイトで表示の制御を行うことはできません。

Q.26 Android Enterprise

Googleアカウントでキッティングしたあとに、端末側でGoogleアカウントが必要なアプリケーションを開いてGoogle Workspaceのアカウントを入れたらどうなりますか。

- **仕事用アカウントが外れ、Android Enterpriseの管理ができなくなります。**
また、Google Workspace側でMDM管理の設定が作成されている場合、競合が発生しMDMが正しく動作しない可能性があります。Google Workspaceアカウントを使用してアプリケーションを使う場合は、以下どちらかの運用を検討してください。
 - Google Workspaceアカウント連携で利用する
 - 『Androidキッティングマニュアル』の「Google WorkspaceアカウントでAndroid Enterprise 連携を行う」
 - 以下の行ったうえで運用してください。
 - Google管理コンソールで「端末管理機能」を「無効」に設定する
 - Google管理コンソールで「ユーザ切り替え」を「無効」に設定する
 - 管理サイトで「セキュリティ設定」の「アカウント制限」を「制限する」に設定する

Q.27 Android Enterprise

端末側でGoogleアカウントを追加できないようにアカウント制限をかけたつ、GoogleドライブなどGoogleアカウントが必要なアプリケーションはアカウントを入れて使わせたいです。設定方法を教えてください。

- **Google WorkspaceでAndroid Enterpriseと連携することで、個別のGoogle Workspaceアカウントを利用してGoogleのアプリケーションを利用することができます。**
以下の2つの設定を行ってください。
 - 管理サイトで [設定] → [Android] → [Device Owner Mode] → [セキュリティ設定] で「アカウント制限：制限する」の設定を作成し制限したい機器に適用する。
 - [設定] → [サービス環境設定] → [Android Enterprise(企業アカウント登録)] でGoogle Workspaceアカウントを登録し、端末をキッティングする
 - 組織に設定を割り当てている場合は、[ユーザー] → 該当ユーザー選択でユーザーが組織に紐付いているかもご確認ください。
 - 『Androidキッティングマニュアル』

Q.28 Android Enterprise

Google Workspaceのデバイス管理を利用している状態から管理サイトのAndroid Enterprise連携に移行したいです。どうしたらいいですか。

- **Google Workspaceのデバイス管理からAndroid Enterpriseへの移行は、Android Enterprise初期導入の手順と同様の操作になります。**
移行用の特別な操作はございません。
なお、Google Workspaceのデバイス管理で使用していた機能については、Android Enterpriseでは設定を引き継ぐことができません。あらかじめご了承ください。
 - 『Androidキッティングマニュアル』の「Google WorkspaceアカウントでAndroid Enterprise連携を行う」

Q.29 Android Enterprise

企業アカウント登録で「Googleアカウント」にチェックを入れ「アカウント登録」をクリックしたら「Google Workspaceは現時点ではmanaged Google Playアカウントに対応していません」という表示が出ました。どうしたらいいですか。

- **操作しているPCがGoogle Workspaceアカウントでログインしていると本エラーが発生します。**
本挙動はGoogleの仕様によるものです。一度Google Workspaceアカウントをログアウトして再度登録の手順を行うか、Google Workspace連携の手順で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』の「GoogleアカウントでAndroid Enterprise連携を行う」
 - 『Androidキッティングマニュアル』の「Google WorkspaceアカウントでAndroid Enterprise連携を行う」

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.30 Android Enterprise

Android端末を初期化せずにライセンス認証する方法はありますか。

- **初期化せずにライセンス認証を行うことはできません。**
各種キッティング方法は以下のマニュアルを参照してください。
 - 『Androidキッティングマニュアル』

Q.31 Android Enterprise

企業アカウントを登録する時にGoogleの画面へ遷移すると「この企業はすでに他のEMMに登録されています」と表示されます。原因と対処法を教えてください。

- **操作しているPCでログインしているGoogleアカウントが、既に別のEMMに紐付いている場合に本画面が表示されます。**
紐付いているEMMを解除するか、新しくGoogleアカウントを作成して、再度企業アカウント登録を行ってください。

Q.32 Android Enterprise

他社MDMの登録に使用したGoogleアカウントは、管理サイトの企業用アカウントとして使用できますか。

- **他社MDMでAndroid Enterpriseの登録に使用しているGoogleアカウントは、管理サイトで併用することはできません。**
紐付いているEMMを解除するか、新しくGoogleアカウントを作成して、再度企業アカウント登録を行ってください。

Q.33 Android Enterprise

機器情報でユーザーを変更しようとしたら「ユーザーは変更できません。機器をワイプ後、管理サイトから機器の情報を削除し、再度認証しなおしてください。」と表示され変更できません。原因を教えてください。

- **Android Enterpriseを連携している機器はユーザーの変更ができません。**
ユーザーを変更する場合は端末を初期化し、管理サイト上で機器を削除したうえで再度キッティングしてください。
 - 『Androidクライアント リファレンスマニュアル』の「エージェントの基本操作」 - 「端末の所有者を変更する」

Q.34 アプリケーション配信

個別アプリケーションを登録しようとしたら「別のパッケージ名で新しいAPKファイルをアップロードしてください」と表示されました。原因を教えてください。

- **登録しようとしたapkファイルがパッケージ名の登録条件を満たしていない場合に本エラーが表示されます。**
パッケージ名のルールは、Google側の仕様に準拠しています。弊社で確認している範囲の発生条件は以下のとおりです。
 - **同じパッケージ名のapkファイルが既にGoogle Play上に存在している。**
Google Playのルールで、既に同じパッケージ名がGoogle Playに存在する場合、そのAPKのアップロードができません。
 - **apkファイル内のパッケージ名に「com.test」や「com.example」という文字が含まれている。**
Google Play側で「com.test」や「com.example」の様にパッケージ名に「test」や「example」という文字が含まれている場合、アップロードが禁止されておりエラーが発生いたします。
 - パッケージ名はプログラムをビルドするときに指定するもので、ファイル名とは異なります。
 - パッケージ名の値につきましては、アプリ開発元にご確認ください。

Q.35 Android Enterprise

Android Enterpriseでキッティングしたあと、管理サイトから端末に設定していた設定を変更することはできますか。

- **キッティング後に設定を変更できます。**
ただし、キッティングした機器に紐付けられているユーザーのみ変更はできません。

Q.36 Android Enterprise

Android Enterpriseの企業アカウント登録に使用するGoogleアカウントに個人のアカウントを使用できますか。

- **登録はできますが、管理用にGoogleアカウントを作成することを推奨しています。**

Q.37 認証

「認証に失敗しました。ネットワーク接続やライセンス情報を確認してください」と出て認証できません。対処法を教えてください。

- **認証時の入力内容が誤っている可能性があります。**
認証画面で「QRコードによる認証情報入力」をタップし、管理サイトの[機器] → [認証手順] の「エージェント認証用QRコード」を読み込んでください。
上記を行っても認証できない場合は、通信環境をご確認ください。

Q.38 認証

キッティング中に「リセット保護が有効になっています」というポップアップが出ました。原因と対処法を教えてください。

- **初期化前にGoogleアカウントでログインしていると、Googleの「スマートフォンの保護機能」により本メッセージが表示されることがあります。**
一度ログインしてアクティベートを行っていただき、設定画面からログアウトしたあとで再度初期化を行ってください。

Q.39 認証

キッティングが完了したはずなのに「ライセンス解除」が活性化しています。原因を教えてください。

- **端末側でキッティングが終わっても、管理サイトでユーザーを紐付けてAndroid Enterpriseを連携済の状態にしないと「ライセンス解除」ボタンは活性化したままになります。**
管理サイトで該当機器にユーザーを紐付けて同期を行ってください。

Q.40 認証

端末をキッティングしたアカウントから別アカウントに切り替えた場合、MDMの認証情報は引き継ぎますか。

- **アカウントを切り替えた場合、MDMの認証情報は引き継ぎません。**
認証されていないユーザーでのご利用は正常な動作をしない場合があるため、マルチユーザー機能は使用しないでください。

Q.41 認証

「当エージェントはDevice Owner Modeでのキッティングが必要です。詳細はマニュアルを参照してください」というポップアップが出て認証ができません。原因と対処法を教えてください。

- **認証を行うときに、Google Playストアからエージェントをインストールし認証しようすると本メッセージが表示されます。**
端末を初期化し、以下のマニュアルを参照のうえキッティングしてください。
 - 『Androidキッティングマニュアル』
 - キッティングの方法は複数ございます。選択したキッティング方法に沿った手順を実施してください。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.42 認証

afwキッティングをするときに初期化前にバックアップしたデータを復元したいです。キッティングの途中で「新規としてセットアップ」ではなく「アプリとデータの保持」を選択するとどうなりますか。

- **Android Enterpriseとアプリとデータの復元は同時にご利用できません。復元のためにGoogleアカウントを入力する必要がありますが、入力を行うとafw識別子やGoogle Workspaceアカウントの入力ができなくなるため、必ず「新規端末としてセットアップ」を選んでください。**
なお、初期化前のデータを復元したい場合は、SDカードなどにデータをバックアップしキッティング後にバックアップしたデータを移行してください。

Q.43 認証

QRコードでキッティングしたとき、「端末をセットアップできません。管理アプリをダウンロードできませんでした。」と表示されます。原因と対処法を教えてください。

- **キッティング時に読み込んだQRコードが最新でない場合に本エラーが発生します。**
以下の手順で最新のQRコードを表示して、そちらを端末でQRコードを端末で読み取ってください。
 1. 管理サイトの【機器】→【認証手順】をクリックする
 2. 【キッティング用QRコード】をクリックする

Q.44 認証

QRコードキッティングで使うQRコードはどこに記載されていますか。

- **管理サイトの【機器】→【認証手順】の順でクリックしてください。**
Android用エージェントの中の「キッティング用QRコード」をクリックするとDevice Owner Modeキッティング用QRコードが表示されます。

Q.45 認証

QRコードキッティングをするときに、端末を初期化せずQRコードを読み取って認証することはできますか。

- **QRコードリーダーでキッティング用のQRコードを読んで認証することはできません。**
キッティングを行うには、端末を工場出荷状態（初期設定画面）にする必要があります。
端末初期化後、所定の手順でインストールされる専用のQRコードリーダーでQRコードを読み取ってください。
 - 『Androidキッティングマニュアル』の「その他のキッティング方法」 - 「QRコードでキッティングする」

Q.46 同期

Android端末にて同期ができません。原因と対処方法を教えてください。

- **確認方法と回避方法の詳細は、以下のマニュアルを参照してください。**
 - 『Androidクライアントマニュアル』の「こんなときは」 - 「同期ができないときは」

Q.47 スクリーンロックパスワード変更

「スクリーンロックパスワード変更」を実施しても端末に変更内容が反映されません。どうしたらいいですか。

- **以下のどちらかの場合、変更内容が反映されません。**

◀端末と正常に通信ができない状態となっている場合▶

 1. 【機器】→該当機器の【詳細】の【同期】をクリックする
 2. 【機器】→該当機器の【詳細】にて「通信日時：1分以内前」であることを確認する
 3. 【機器】→該当機器の【詳細】→【スクリーンロックパスワード変更】をクリックする
 4. 「新規パスワード」を入力し、「実行」をクリックします
 5. 【機器】→該当機器の【詳細】→【ログ】にて下記のログが表示されていることを確認する
⇒「機器[**機器名**」のエージェントがスクリーンロックの設定を行いました。



◀端末が「ダイレクトブートモード」になっている場合▶

Android端末の機能に「ダイレクトブートモード(Direct Boot Mode)」というものがございます。
この状態になっている場合には、管理サイトより「スクリーンロックパスワード変更」などの、リモート操作の命令を受け付けられない仕様となっております。
この場合、「スクリーンロックパスワード変更」を実行できません。

 - ver9.9.101.0以降では「リモートワイプ」の実行のみ可能となりました。

Q.48 アプリケーション検知

Androidでアプリケーションの削除を制限する機能はありますか。

- **アプリケーションの削除を制限する機能はございません。**
回避策として、「アプリケーション検知」機能を利用することで、インストールが必要なアプリケーションが、インストールされていない場合、管理者に通知されます。
下記手順でアプリケーション検知の設定を行ってください。
 - **「アプリケーション検知」設定を割り当てる**
 1. 【設定】→【Android】→【アプリケーション】→【アプリケーション検知】を選択する
 2. にて新規作成を行う
 3. 設定名を入力する
 4. 「インストール推奨アプリケーション」より、「+」にて行追加を行う
 5. 以下の値を入力する
 - アプリケーション名
 - パッケージ名
 - バージョン条件
 - 記載方法については、下記マニュアルをご参照ください。
 - 『管理サイトリファレンスマニュアル』の「設定-Android」 - 「アプリケーション」 - 「アプリケーション検知」
 6. 「保存」をクリックする
 7. 【機器】→一覧→【該当端末の詳細→設定の割り当て】をする
 8. 「アプリケーション検知」にて手順6で作成した設定名を選択し【保存】する
 9. 同期を実施する
 - **「通知先のメールアドレス」を設定する**
 1. 【設定】→【サービス環境設定】→【通知設定】を選択する
 2. 「ログメール通知」の【編集】をクリックする
 3. 「メール通知対象ログ」より「アプリケーション検知」にチェックし【保存】する
 4. 以下のとおり設定する
 - ◀管理者を送信先に設定する場合▶
 - 「管理者」にチェックを入れる
 - ◀管理者以外の指定アドレスを送信先に設定する場合▶
 - 「メール送信先(カスタム)」ににて行追加を行い、指定のメールアドレスを入力する
 5. 【保存】をクリックする
 6. 同期を実施する

Q.49 アプリケーション配信

アプリケーションを利用しようとすると、「利用するためにはアプリの更新が必要です。更新しますか？」と表示されますが、更新をしようとすると、「管理者からこのアイテムへのアクセス権を与えられていません。」と表示され更新できません。原因と対処法を教えてください。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト



用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- **当該アプリケーションが、管理者によって許可アプリに登録されていないために発生しています。**
端末に適用しているアプリケーション配信の設定にて、該当アプリケーションを許可することで、アプリケーションを更新および利用できます。アプリケーション配信設定をご確認のうえ、以下の手順を行ってください。

◀指定アプリのみインストール可能を設定している場合▶

1. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [企業許可アプリ] をクリックする
2. [アプリを選択する] をクリックする
3. 該当アプリケーションを選択して、[選択] をクリックする
4. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [個別アプリケーション] にて、 をクリックする
5. 「アプリ設定」に任意の値を入力、「アプリ選択」にて該当アプリケーションを選択し「保存」をクリックする
6. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [アプリケーション配信] → 該当設定を選択 → [編集] をクリックする
7.  をクリックする
8. 手順2で作成した設定を追加する
9. [保存] をクリックする
10. [機器] → 該当機器を選択 → [詳細] にて、[同期] をクリックする
⇒端末側にて、アプリケーションを更新および利用できるかご確認ください。

◀企業許可アプリのみインストール可能を設定している場合▶

1. [設定] → [Android] → [アプリケーション] → [Android Enterprise] → [企業許可アプリ] をクリックする
2. [アプリを選択する] をクリックする
3. 該当アプリケーションを選択して、[選択] をクリックする
4. [機器] → 該当機器を選択 → [詳細] にて、[同期] をクリックする

Q.50 認証

Google Workspaceアカウントを使用したキッティングが失敗します。原因と対処方法を教えてください。

- **キッティングを行うための条件を満たしていない可能性があります。以下を確認してください。**

- Android Enterprise企業アカウント登録でGoogle Workspaceアカウントが登録されていない
対処方法：管理サイトで企業アカウント登録を行ってください。
 - 『Androidキッティングマニュアル』の「Google WorkspaceアカウントでAndroid Enterprise連携を行う」 - 「Google Workspaceアカウントを登録する」
- Wi-FiやLTEなどの有効なネットワークに接続されていない
対処方法：インターネットに接続可能なWi-Fiやモバイル通信に接続してください。
- 入力された内容（メールアドレス、企業コード、認証コード）が間違っている
対処方法：メールアドレスを「[管理] タブ」、企業コード、認証コードを「認証手順」で確認し、間違っている場合は修正してください。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「認証手順」
 - 『管理サイト リファレンスマニュアル』の「ユーザー」 - 「一覧」 - 「[管理] タブ」
- 入力したユーザーがGoogle Workspace管理コンソール、管理サイトに登録されていない
対処方法：Google Workspaceアカウントのメールアドレスが登録されたユーザーを作成し、再度ご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』の「Google WorkspaceアカウントでAndroid Enterprise連携を行う」 - 「ユーザーを作成する」
- 端末が管理サイトに登録されていて、ユーザーが紐づいている
対処方法：該当端末の情報を1度削除し、再度ライセンス認証を行ってください。
 - 『管理サイト リファレンスマニュアル』の「機器」 - 「一覧」 - 「機器の個別削除」
- ライセンス認証時に端末のライセンス数が不足している
対処方法：端末のライセンス数を確認し、不足している場合はライセンスを追加してください。
- 上記に該当しない場合は、端末側の不具合の可能性があります。

Q.51 DM Browser

特定のサイトを「DM Browser」で開いた状態で端末の再起動すると、該当サイトのタブが閉じてしまいます。タブを開いたままにする方法はありますか。

- **「DM Browser」では、タブの状態を保存・再表示する仕様はございません。**
再起動により自動的にタブを閉じる仕様となっています。そのため、タブを開いたままにする機能はございません。

Q.52 位置情報

エージェントをバージョンアップしてから、位置情報の通知がステータスバーから消えません。該当の通知をオフにしたいので、対処法を教えてください。

- **位置情報の通知は、通知領域より消すことができない仕様となります。**
Googleのプライバシーポリシーの強化により、位置情報を利用する機能を有しているアプリケーションは、明示的に位置情報取得していることを提示することが定められております。

Q.53 Device Owner Mode

端末のPlayストアで「Playプロテクト」の「スキャン」項目がグレーアウトしていてタップできません。原因と対処方法を教えてください。

- **管理サイトの「アプリ確認の強制」設定にて「強制する」を割り当てていないことが原因で、該当項目がグレーアウトとなっています。**
以下手順を行い、解消されることを確認してください。
 1. [設定] → [Android] → [Device Owner Mode] → [セキュリティ設定] より対象の設定を選択する
 2. [編集] をクリックする
 3. 「アプリ確認の強制」の項目にて「強制する」を選択する
 4. [保存] をクリックする
 5. 同期を実施する
 - 『管理サイトリファレンスマニュアル』の「設定 - Android」 - 「Device Owner Mode」 - 「セキュリティ設定 (DOM)」

Q.54 アプリケーション配信

Android Enterpriseのアプリケーション配信にて、「全てのアプリをインストール可能」から「指定アプリのみインストール可能」に変更した場合、インストール済みのアプリケーションは利用可能ですか。

- **「全てのアプリをインストール可能」によりインストールされたアプリケーションは、本変更によりアンインストールされることはなく、引き続き利用可能です。**
しかし、該当アプリケーションが「指定アプリのみインストール可能」のアプリ個別設定に指定されていない場合、バージョンアップができない点にご注意ください。詳細は以下のマニュアルを参照してください。

- 『Android Enterprise アプリケーション配信手順書』の「アプリをインストールする」 - 「アプリを強制インストールする」 - 「アプリ個別設定を作成する」

また、上記設定を行ってしまうと、以降、別のAndroid Enterpriseアプリケーション配信設定に切り替えた際、アプリケーションのアンインストールが実行される可能性がある場合がございます。

Q.55 リモート操作

管理サイトからのリモート操作指示（リモートロックやリモートワイプなど）をAndroid端末が受け取れなかった場合、どのように処理が行われますか。

- **Android端末でリモート操作の指示が受け取れなかった場合、再指示（リトライ）や再指示され続ける期間（リトライ期間）、次回同期時は、以下のとおりです。**

FAQ一覧

目次

[管理サイト](#)

[Androidエージェント](#)

[iOSエージェント](#)

[Windowsエージェント](#)

[サービス企業用サイト](#)

[用語一覧](#)

- リトライは行われず、リトライ期間もありません。
- 電源断や端末のスリープ、ネットワーク切断などで指示が受け取れなかった場合は、次の同期時に指示された動作を実行します。

Q.56 Android Enterprise

管理サイトで設定している内容（ランタイムパーミッションなど）と、「権限移譲対象アプリ」からの処理はどちらが優先されますか。

- 管理サイトの設定と権限移譲対象アプリの設定では、あとから行った設定が有効となります。**
ただし、管理サイトの設定と異なる権限移譲対象アプリの設定をあとから行った場合は、端末の挙動が管理サイトの設定内容と異なってしまうため、管理上でのアプリに対してどの設定を行ったかを把握しておく必要があります。
「権限移譲対象アプリ」の設定手順、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 - Android」 - 「アプリケーション」 - 「Android Enterprise」 - 「Android Enterprise / 個別アプリケーション」 - 「画面（編集画面）」

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

■ 目次

[管理サイト](#)[Androidエージェント](#)[iOSエージェント](#)[Windowsエージェント](#)[サービス企業用サイト](#)[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.1 ライセンス認証が行えません。

- **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。
- **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』の「Apple Push証明書登録・削除」 - 「Apple Push証明書の登録」
- **企業コードや認証コードが間違っていないか。**
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。
- **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、またはオペレーターにお問い合わせください。
- **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、ライセンス認証が行えません。
一時的に [設定] → [Safari] → [Cookieを受け入れる] で [常に] を選択してください。
- **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、またはオペレーターにお問い合わせください。
- **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および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。

Q.2 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。

- **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。

Q.3 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。

- **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。
 - 『iOSキッピングマニュアル』の「ライセンス認証を行う」 - 「MDM構成プロファイルをインストールする」

Q.4 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。

- **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。

Q.5 プロファイルを誤って削除してしまいました。

- **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キッピングマニュアル』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」

Q.6 再度ライセンス認証を行いたい場合はどうすればいいですか。

- **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キッピングマニュアル』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」

Q.7 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。

- **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. ポータルをタップする
2. ポータル画面で、[エージェントを認証する] をタップする
3. [App Storeからインストール] をタップする
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] をタップする
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] をタップする
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] をタップする
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. ポータルをタップする
2. ポータル画面で、[エージェントを認証する] をタップする
3. ポータル画面で、[起動して認証] をタップする
4. 「デバイス管理 エージェントで開きますか?」のポップアップが表示されるので、[開く] をタップする
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

Q.8 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。

- **エージェントがインストールおよび認証されていないと、以下の機能は利用できません。**

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

- 位置情報測位または送信
- Jailbreak検知
- メッセージ通知（オプション機能）
- DM Browser（オプション機能）

Q.9 iOSエージェントが自動同期を行うタイミングを教えてください。

● 以下のような場合に、自動同期が行われます。

- エージェントを認証したとき
- ホーム画面やメッセージ画面の[同期]ボタンをタップしたとき
- 管理サイトで位置情報の更新の操作がされて、そのプッシュ通知を受け取ったとき
- エージェントが位置情報を取得したとき
 - 取得した位置情報を管理サイトに送信したときに同期を行います。位置情報の諸条件などについては、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」 - 「機器の情報」 - 「（情報-iOS）位置」
- 「通信日時（(MDM構成プロファイル）」と「通信日時（エージェント）」は、異なる通信手段です。「通信日時（(MDM構成プロファイル）」は自動同期が行われますが、「通信日時（エージェント）」は定期的な自動同期は行われません。

Q.10 連絡先を端末に反映する方法を教えてください。

● CardDAVを用いて作成した構成プロファイルを、MDMで配信することで反映できます。Apple Configurator2を使用する手順は以下のとおりです。

◀構成プロファイルの作成・配信手順▶


1. 「CardDAVサーバー」と連絡先情報（CardDAV）を用意する
2. Apple Configurator2を起動する
3. 「ファイル」→「新規プロファイル」をクリックし、新規作成のページを開く
4. 一覧から「連絡先」を選択する
5. 構成プロファイルの作成に必要な情報を入力し、構成プロファイルを作成する
6. 作成した構成プロファイルを管理サイトにアップロードする
構成プロファイルのアップロードについては、以下を参照してください。
 - 『管理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」
7. 配信したい端末に設定を適用する

Q.11 アプリケーション配信

構成プロファイルでApp Storeを禁止にしている状態で、Appとブックを使用しないでアプリケーションを配信する方法はありますか。

● 以下の手順でアプリケーションを配信してください。



なお、前提条件として端末がApp Storeにサインインしている必要があります。

1. 管理サイトの【設定】→【iOS】→【アプリケーション】→【アプリケーション配信】を選択する
2. で新規作成する
3. 「設定名」に任意の値を入れる
4. 「Store ID」欄に配信したいアプリケーションのStore IDを入力する
5. 「管理」欄にチェックを入れる
 - 「ポリシー」欄は任意で指定してください。
6. 【保存】をクリックする
7. 【機器】→該当機器を選択→【設定の割り当て】にて【編集】をクリックする
8. 手順6で保存した設定名を選択する
9. 【同期】をクリックする

Q.12 アプリケーション配信

構成プロファイルでApp Storeを禁止にしている状態で、アプリケーションのバージョンアップはできますか。

● はい。「自動的にバージョンアップする」を有効にした管理対象アプリポリシーを使用することで、App Storeを禁止していてもバージョンアップできます。以下の手順でアプリケーション配信設定を作成し、機器に適用してください。

1. 管理サイトの【設定】→【iOS】→【アプリケーション】→【管理対象アプリポリシー】を選択する
2. で新規作成する
3. 「ポリシー名」に任意の値を入れる
4. 「アプリのバージョンアップ」の「自動的にバージョンアップする」にチェックを入れる
5. 【保存】をクリックする
6. 管理サイトの【設定】→【iOS】→【アプリケーション】→【アプリケーション配信】を選択する
7. で新規作成する
8. 「設定名」に任意の値を入れる
9. 「Store ID」欄に配信したいアプリケーションのStore IDを入力する
10. 「管理」欄にチェックを入れている
11. 「ポリシー」欄に手順5で保存したポリシー名を指定する
12. 【保存】をクリックする
13. 【機器】→該当機器を選択→【設定の割り当て】にて【編集】をクリックする
14. 手順12で保存した設定名を選択する
15. 【保存】をクリックする
16. 【同期】をクリックする

Q.13 アプリケーション配信

端末側のスクリーンタイムを利用し、App Storeを非表示にしている状態でアプリケーションの配信はできますか。

● はい。管理対象アプリとして配信することで、App Storeを非表示の場合でもアプリケーションを配信できます。

配信方法は以下の3種類です。いずれかで設定してください。

- 管理対象アプリとして配信する
 - 事前にApp Storeにログインしたうえで、スクリーンタイムでApp Storeを禁止する必要があります。
- 端末に「Appとブック」ライセンスを割り当てて配信する
 - Appとブックの事前設定を行っていただく必要があります。
 - この方法の場合、App Storeにログインする必要はありません。
- ユーザーに「Appとブック」ライセンスを割り当てて配信する
 - 事前にAppとブックの事前設定を行っていただく必要があります。
 - 管理サイトから配布するAppとブックの参加依頼を許可するためにApp Storeにログインする必要があります。App StoreにログインしたうえでスクリーンタイムでApp Storeを禁止してください。
- 『iOSアプリケーション配信手順書』の「アプリをインストールする」 - 「管理対象アプリをインストールする」、「アプリを強制インストールする」、「アプリ管理用の共通Apple IDでアプリをインストールする」

Q.14 アプリケーション配信

Appとブックを利用したアプリケーション配信で、使用しているApple IDとは別のApple IDを端末側で所持しても配信に問題はありませんか。

● 端末に「Appとブック」ライセンスを割り当てる配信方法は、端末側で別のApple IDを所持していても配信に問題はありません。

ユーザーに「Appとブック」ライセンスを割り当てる配信方法は、端末側で別のApple IDでログインしているとアプリケーション配信ができません。必ずAppとブックに紐づくApple IDでログインしてください。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Q.15 アプリケーション配信

Appとブックで配信したアプリケーションをアンインストールするにはどうしたらいいですか。

- **以下のいずれかの条件を満たすとサイレントアンインストールされます。**
 - 対象のアプリケーションをアプリケーション配信設定から削除し機器に同期する
 - 対象のアプリケーション配信設定の「管理」のチェックを外し、機器に同期する
 - 対象のアプリケーション配信設定を機器から外し同期する

Q.16 アプリケーション配信

Appとブックを利用してアプリケーション配信を行った後に「Appとブック」ライセンスを一時的に他のトークンに譲渡した場合、端末に何か影響はありますか。

- **一時的に他のトークンにライセンスを譲渡しても端末側に影響はありません。**
ただし、他のトークンに譲渡した結果ライセンスが不足してしまうと、端末にライセンスが付与されていない状態となるため早めにライセンス数の調整を行い、元のライセンス付与状態にもどしてください。
 - Appleの仕様により、端末のライセンス付与状態が確認できない場合は端末側に警告のポップアップが表示されます。また、ポップアップが表示されてから30日後にライセンス付与状態が確認できない場合は、アプリケーションが削除される場合があります。

Q.17 Appとブック

「Appとブック」ライセンスの「更新」をクリックしたら、「『Appとブック』ライセンスの更新に失敗しました。」というメッセージが出ました。原因と対処法について教えてください。

- **以下のどちらかの原因で処理が正常に行われなかった場合、本エラーが発生します。**
エラーが発生した場合は、一度時間をおいて「更新」をクリックしてください。
 - Appleで更新処理に失敗した
 - Appleから何らかのエラーが返ってきて更新処理が行えなかった
 - こちらが原因の場合、本エラーメッセージと同時に以下の管理ログが出力されます。
 - 管理ログ：「(アプリ名)」のライセンス割り当ての更新が失敗しました。

Q.18 Appとブック

機器の「Appとブック」設定で「個別設定」、「取消」、「削除」のボタンが表示されません。原因を教えてください。

- **組織の「Appとブック」設定でユーザーを選択している状態で、機器の所属が「ユーザー」になっている場合は、「取消」や「削除」のボタンは表示されません。**

Q.19 Appとブック

1つの「Appとブック」場所のトークンを複数のMDMで併用することはできますか。


- **1つの「Appとブック」場所のトークンを複数のMDMで併用することはできません。**
1つのMDMに対して1つの「Appとブック」場所のトークンを使用してください。

Q.20 Appとブック


組織の「『Appとブック』ライセンス付与対象」を「機器」にして、機器の「所属」を「組織」にして配信しています。機器の所属を「組織」から「ユーザー」に変えた場合、インストールしたアプリケーションに何か影響はありますか。

- **すぐにアプリケーションがアンインストールされることはありません。**
ただし、所属を変更することにより機器に割り当てられていた「Appとブック」設定が解除され、ライセンス付与状態ではなくなります。この状態が続くと、Appleのポリシー変更などでアンインストール対象となる場合があるので、ユーザーもしくは端末に「Appとブック」ライセンスを割り当て直し、再度ライセンスを付与してください。

◀端末に「Appとブック」ライセンスを割り当てる場合▶

1. 管理サイトで「機器」→該当機器を選択→「詳細」→「設定」→「他の設定を見る」→「『Appとブック』設定」に遷移する
2. 「新規作成」をクリックする
3. 「『Appとブック』ライセンス」を選択する
4. 「『Appとブック』アプリライセンス付与」欄で、をクリックする
5. 配信済みのアプリケーションを選択する
6. 「保存」をクリックする
7. 「設定」→「iOS」→「アプリケーション」→「『Appとブック』ライセンス」に遷移する
8. 「更新」をクリックする
 - このとき「未割り当て数」の数字が減り「使用数」の数字が増えることを確認してください。
9. 「機器」→該当機器を選択→「詳細」にて「同期」をクリックする

◀ユーザーに「Appとブック」ライセンスを割り当てる場合▶

1. 管理サイトで「ユーザー」→機器に当てるユーザーを選択→「『Appとブック』設定」に遷移する
2. 「新規作成」をクリックする
3. 「『Appとブック』ライセンス」を選択する
4. 「『Appとブック』アプリライセンス付与」欄で、をクリックする
5. 配信済みのアプリケーションを選択する
6. 「保存」をクリックする
7. 「同期」をクリックする
8. 端末側で「Appとブック参加依頼」のポップアップが表示されたら「続ける」をタップする
9. 「Agree」をタップする
10. 管理サイトで「設定」→「iOS」→「アプリケーション」→「『Appとブック』ライセンス」に遷移する
11. 「更新」をクリックする
 - このとき「未割り当て数」の数字が減り「使用数」の数字が増えることを確認してください。
12. 「機器」→該当機器を選択→「詳細」にて「同期」をクリックする

Q.21 Appとブック

「Appとブック」場所のトークンを管理サイトに複数登録しても問題はありませんか。

- **問題ありません。**
「Appとブック」場所のトークンを複数登録しても適用している端末などには影響は出ません。設定するうえでライセンスを付与するトークンを間違えないように注意してください。

Q.22 Appとブック

1つのABMアカウントで複数の企業のADEや「Appとブック」場所のトークンを管理できますか。

- **1つのABMアカウントで複数のトークンを管理することはできます。**

Q.23 Appとブック

「登録済のトークンと異なるトークンであるか、もしくは登録済のトークンが他のサービスで利用された可能性があります。トークンを登録する場合は一度削除を行い再登録してください。」と表示されます。対応方法を教えてください。

- **「Appとブック」トークンを削除、再登録する必要があります。**
以下の手順で「Appとブック」トークンを再登録してください。

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

◀事前準備▶

「Appとブック」トークンを削除した場合、「Appとブック」設定テンプレート、ユーザー、機器、組織の「Appとブック」設定が消える仕様となっております。設定を削除する前に上記設定状況を控えてください。また、設定が消えることで、「Appとブック」のライセンスが紐付いていない状態になるため、そのまま利用を続けるとAppleからの警告が表示されます。以降の設定を早々にご対応ください。

● トークンの削除

[設定] → [iOS] → [アプリケーション] → [「Appとブック」ライセンス] で [操作] → [削除] をクリックし、トークンを削除してください。

● トークンの登録手順

トークンの登録方法は以下のマニュアル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)』の「Appとブック」 - 「Appとブック」場所のトークンの年次更新 - 「Appとブック」場所のトークンをダウンロードする、 「Appとブック」場所のトークンをアップロードする」

◀「Appとブック」の再設定▶

「Appとブック」の設定方法は以下のマニュアルを参照してください。

- 『iOSアプリケーション配信 手順書』 - 「アプリをインストールする」 - 「アプリを強制インストールする」、「アプリ管理用の共通Apple IDでアプリをインストールする」
- 『Apple Business Manager (ABM) マニュアル (利用方法・年次更新手順)』の「Appとブック」 - 「書籍を配信する」

Q.24 ADE

ADEのキッティング中に表示される「リモートマネージメントから離れる」を非表示にする方法がありますか。

- **Apple側の仕様のため、非表示にはできません。**

Q.25 ADE

「ADE機器管理」の画面で端末が追加されません。どうしたらいいですか。

- **【ADEトークン登録】画面で【ADE機器再読込】をクリックして改善するか確認してください。**

改善しない場合は、以下の手順でADEトークンを削除し、ADEトークンの再登録をしてください。なお、ADEトークンを削除するとADE定義プロファイルを再度作成する必要があります。あらかじめADE定義プロファイルの内容を確認したうえでADEトークンを削除してください。

- ADE定義プロファイルの作成方法は以下のマニュアルを参照してください。
 - 『iOSキッティングマニュアル』の「ADEを利用してライセンス認証を行う」 - 「ADEを利用するための準備をする」 - 「ADE定義プロファイルを作成する」

● トークンの削除

1. 管理サイトの [設定] → [iOS] → [ADE] → [ADEトークン登録] を選択する
2. [トークンを削除] をクリックする
⇒ポップアップが表示されるので [OK] をクリックする

● トークンの登録

1. [新規作成] をクリックする
2. [ダウンロード] をクリックし、PEMファイルをダウンロードする
3. ABM (Apple Business Manager) にサインインしていただき [設定] → [MDMサーバー] 欄でトークン削除前に登録していたMDMサーバートークンを選択する
4. [編集] をクリックする
5. [MDMサーバの設定] 欄の [新規アップロード] をクリックする
6. 手順2でダウンロードしたPEMファイルを選択する
7. [保存] をクリックする
8. [トークンをダウンロード] をクリックし、ADEトークンをダウンロードする
9. 管理サイトの「ADEトークン登録」にて [アップロード] をクリックする
10. 手順8でダウンロードしたトークンを選択する
11. [保存] をクリックする
12. [設定] → [iOS] → [ADE] → [ADE機器管理] 画面に機器が表示されているか確認する
13. 表示されていない場合は [ADEサービスと同期] をクリックする

Q.26 ADE

ABMで「デバイスの所有を解除」を行った場合、ADEを利用中の端末はどうなりますか。

- **次回端末初期化後のアクティベート時まではADE端末として使用できます。**

ただし、初期化を行うとADE端末としては使うことができなくなります。また、「デバイスの所有を解除」の操作を行うと、ABM側でADE機器としての情報が削除されるため再度ADE端末として利用するにはAppleに申請するか、Mac端末に接続してApple Configrator 2からADE端末の登録を行う必要があります。

Q.27 ADE

「ADEサーバーとの同期を行いました、一部の機器へのプロファイル割り当てまたは割り当ての解除に失敗しました」というエラーが発生しました。原因と対処法を教えてください。

- **以下の状態でエラーメッセージが発生する場合があります。**

- ADEサーバーの情報何らかの原因で取得ができず、Apple側の最新情報と差分が発生している
- ADEサーバー上で該当の端末が削除されている

[設定] → [iOS] → [ADE] → [ADEトークン登録] にて [ADE機器再読込] をクリックし機器情報を読み込み直してください。

- ライセンス情報の更新には、通常「ADE機器管理」画面の [ADEサービスと同期] を使用しますが [ADEサービスと同期] は前回から変更した情報しか取得しないため、画面の内容と実際のライセンス割り当て状況の間に誤差が発生してしまう場合があります。その場合は [ADE機器再読込] を使用してADEトークンの情報をすべて更新してください。

Q.28 ADE

ADEの利用申し込みをしたのですが、利用できるようになったかを確認したいです。確認する方法を教えてください。

- **管理サイトの以下の場所に [ADE] の項目が表示されていれば適用されています。**

- [設定] → [iOS] →画面左側のメニュー

Q.29 ADE

ADE定義プロファイルの「セットアップアシスタントの省略する手順」で設定した内容は、端末に割り当てた後に変更することはできますか。

- **作成したADE定義プロファイルの設定を後から編集することはできません。**

変更する場合は管理サイトで別のADE定義プロファイルを作成し、端末に割り当てたうえで端末を初期化してください。

Q.30 ADE

「このiPhoneは監視されています。」というメッセージが表示されます。原因を教えてください。

- **本メッセージは、端末が監視対象の時に表示されます。**

- 『用語集』

Q.31 ADE

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

ADE端末がパソコンとペアリングできません。原因を教えてください。

- **ADE定義プロファイルの「Macとペアリングを許可する」設定が「いいえ」になっている可能性があります。**
「Macとペアリングを許可する」を「はい」に指定したADE定義プロファイルを新しく作成し、端末に適用後再度キッティングを行ってください。

Q.32 ポータル

ライセンス認証後のポータルにてユーザー登録画面が表示されません。原因を教えてください。

- **管理サイトの機器が組織に直接所属している場合、ライセンス認証後のポータルにてユーザー登録を行うことができません。**
管理サイトの機器を組織から外していただくか、ユーザーを介して組織に所属させることで、ポータルよりユーザー登録および変更を行うことが可能となります。

Q.33 ポータル

端末でポータルのアイコンをタップすると「長時間アクセスがなかったためサーバーから切断されました」と表示され、ポータルのホーム画面が開けません。どうしたらいいですか。

- **端末側のトークンと管理サイト上のトークンが不一致により認証エラーとなったときに、該当のメッセージが表示されます。**
表示された場合は以下を確認してください。
 - 管理サイトと端末の同期を実行する
⇒ポータルは、同期が実行されるごとに生成されますので、同期がとれない状態ですと、ポータル画面は表示できません。
 - Cookieの設定を見直す
⇒ポータルではCookieを利用しているため、Cookieの利用を許可に設定してください。

Q.34 アプリケーション配信

iOSにてアプリケーションの自動バージョンアップが行われません。どうしたらいいですか。

- **管理サイトの【機器】→該当機器の【詳細】→【ログ】にて、以下のログが表示されているかをご確認ください。**

- 機器「(機器名)」にアプリケーション「(対象アプリケーション名)」のバージョンアップを通知しました。
- 機器「(機器名)」にアプリケーション「(対象アプリケーション名)」のバージョンアップします。

「ログがある場合」

管理サイトからは、正常にアップデートの命令が出力されており、端末側にて実行されていない状態です。
端末でのアプリケーションのバージョンアップ実行については、Appleの仕様に依存いたします。

「ログがない場合」

以下をご確認ください。

- 自動バージョンアップの設定が行われているか
⇒ [設定] → [iOS] → [アプリケーション] → [アプリケーション配信] にて該当設定を選択し、「ポリシー」に自動バージョンアップを行う設定が適用されているかを確認
- 管理対象アプリポリシーの設定が正しく行われているか
⇒ [設定] → [iOS] → [アプリケーション] → [管理対象アプリポリシー] にて該当設定を選択し、「アプリのバージョンアップ：自動的にバージョンアップする」が選択されているかを確認
- 公開されているアプリケーションのバージョンと、端末内のアプリケーションのバージョンが同一でないか
 1. 管理サイト【機器】→該当機器の【詳細】→[アプリケーション]→[該当アプリケーション]→[バージョン]にて、現在インストールされているアプリケーションのバージョンを確認
 2. App Store「アップデート履歴」のバージョンより、現在インストールされているアプリケーションのバージョンと同一でないことを確認
- 公開されているアプリケーションのバージョンと、端末内のアプリケーションのバージョンが同一でないか
 1. 管理サイト【機器】→該当機器の【詳細】→[OS]より現在の端末のOSバージョンを確認
 2. App Store【情報】→[互換性]より、OSバージョンが対応しているかを確認
- 端末と同期は取れているか

Q.35 ADE

「ADEサーバーとの通信に失敗しました」と表示されたときの原因と対処方法を教えてください。

- **以下のケースにて、ADEサーバーと通信ができなくなることが過去事例に判明しております。**

- ADEトークンをダウンロード後、15～30分前後利用しなかった場合
- ADEの利用規約が更新されている場合
iOSの新規バージョンが発表されたタイミングなどに、一緒にADEの利用規約が更新される場合があり、規約の同意を行わないと、特定タイミングでADEサーバーと通信できなくなります。
- ADEサーバーにログインするときのApple IDのパスワードを変更した場合

対処方法につきましては、ADEトークンの再登録にて解消することを確認しています。

- ADEトークンを再登録した場合には、ADE定義プロファイルの再作成する必要があります。
既存キッティング済み端末には影響はありません。新しくADEトークンを登録し直したあとにキッティングする端末では、既存のADE定義プロファイルが利用できません。

1. [設定] → [iOS] → [ADE] → [ADEトークン登録] より、[トークンを削除] をクリックする
2. [編集] → [ダウンロード] より、「PEMファイル」をダウンロードする
3. ABM (Apple Business Manager) にサインイン後、[設定] → [対象MDMサーバー] を選択し [編集] をクリックする
○ ABMにサインイン後、利用規約が更新され、再度同意する旨のポップアップが表示される場合は同意する必要があります。
4. 「MDMサーバー設定」にダウンロードした「PEMファイル」を選択し適用する
5. [トークンをダウンロード] をクリックする
6. 「ADEトークン登録」へダウンロードしたトークンを登録する
○ 手順5にて、ADEトークンをダウンロード後には、即時、手順6を実施する必要があります。

Q.36 構成プロファイル

iOS端末がパソコンとペアリングできません。原因と対処方法を教えてください。

- **場合によって対処方法が異なります。**

「監視対象端末ではない場合」

管理サイトにて接続についての制御は行っておりません。

「監視対象端末である場合」

- 構成プロファイル「Apple Configurator 2 以外のホストとのペアリングを許可(監視対象のみ)：しない」
- ADE定義プロファイル「Macとのペアリングを許可する：しない」

上記の設定でPCに接続した場合は、他のPCとの接続が許可されなくなります。以下の手順にて設定を変更の上解消されるかをご確認ください。

「構成プロファイル「Apple Configurator 2 以外のホストとのペアリングを許可(監視対象のみ)：しない」にしていた場合」

● 構成プロファイルアップロードを編集

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] → 該当設定を選択 → [機能制限] にて、[編集] をクリックする
2. 「Apple Configurator 2 以外のホストとのペアリングを許可(監視対象のみ)」にチェックを入れ、[保存] をクリックする

● 設定を適用

1. [機器] → 該当機器を選択 → [詳細] → [設定の割り当て] → [構成プロファイル] にて、[編集] をクリックする
2. 手順1で作成した設定が含まれる構成プロファイルを選択し、[保存] をクリックする
3. [機器] → 該当機器を選択 → [詳細] より、「同期」をクリックする

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

4. [機器] →該当機器を選択→[詳細] → [ログ] にて、「機器[機器名]」に構成プロファイル[プロファイル名]をインストールしました。」が表示されていることを確認する

◀ADE定義プロファイル「Macとのペアリングを許可する：しない」にしていた場合▶
詳細は、Q.32をご参照ください。

Q.37 クライアント証明書

配信したクライアント証明書のファイルは、端末のどこに保存されますか。

- **クライアント証明書の保存先は、機種などにより異なります。保存先については、端末メーカーにお問い合わせください。**
 - 管理サイトはクライアント証明書の配信まで行い、インストールは端末側が行います。

Q.38 同期

iOS端末にて同期ができません。原因と対処方法を教えてください。

- **考えられる要因を下記に記載させていただきます。**
ご確認いただき該当している場合、回避方法をご実施いただきますようお願いいたします。
 - OS毎に表示項目名や手順が異なる場合があります。
 - Apple Push証明書の有効期限が切れていないか
 - 確認方法：管理サイトの [トップ画面] → [Apple Push証明書登録] の「証明書」欄
 - 回避方法：Apple Push証明書の更新作業を行う
 - Apple Push証明書の更新時に別の証明書を登録していないか
 - 確認方法：管理サイトの [機器] →該当機器選択→ [詳細] → [デバイス] の「MDMプロファイルトピック」の値と管理サイトの [トップ画面] → [Apple Push証明書登録] の「トピック」の値が一致しているか
 - 回避方法：該当機器の [MDMプロファイルトピック] の値と同じ証明書を管理サイトに登録する
 - 端末側で構成プロファイルを削除していないか
 - 確認方法：端末の [設定] → [一般] → [デバイス管理]
 - 回避方法：MDM構成プロファイルを再インストールし再認証する
 - 機内モードがONになっていないか
 - 確認方法：端末の [設定] → [機内モード]
 - 回避方法：[機内モード] をOFFにする
 - 帯域制限を使用している場合、通信要件を満たしているか
 - 確認方法：ネットワーク管理者に問い合わせる
 - 回避方法：制限しているサービスの設定で、MDMの通信要件を満たすようポートを許可する
 - 端末の電源がオフとなっていないか
 - 回避方法：電源を入れ、同期を実行する
 - 有効なSIMによるモバイル通信もしくは有効なWi-Fiアクセスポイントに接続されているか
 - 回避方法：通信が良好なWi-Fiに接続し、同期を実行する
 - 圏外および電波が届かない場所で利用していないか
 - 回避方法：通信できる環境で、同期を実行する

上記全てに該当しない場合、可能であればMDM構成プロファイルのアンインストールおよび、再度ライセンス認証を行っていただき、改善されるかをご確認ください。

Q.39 認証

iOS端末をキッキング中に「ライセンス認証中」の画面から進みません。どうしたらいいですか。

- **「ライセンス認証中」の画面から進まない場合、以下を確認することで解決する場合があります。**
 - **Apple Push証明書の値を確認**
 1. [設定] → [サービス環境設定] → [Apple Push証明書] を選択する
 2. 「トピック」の値を記録する
 3. [編集] より「2. 証明書ファイルの取得」のURL (https://identity.apple.com/pushcert/) へアクセスする
 4. 証明書一覧の各「i」のボタンより「UID=」の値と手順2で記録した値が一致するかを確認する

◀一致する証明書がある場合▶
該当証明書の「Status」が「Revoked」となっているかを確認してください。「Revoked」となっている場合、「Renew」よりApple Push証明書の更新を実施ください。

◀一致する証明書がない場合▶
新しいApple Push証明書の登録を行なってください。
 - **通信状況の確認**
接続する回線から、別のWi-Fi回線またはキャリア回線に変更して確認します。
 - ネットワーク環境の不具合により、Appleとの通信ができていない可能性も考えられます。
 - **再ライセンス認証**
APNsサーバー（Apple社側のサーバー）の処理が失敗している可能性がございます。
 1. 端末を再起動する
 2. 構成プロファイルを削除する
 3. 時間をおいてライセンス認証を実行する
 - **「Safari」のCookie設定確認・履歴の削除**
 1. OS11以降の場合：[設定] → [Safari] → [すべてのCookieをブロック] が「オン」でないことを確認する
 2. 端末にて [設定アプリ] → [Safari] → [履歴とWebサイトデータを消去] を実行する
 - **初期化・再キッキング**
 1. 管理サイトにて [機器] →該当機器を選択→ [詳細] → [この機器を削除する] をクリックする
 2. 端末を初期化する
 3. キッキングを実行する

Q.40 Webフィルタリング

Safari利用時に「以下のページは制限されているのでブラウズができません」(URL) と表示されます。原因と対処方を教えてください。

- **該当ページが「コンテンツフィルタ設定」の「アダルトコンテンツを制限」により、アクセス制限の対象となっている可能性があります。**
以下の手順にて、対象サイト自体を「許可されたURL」にすることで制限の対象から外することができます。
 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] をクリックする
 2. 対象のプロファイル名を選択する
 3. [その他] → [コンテンツフィルタ設定] を選択する
 4. [編集] を選択する
 5. 「許可されたURL」に「(制限対象になっているURL)」を設定して保存する
 6. 同期を行う

Q.41 構成プロファイル

iOS端末のコントロールセンターにQRコードのアイコンが表示されなくなりました。どうしたらいいですか。

- **「構成プロファイルアップロード」の「Appの使用を制限」で「一部のAppのみを許可」を指定している場合、コントロールセンターにQRコードのアイコンが表示されなくなります。**

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

こちらはiOS 13以上の、Appleの仕様です。「Appの使用を制限」の「一部のAppのみを許可」に、アプリケーションID「com.apple.BarcodeScanner」を設定して下さい。

- 『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)」

Q.42 ADE

ADEトークン登録画面にて「アカウント情報が取得できませんでした。」表示され、サーバー名などの情報が表示されません。原因と対処法を教えてください。

- **以下の状態にて、該当事象が発生することを確認しております。**

- Apple社側でADEの利用規約の更新、および同意を求められている状態になっている。
- ADE定義プロファイルが無効になっている。
- Apple IDに変更が生じた。

以下の手順で、改善するかをご確認ください。

◀ADE機器再読込の実行▶

[設定]→[iOS]→[ADE]→[ADEトークン登録]にて「ADE機器再読込」を実行し、「アカウント情報」が表示されるかをご確認ください。アカウント情報が表示されている画面のイメージは以下のマニュアルをご参照ください。

- 『管理サイトリファレンスマニュアル』の「設定-iOS」-「ADE」-「ADEトークン登録」-「画面 (登録後)」

◀ADEトークン登録の削除と再登録▶

1. 管理サイト [設定] → [iOS] → [ADE] → [ADEトークン登録] → [トークン削除] をクリックし、[OK] をクリックする
2. [編集] → 「1.サーバー公開鍵証明書(PEM)ファイルの生成とダウンロード」の [ダウンロード] をクリックし、PEMファイルをダウンロード、任意の場所に保存する
 - この画面は開いたままにしておいてください。
3. ABM (Apple Business Manager) にサインイン、[設定] → [対象MDMサーバー] の [編集] をクリックする
 - ファイル名: 「ADE_public_key_cer.pem」
4. 「MDMサーバの設定」 → [新規アップロード] をクリックし、手順3にて保存したPEMファイルをアップロードする
5. 「トークンをダウンロード」をクリックし、任意の場所に保存する
 - ファイル名: 「xxx_Token_yyyy-mm-ddxxx-xx-xxx.xxx.p7m」
6. 手順2で保持していた画面にて、「3.サーバートークンファイルの登録」の [参照] をクリックし、手順5にて保存したトークンをアップロードする
7. [設定] → [iOS] → [ADE] → [ADEトークン登録] にサーバー名などの情報が表示されていることを確認する

◀ADE定義プロファイルの再作成・既存ADE定義プロファイルの削除▶

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「ADEを利用してライセンス認証を行う」-「ADEを利用するための準備をする」-「ADE定義プロファイルを作成する」、「ADE定義プロファイルを適用する」

Q.43 ADE

初期設定で「"" x x x ""から構成をインストール中プロファイルをインストールできませんでした プロファイル""net.ntt-east.sdm.mdm.mdm_configuration""は対話形式でインストールする必要があります」と表示され、進めなくなりました。どうしたらいいですか。

- **端末がiOS 13以降のADE端末の場合、OSの不具合により発生することがあります。**
端末を初期化の上、再度キッティングを実施してください。

Q.44 構成プロファイル

設定アプリより「iCloud Drive」をONにできません。対処法を教えてください。

- **構成プロファイルアップロードにて、「アカウント設定の変更を許可(監視対象のみ)」が「しない」に設定をされている可能性がございます。**
以下の手順で設定を「する」に変更してください。

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] → 該当設定を選択 → [iOS制限設定] → [機能の制限] をクリックする
2. [編集] をクリック、「アカウント設定の変更を許可(監視対象のみ)」にチェックを入れ、[保存] をクリックする
3. [機器] → 該当機器を選択 → [詳細] にて、[同期] をクリックする

Q.45 位置情報

位置情報の取得契機を教えてください。

- **位置情報の測位(取得)と、管理サイトへの送信契機は異なります。**
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」-「機器の情報」-「(情報-iOS) 位置」-「iOS端末の位置情報の諸条件」

Q.46 ローミング設定

「「(機器名)」にローミング設定の変更を行いました。」のログが頻発しています。原因と対処方法を教えてください。

- **iOS12以降の端末に対して「ローミング設定」の「音声ローミング」が有効の設定を割り当てると、「(機器名)」にローミング設定の変更を行いました。」のログが同期毎に出力されます。**

原因はAppleの仕様変更で、iOS12以降より端末の [設定]→[モバイル通信] より「音声ローミング」に該当する項目が削除されたためです。上記ログが出力されている状況で、その他機能に対する影響は現状ありません。以下の手順で設定を変更の上、解消されるか確認してください。

1. [設定]→[iOS]→[便利機能]→[ローミング設定]より対象の設定を選択する
2. [編集] をクリックする
3. 「音声ローミング設定」の項目にて「無効にする」を選択する
4. [保存] をクリックする
5. 同期を実施する

Q.47 認証

ポータルを「非表示」設定にしているため、エージェントの認証はアクティベーションコードを使用しています。認証時に誤って別の端末のアクティベーションコードを使用してしまった場合はどうしたらいいですか。

- **エージェントアプリをアンインストールしたうえで、再度インストールし認証してください。**
そのまま利用すると、管理サイトに登録されている機器と実際の端末が異なってしまう、管理・運用に影響がでる恐れがあります。

Q.48 リモートワイブ

リモートワイブ (管理領域) を実行しましたが、端末の設定アプリ上部に「このiPhone (iPad) は、"" x x x ""によって監視および管理されています」と表示されています。この表示の原因と、削除する方法を教えてください。

- **「このiPhone (iPad) は、"""" x x x """"によって監視および管理されています」という表示は、監視対象端末の場合に発生します。**
リモートワイブ (管理領域) を実行することでオフィスまるごとサポートデバイスマネジメントの管理下から外れますが、監視対象端末の場合、オフィスまるごとサポートデバイスマネジメントの管理下から外れた場合でも監視対象の状態が継続されます。
該当の表示を削除したい場合は、端末の初期化を実行してください。

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)株式会社オプティム
(c)東日本電信電話株式会社

Q.49 リモート操作

管理サイトからのリモート操作指示（リモートロックやリモートワイプなど）をiOS端末が受け取れなかった場合、どのように処理が行われますか。

- **iOS端末でリモート操作の指示が受け取れなかった場合、再指示（リトライ）や再指示され続ける期間（リトライ期間）、次回同期時は、以下のとおりです。**
 - ・ リモートワイプが指示された場合は、指示が実行されるまでリトライを繰り返します。
 - ・ APNsの仕様に準拠しますが、Appleサーバー側でも少なくとも一度は配信を試み、初回に通知を配信できない場合は、必要に応じてリトライを繰り返します。
 - ・ APNsの仕様は、予告なく変更される場合があります。

Q.50 シングルAPPモード

シングルAPPモードの設定を割り当てたら、端末の画面に「アクセスガイドが利用できません」と表示され、操作ができなくなりました。原因と対処方法を教えてください。

- **対象のアプリが端末にインストールされていない場合や、対象のアプリが起動できない場合に、端末の画面に「アクセスガイドが利用できません」と表示され、操作ができなくなります。**

◀対象アプリが端末にインストールされていない場合▶


- ・ 管理サイトの [機器] → [一覧] → 対象のiOS機器 → [] → 「情報」の [アプリケーション] で、対象アプリのインストール状況を確認します。端末にアプリがインストールされていない場合は、管理対象アプリとして対象のアプリをアプリケーション配信などでアプリを配信し、端末にインストールしてください。
- ・ プリインストールアプリは、アプリケーション一覧で確認できません。
- ・ 『管理サイト リファレンスマニュアル』の「機器」 - 「一覧」 - 「機器の情報」 - 「（情報 - iOS）アプリケーション」
- ・ 削除してしまったプリインストールアプリなど、端末にインストールされていないプリインストールアプリを対象アプリに指定してしまった場合は、それぞれの端末でApp Storeから再度インストールし直してください。
- ・ App Storeからインストールできない場合の回避策はありません。可能であれば別のアプリの指定を検討してください。
- ・ iOS端末ではプリインストールされているアプリが、iPad OS端末ではプリインストールされていない場合があります。プリインストールアプリをシングルAPPモードに設定する場合は、対象のアプリがプリインストールされているか必ず確認してください。

◀対象アプリが起動できない状態にある場合▶

- ・ オリジナルアプリを対象アプリに指定している場合、オリジナルアプリが管理対象アプリとして配信されておらず、信頼が確立されていないため、起動できない状態です。管理サイトの [アプリケーション配信] で、「オリジナルアプリ」の「管理」を有効にしてください。
- ・ 『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」






Q.51 シングルAPPモード

端末と通信ができないのですが、端末からシングルAPPモードを解除する方法を教えてください。

- **端末を監視対象に設定した方法により、解除方法が異なります。**
以下のいずれかの方法で解除してください。
 - ・ 端末を監視対象に設定した方法がADE定義プロファイルで、条件1、条件2を満たしている場合は、任意のMac OS PCに接続してApple Configurator 2で解除してください。
条件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] → [iOS制限設定] の「Configurator以外のホストとのペアリングを許可(監視対象のみ)」を無効にした設定を割り当てていない
条件2： [設定] → [iOS] → [ADE] → [ADE定義プロファイル] の「Macとのペアリングを許可する」を有効にした設定を割り当てている
 - ・ 『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」
 - ・ 『管理サイト リファレンスマニュアル』の「設定 - iOS」 - 「ADE」 - 「ADE定義プロファイル」
 - ・ 端末を監視対象に設定した方法がApple Configurator 2で、監視対象にするために利用したMACアドレスが接続先のMACアドレスの場合は、監視対象にするために利用したMac OS PCに接続し、Apple Configurator 2で解除してください。
 - ・ 上記の方法で解除できない場合や、条件1、条件2のいずれかしか満たしていない場合、監視対象にするために利用したMACアドレスが接続先のMACアドレスではない場合は、USBイーサネット変換アダプタなどを用意し、有線LANでネットワークに接続して管理サイトで以下の操作を行うことで、解除することもできます。
1. [機器] → [一覧] → 対象のiOS機器 →  [機器] → [設定の割り当て] → [シングルAPPモード] の [編集] をクリックする
 2. [シングルAPPモード] のリストボックスから [(設定内)] を選択する
 3. [保存] をクリックする
 4. [同期] をクリックする
 5. 『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」

Q.52 シングルAPPモード

シングルAPPモードの対象に指定したアプリが自動アップデートされません。原因を教えてください。

- **非管理対象として配信されたアプリはアップデートされません。**
自動アップデートを有効にした管理対象アプリとして、対象のアプリをAppストアから再配信してください。
 - ・ プリインストールアプリは管理対象として配信できないため、本事象の回避策はありません。
1. [設定] → [iOS] → [アプリケーション] → [管理対象アプリポリシー] →  をクリックする
 2. 「ポリシー名」を入力する
 3. [自動的にバージョンアップする] にチェックを入れる
 4. [保存] をクリックする
 5. [設定] → [iOS] → [アプリケーション] → [アプリケーション配信] →  をクリックする
 6. 「設定名」を入力する
 7. 「App Storeアプリ一覧」の  をクリックする
 8. 「Stoer ID」を入力する
 9. [有効] にチェックを入れる
 10. 手順1~4で作成したポリシーをリストボックスから選択する
 11. [保存] をクリックする
 12. [設定] → [iOS] → [アプリケーション] → [シングルAPPモード (監視対象のみ)] →  をクリックする
 13. 「設定名」と「アプリケーションID (Bundle Identifier)」を入力する
 14. [保存] をクリックする
 15. [機器] → [一覧] → 対象のiOS機器 →  [機器] → [設定の割り当て] → [シングルAPPモード] の [編集] をクリックする
 16. [シングルAPPモード] のリストボックスから、手順12~14で作成した設定を選択する
 17. [保存] をクリックする
 18. [同期] をクリックする
- ・ 『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」
 - ・ 『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」
 - ・ 『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」 - 「シングルAPP モード (監視対象のみ)」
 - ・ 『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」

Q.53 ロックダウンモード中にデバイスマネジメント エージェントを利用できますか。

- **ロックダウンモード中はデバイスマネジメント エージェントを利用できません。**
ロックダウンモードは、ごく一部の個人を対象としたサービスで、モード中は端末が通常通りに機能しなくなるため、動作をサポートしていません。ロックダウンモードの詳細については、Appleのサイトを参照してください。
- ・ <https://support.apple.com/ja-jp/HT212650>
- ・ ロックダウンモード中は、プロファイルのインストールができないため、ライセンス認証や構成プロファイル、教育プロファイルなどもインストールできなくなります。

- ライセンス認証後にロックダウンモードに切り替えた場合は、一部の機能は動作しますが動作は保証できません。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社


Q.54 同期

iOSの同期はどのような契機で行われますか。



- **iOSの同期は、MDM構成プロファイルによって行われる同期とエージェントによって行われる同期があります。**

MDM構成プロファイルによって行われる同期では、エージェントの変更された内容は更新されず、エージェントによって行われる同期では、MDM構成プロファイルの更新などは行われません。

◀MDM構成プロファイルによって行われる同期の契機▶

- 定期同期による自動同期が行われたとき
 - 定期同期は、前回の自動同期から約8時間毎に行われます。
- 端末側のポータルで [同期] をタップしたとき
- 管理サイトの [機器] → [一覧] →  で「同期」をクリックしたとき
- 端末を起動、または再起動したとき (Appleの仕様により、同期される場合があります。)
- 端末がスクリーンロック中に構成プロファイルを配信し、構成プロファイルのインストールが延期された状態で、パスコードを入力してスクリーンロックを解除したとき (Appleの仕様により、同期される場合があります。)

◀エージェントによって行われる同期の契機▶

- エージェント認証時
- エージェントの  をタップしたとき
- メッセージ配信を受信後にメッセージ画面を表示したとき
- 管理サイトの [機器] → [一覧] →  で「同期」をクリックしたとき
- 基地局を変更したとき
- Background Fetchを使用したとき

目次

[管理サイト](#)[Androidエージェント](#)[iOSエージェント](#)[Windowsエージェント](#)[サービス企業用サイト](#)[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

Windowsエージェント

Q.1 エージェントがインストールできません。

- **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クライアント リファレンスマニュアル』の「Windowsクライアントについて」 - 「エージェントの動作環境」
 - 『Windowsキティングマニュアル』の「Windowsクライアントについて」 - 「エージェントの動作環境」
- **エージェントダウンロード時にInternet Explorer 9をご利用の場合**
エージェントダウンロードができない場合があります。インターネットオプションの「詳細設定」タブにある「暗号化されたページをディスクに保存しない」のチェックを外し、再度ダウンロードを行ってください。

Q.2 エージェントのライセンス認証が行えません。

- **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。
- **企業コードや認証コードが間違っていないか。**
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。
- **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。

Q.3 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。

- **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できます。以下を参照して、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「エージェントの基本操作」 - 「エージェントの状態を確認する」
- **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キティングマニュアル』の「エージェントのインストール」 - 「エージェントをインストールする」
 - 『Windowsクライアント リファレンスマニュアル』の「エージェントの基本操作」 - 「ライセンスを認証する」

Q.4 パスワードの入力を求められます。

- **以下の場合に求められます。**
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。

Q.5 ライセンス認証の解除が行えません。

- **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。以下を参照して、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「コントロールパネルの使用法」 - 「エージェントを起動する」

Q.6 エージェントの操作マニュアルを閲覧したいです。

- **管理サイト上で閲覧できます。**
管理者へお問い合わせください。

Q.7 複数の機器が同一機器として登録されてしまいます。

- **管理サイトではMACアドレスなどで機器の識別を行っています。**
しかし、認証時に同一のUSB LANアダプターを使いまわしたり、仮想化ソフトウェアなどによる仮想ネットワークアダプターが設定されている場合に、異なる機器でも同一のMACアドレスが割り当てられるため、管理サイトでは、各機器を同一機器として判定し、機器情報を上書きします。同一のMACアドレスを持つ機器や仮想ネットワークアダプターを機器から削除した後に、Windowsエージェントのライセンス解除/再認証を行うことで、別々の機器として認識されるようになります。

Q.8 1つの機器が別の機器として登録されてしまいます。

- **以下のような場合に別の機器として認識されることがあります。**
OS再インストールやリカバリー後の再認証時、SIDが再発行されるため、別の機器として認証される場合がございます。別の機器として登録された場合は、機器画面より、古い方の機器の削除を行ってください。

Q.9 機器検出

機器検出機能を停止させる設定方法を教えてください。

- **「管理外機器の検出」を無効にすると、機器検出機能の停止が可能になります。以下の手順で「管理外機器の検出」を無効にしてください。**

≪認証済み機器を個別に設定する場合≫

1. [サイトマップ] → 「Windows」の [エージェント個別管理] をクリックする
2. 対象の設定を選択して、「編集」をクリックする
3. 「管理外機器の検出」で [無効] を選択し、「保存」をクリックする
4. [機器] → 対象機器を選択 → [設定] → 「設定」の [設定の割り当て] をクリックする
5. [エージェント個別管理] → [編集] をクリックする
6. 手順3で作成した設定を選択し、「保存」をクリックする
7. 「同期」をクリックする
8. 手順4で選択した対象機器のみ機器検出機能が停止します。全機器に設定する場合は、「全機器一括設定」を使用してください。

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)株式会社オプティム
(c)東日本電信電話株式会社

◀対象のネットワーク内の機器全てに対して設定する場合▶

1. [設定] → [Windows] → [管理アプリの通信と動作] → [編集] をクリックする
2. 「ライセンス認証オプション」の「なし」を選択し、「保存」をクリックする
3. [サイトマップ] → 「機器」の「ネットワーク」をクリックする
4. エージェント認証済の対象のネットワークを選択して、「編集」をクリックする
5. 「管理外機器の検出」で「無効」を選択し、「保存」をクリックする
6. 既に機器検出機能が有効な端末には、すぐに反映されません。端末の再起動を行ってください。

Q.10 認証

エージェントをインストールしたWindows端末のデータを他の端末に複製（クローニング）することで、複数台の端末を同時にキッキングすることはできますか。

- **親となるWindows端末のデータを他の端末に複製する場合、エージェントのインストールまでできます。**
エージェント認証作業は別途行う必要があります。

Q.11 外部デバイス

USBデバイスまたは、SDデバイスが禁止できません。原因を教えてください。

- **『禁止できる外部デバイスのパターン一覧』に記載のないデバイスを使用されている可能性があります。**
外部デバイス設定では、外部デバイスの列挙子、サービスおよびクラス GUIDの組み合わせが特定のパターンに該当する場合のみ、「禁止」の設定が有効になります。
 - 『管理サイトリファレンスマニュアル』の「設定 - Windows」 - 「セキュリティ」 - 「機能制限 / 外部デバイス」 - 「禁止できる外部デバイスのパターン一覧」

Q.12 SIM抜き差し監視

SIMの抜き差しを行っていないのに、ロック画面が表示されます。対処法を教えてください。

- **Windowsの「WWAN Auto Config」サービスのスタートアップの種類を「自動」に変更することによって改善する場合があります。**

● 「WWAN Auto Config」サービスの設定値を確認する手順

1. デスクトップ上のタスクバー左下にある「Windowsマーク」を右クリックする
2. [Windows PowerShell(管理者)]をクリックする
3. 以下のコマンドを入力し、Enterキーを押す
 - `get-service WwanSvc | select-object displayname,name,starttype`

⇒出力された情報が以下の場合、サービスは「手動」に設定されています。

DisplayName Name StartType

WWAN AutoConfig WwanSvc Manual

● 「WWAN Auto Config」サービスの設定値を確認する手順

1. デスクトップ上のタスクバー左下にある「Windowsマーク」を右クリックする
2. [Windows PowerShell(管理者)]をクリックする
3. 以下のコマンドを入力し、Enterキーを押す
 - `set-service -Name WwanSvc -StartupType Automatic`

4. 設定状態を確認するため、以下のコマンドを入力し、Enterキーを押す
 - `get-service WwanSvc | select-object displayname,name,starttype`

⇒出力された情報が以下の場合、サービスは「自動」に設定されています。

DisplayName Name StartType

WWAN AutoConfig WwanSvc Automatic

5. 機器を再起動するため、以下のコマンドを入力し、Enterキーを押す
 - `Restart-Computer -Force`

Q.13 スクリーンロック

端末から設定した管理用・利用者の[プロパティ]→[パスワードの有効期限]をオフィスまるとサポートデバイスマネジメントから「無制限」に設定することはできますか。

- **オフィスまるとサポートデバイスマネジメントから「無制限」に設定することはできません。**
オフィスまるとサポートデバイスマネジメントからパスワードの有効期限を無期限に設定した場合でも、端末の管理用・利用者の[プロパティ]→[パスワードの有効期限]→[パスワードを無期限にする]の設定は無効となります。

Q.14 リモート操作

管理サイトからのリモート操作指示（リモートロックやリモートワイプなど）をWindows端末が受け取れなかった場合、どのように処理が行われますか。

- **Windows端末でリモート操作の指示が受け取れなかった場合、再指示（リトライ）や再指示され続ける期間（リトライ期間）、次回同期時は、以下のとおりです。**
 - リトライは行われず、リトライ期間もありません。
 - 電源断や端末のスリープ、ネットワーク切断などで指示が受け取れなかった場合は、次回の同期時に指示された動作を実行します。

Q.15 同期

Windowsの同期はどのような契機で行われますか。

- **Windowsの同期は、以下の契機で行われます。**
 - 端末を起動 / 再起動したとき
 - 管理サイトで指定した時間が経過したとき（定期同期）
 - 『管理サイト リファレンスマニュアル』の「設定 - Windows」 - 「管理アプリの通信と動作」
 - Windows端末のツールバーから同期をしたとき（手動同期）
 - 「デバイスマネジメント エージェントコントロールパネル」から [終了] → [起動] をクリックしたとき
 - アップデートしたとき
 - デバイスマネジメント エージェントをインストールしたとき

Q.16 同期

Windows端末と同期ができません。原因と対処方法を教えてください。

- **端末側で同期を行うための条件を満たしていない可能性があります。以下を確認してください。**

- 端末の電源がオフになっていないか
対処方法：電源をオンにして同期する
- 端末がスリープ状態になっていないか
対処方法：スリープを解除して同期する
- 機内モードがオンになっていないか
確認方法：端末の [設定] → [ネットワークとインターネット] → [機内モード]

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

対処方法：[機内モード] をオフにする

- Wi-Fiがオフになっていないか
確認方法：端末の[設定] → [ネットワークとインターネット] → [Wi-Fi]
対処方法：[Wi-Fi] をオンにする
- ライセンスが認証状態にあるか
確認方法：端末の画面を確認する（タスクアイコンに赤色の！マークが表示されている）
対処方法：ライセンスを認証する
 - 『Windowsクライアント リファレンスマニュアル』の「エージェントの基本操作」 - 「ライセンスを認証する」
- 通信ができない場所で利用していないか
対処方法：通信が可能な環境で同期する
- Windows端末起動時にハイパーネーションが発動すると、同期が行われない場合があります。
- OSや端末により、表示項目や手順が異なる場合があります。

Q.17 同期

管理サイトとWindows端末間で最後に同期が行われてから、次の定期同期が行われるまでの時間を教えてください。

- **次回の定期同期は、最後の同期（定期同期、または手動による同期）が行われてから、管理サイトで設定された通信間隔が経過すると開始されます。**
ただし、時刻のカウントは端末内のタイマー機能で行われるため、端末を休止状態やS3スリープ状態にした場合は、カウントが停止し、停止していた時刻の分だけ遅れて同期が開始されます。
 - 定期同期の間隔を30分に設定し、端末を10分間休止状態にした場合の動作例
最終回同期時刻 09:00（10分間カウント）
端末休止開始時刻 09:10（10分間カウント停止）
端末休止終了時刻 09:20（20分間カウント）
次回同期時刻 09:40
 - 端末の電源をオフにした場合もタイマーは停止しますが、次回の端末起動時に自動的に同期が行われます。
 - 定期同期の通信間隔は、[管理アプリの通信と動作]の「管理サーバーとの通信間隔」で「分数」「時間」「日数」ごとに指定できます。。
 - 『管理サイト リファレンスマニュアル』の「設定 - Windows」 - 「管理アプリの通信と動作」

目次

[管理サイト](#)

[Androidエージェント](#)

[iOSエージェント](#)

[Windowsエージェント](#)

[サービス企業用サイト](#)

[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

■ サービス企業用サイト

Q.1 サービス企業用サイトが開けません。

- **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。
- **ご使用お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「サービス企業用サイトとは」 - 「管理サイトの動作環境」

Q.2 「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。

- **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日目を過ぎると、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。

Q.3 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。

- **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。

■ 目次

[管理サイト](#)[Androidエージェント](#)[iOSエージェント](#)[Windowsエージェント](#)[サービス企業用サイト](#)[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

用語	解説
5G	5th Generation (第5世代移動通信システム) の略称。 4G (第4世代移動通信システム) に比べ飛躍的に通信速度が向上した通信システム。
Active Sync	Microsoftが提供するモバイル端末用のデータ同期用のソフトウェア。
Android	Googleが開発した携帯端末用のOS (オペレーションシステム) 。
Android Enterprise	Android のビジネス向けプログラム。本製品でAndroid端末を管理する場合は、事前にこのプログラムと連携します。
App Manager	本製品の関連アプリケーションを安全にインストール/アップデートできるAndroidエージェントの機能。従来版エージェントで使用します。 従来版エージェントのサポートは終了しました。
App Store	Appleが運営する、有料または無料でApple製携帯端末用のアプリを配信するサービス。
Apple Configurator	Mac OS端末に搭載されている、企業や学校法人に向けたiOS端末の管理アプリ。 USBでiOS端末に接続することで、端末情報の取得、アプリケーション配信、制限設定などが行えます。
Apple Push証明書	Apple のサーバーへアクセスするための証明書。iOS端末と管理サイト間で通信を行うために使用します。
Background Fetch	iOSが日々のユーザーの使用状況を学習し、適切なタイミングで対象のアプリを起動する機能。 Appleが提供している機能でiOS 7.0 以上に搭載されています。
Bluetooth	数メートルの端末間接続に使われる、短距離の無線通信技術。
Bypass Code	iOS 7.1 以上の端末のアクティベーションロックの解除を行う場合に、管理サイト、端末およびアクティベーションサーバー (Apple) 間のやり取りで発生する26文字の英数字のコード。 通常、管理者や端末利用者が使用する必要はありませんが、Apple への確認や救済措置に必要となります。
CA証明書	認証局 (CA) により発行されたデジタル証明書。 CA : Certification Authority
Device Owner Mode (DOM)	Android 5.0 からGoogle が提供を開始した、MDM製品 (本製品など) から端末へより強固な設定を行うための特別なモード。 一部、端末によってはDOM に対応していない場合があります。
Exchange設定	Exchange Serverと端末を接続するための、接続先や接続ポリシーなどの設定。
Full device management solution set	企業所有のデバイス向けに設計された機能。 この機能を使うと、管理者はデバイス全体を管理でき、より強固なポリシー制御を実現できます。
Exchange設定	Exchange Serverと端末を接続するための、接続先や接続ポリシーなどの設定。
Google Playストア	Googleが運営する、有料または無料でAndroid携帯端末用のアプリケーションを配信するサービス。
GPS	人工衛星からの電波を受信して位置を特定するシステム。
GUID	管理サイトに登録されている端末を個々に識別するために使用するための識別子。
IMEI/MEID	端末を識別するためにつけられている固有の識別子。 IMEI : すべてのモバイル端末につけられている固有の値。 MEID : CDMA系の移動機識別番号。
iOS	Appleが製造するiPhone用のOS (オペレーションシステム) 。
iPad OS	Appleが製造するiPad用のOS (オペレーションシステム) 。 iPadはiOSを使用していたが、2019年9月のiOS 13リリースよりiPad専用のiPad OSを使用しています。
iTunes Store	Appleが運営する、音楽や動画、アプリケーションなどを配信するサービス。
Jailbreak状態	開発元が端末にかけている制限が、非正規な方法で解除された状態。
managed Google Playストア	企業向けのGoogle Playストア。 一般に公開されているアプリケーションのほか、企業が個別にオリジナルアプリを公開することもできます。 Android Enterpriseを利用する場合は、managed Google Playストア経由でないとアプリケーションの配信はできません。
managed Google Play Account	Android Enterpriseアカウント登録を行い、管理サイト上で端末とユーザーを紐付けると、自動的に作成・端末へ紐づけられるアカウント。このアカウントに対してアプリケーションが配信されます。
MDM	Mobile Device Managementの略称。 企業などで利用されるモバイル端末を一元的に監視・管理するための情報システムやソフトウェアのこと。
MDM構成プロファイル	MDMに関する各種の設定が記述されたXML形式のファイル。 iOS端末を管理するときに端末にインストールします。
NFC	数センチ程度の通信に使われる近距離無線通信技術。
NFCキッピング	NFCを使ったAndroidエージェントのキッピング方法。 Android 6.0~9のNFC対応端末でのみ利用できます。
Push通知	管理サイトから端末に対して、リアルタイムに通信を行うこと。
QoS マーキング	指定した特定のオーディオ/ビデオ通話アプリをマーキングし、他のアプリよりも優先して通信を行い、ネットワークを適切に管理する機能。
QRコード	デンソーウェーブが開発した2次元コード。 特定のQRコードを読み込むことで、Androidエージェントのキッピングを行います。 Android 7.0以上に対応しています。
root化	解放されていないAndroid OSのシステム管理者権限を、特殊な方法で取得し、Linuxカーネル部分を含むファイルシステムにアクセスができる状態にすること。
SIM	携帯端末などで通信をするために必要なICカード。 電話番号や契約内容など、加入者を特定する情報が記録されています。

FAQ一覧

目次

管理サイト

Androidエージェント

iOSエージェント

Windowsエージェント

サービス企業用サイト

用語一覧

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

SSID	Wi-Fiのアクセスポイントに付けられる英数字の名称。
Store ID	App Storeで管理されているアプリケーションごとのID。 IDの確認方法は、使用しているブラウザにて「アプリ名 App Store」で検索します。表示されたURLにStore IDが含まれています。
URL	Webサイトのアドレス。 例) http://www.xxxx.co.jp/
USBデバック	Android端末のアプリケーション開発を行うときに利用する、開発向けの機能。
VPN	インターネット上に作る仮想の専用ネットワーク。 専用線のような通信が可能となり、特定の人のみが安全に利用できます。
Wi-Fi	無線LAN通信。
Windows	マイクロソフト社が開発したOS（オペレーションシステム）。
アクティベーションコード	本製品のエージェント認証時に必要な英数字の文字列。
アップロード	ネットワークを通じて、データや情報をホストコンピュータに転送する操作。
アプリケーション、アプリ	アプリケーションソフトウェアの略称で、ソフトウェアの一種。 OS（オペレーションシステム）上で動作します。
アプリケーションID	アプリを識別するためにアプリに付けられている固有の文字列。 アプリの使用制限などで、アプリを指定する場合に使用されます。
インストール	アプリケーションやソフトウェアなどを、スマートフォンやPCに読み込んで使用できる状態にする操作。
エージェント	管理サイトと通信を取り、端末やシステムの監視、制御などを自律的に行うアプリケーション。
オプションパッケージ	標準で備わっている機能に加え、任意に追加するプランの総称。
キッティング	本製品で端末を管理するために必要な設定を行うこと。 端末を設定するための管理サイトの設定も含まれます。
キャプティブネットワーク	ユーザ登録や通信料の支払いが必要な公共のWi-Fi ネットワーク。
クライアント	情報や機能の提供を受ける端末、ソフトウェア。
クライアント証明書	電子証明書の種類。 端末の使用者が正規の利用者であることを証明します。
グループポリシー	端末やアプリケーションの設定内容を一括で管理するWindowsの機能。
コントロールパネル	Windowsエージェントの制御（一時停止やアンインストールなど）を行うためのGUI（グラフィカルユーザーインターフェース）。
サーバートークン	外部サーバーと通信をとるために必要となる情報を集約している文字列のデータ。
サービス企業	本製品を提供する企業。サービス企業は利用企業の登録などを行います。
スクリーンロック	各OSに標準装備されているロック画面。
ストレージ	スマートフォンやPCのデータを保存する補助記憶装置。 HD、DVD、USBメモリのほか、インターネット上の補助記憶装置としてオンラインストレージなどがあります。
スワイプ	タッチパネルにて指を触れたまま特定の方向になでる操作。
ソフト、ソフトウェア	WindowsやiOSなど、PCやスマートフォンを制御するコンピュータープログラムの総称。
タスクトレイアイコン	Windowsエージェントがインストールされている端末で、画面右下に表示されるアイコン。 ユーザーの環境により表示される位置は異なります。
チャンネル	データの通り道。接続するチャンネルによって、配信される更新プログラムが異なります。
ツールバー	Windowsエージェント起動時に、画面右下に表示される棒状のエリア。
トークン	一定時間のみの有効な文字列のデータ。
バージョン番号	アプリケーションに定められたバージョン管理用の整数表示番号。
パスコード	iOS端末に標準装備されている画面ロックを解除するときに入力する文字列。
パッケージ	特定の要素でまとめられたサービス群。
ブラウザ	インターネット上にあるWeb サーバーの情報をみるためのアプリケーション。 例) Google Chrome やFirefox など
プロキシ設定	プロキシサーバーへ接続するための設定。 Wi-Fi 設定でのプロキシ設定と3G 設定でのプロキシ設定がありますが、特に指定がない場合は、Wi-Fi 設定でのプロキシ設定のことを指します。
ブラックリスト	禁止するものや項目を列挙したリスト。
ホワイトリスト	許可するものや項目を列挙したリスト。
モデル	端末の型番。
ライセンス	本製品を使用するために契約する権利。 ライセンス契約数の範囲内で、端末やユーザーを登録できます。
ライセンス認証	本製品を利用するために端末で認証すること。
リモート操作	端末を遠隔で操作すること。
ランタイムパーミッション	端末で実行中のアプリケーションがカメラやアドレス帳などのアプリケーションを使用する場合に、それらのアプリケーションを使用するための、アクセス権限の許可を求める仕組み。
ログ	端末の利用状況、データが送受信された日時や操作内容などの記録。
監視対象	iOS端末に対して管理範囲を拡張できる端末設定モード。 Apple Configurator 2やAutomated Device Enrollmentを活用し端末を設定できます。
管理サイト	管理下にある端末の情報を確認したり、その端末に対して各種の設定や制御を行うためのサイト。
管理者	システム全体のすべての内容に対して強力な権限を有する人。
管理対象	管理者によって管理されている、端末やアプリケーション。

FAQ一覧

目次

[管理サイト](#)

[Androidエージェント](#)

[iOSエージェント](#)

[Windowsエージェント](#)

[サービス企業用サイト](#)

[用語一覧](#)

最終更新日 2024年4月11日
(Web サイトver.9.18.0)

株式会社オプティム
(c)東日本電信電話株式会社

企業コード	管理サイトを識別するための文字列。
企業ドメインメールアドレス	法人、企業などが仕事で使用するためのメールアドレス。 法人メールアドレスとも呼ばれ、企業などでドメインを購入して独自にアドレスを作成します。
構成プロファイル	管理サイトや、Appleが提供しているApple Configurator 2上で作成できるプロファイル。 iOS端末に対する制御や設定ができます。
従来版Androidエージェント	Android 9未満のOSに対応していたAndroidエージェント。 Android 9以上では使えません。
設定セット	端末に対する設定や制御を管理サイト上で定義した設定値で、機器、ユーザー、組織に割り当てられる状態を指す。 設定セットを割り当てることで設定を反映することができます。 ポリシーや設定セットに紐づける設定は「設定」や「設定値」になります。
組織	ユーザーや端末の情報をまとめるためのグループ。
端末使用者	本製品を利用する端末の使用者。
同期	管理サイトと端末で通信を取ること。 通信を取ることによって端末の情報を収集したり、端末に設定を送ることができます。
認証コード	本製品のライセンス認証に必要な英数字の文字列。 企業コードと合わせて端末から指定することで、本製品が使用できるようになります。
非公開ネットワーク	Wi-Fi のネットワーク名称を非表示としているネットワークが、端末のネットワークリストに表示された場合のネットワーク名称。
紛失モード	Appleが提供しているiOSの紛失モードに対応した機能。 紛失、盗難にあった場合に遠隔ロックをかけたり、メッセージを表示することができます。
利用企業	本製品を利用する企業。利用企業はサービス企業に対して本製品の利用の申し込みを行います。