Optimal Biz

かんたん初期設定マニュアル

最終更新日　2024 年 7 月 15 日

（Web サイト ver.9.21.0）

株式会社オプティム

はじめに

本マニュアルは、Optimal Biz（以降、本製品と呼ぶ）を使用する以下の方を対象に、設定方法や操作方法を説明します。

●はじめて本製品を使用する方

●小規模に Android 端末や iOS 端末を導入したい方

●簡単なセキュリティ設定を行いたい方

本マニュアルの第 1 章「端末の管理を開始する」では、本製品で端末の管理を開始する最低限の設定方法を記載しています。また、第 2 章「補足・便利な操作」は、設定にかかわる補足や知っていると便利な操作などを説明しています。必要に応じて参照してください。

本マニュアルの内容を理解いただくために要点となる各種の内容を以下に記載しています。マニュアルを読まれる前に、これらの内容をご理解ください。

名称・呼称

本マニュアルに登場する特定の企業、人について、以下の定義で記載しています。

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

注意・ポイントマーク

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

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

記号

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

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

参照マーク

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

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

用語集

不明な用語は、以下を参照してください。

☞『よくあるご質問（FAQ）』

免責事項

- 本マニュアルは、ユーザー種別が［管理者］のユーザーを対象としています。［管理者］以外のユーザー種別でログインした場合は、操作が制限されます。
- iPad OS の操作は iOS と同様です。差異がある場合は iPad OS 用の記載をしています。
- 画面上のバージョン表記は、実際の表示と異なる場合があります。
- 本マニュアルに記載されている Web サイトの URL は、予告なく変更される場合があります。
- OS のバージョンやブラウザーにより、一部の画面や操作が異なる場合があります。本マニュアルでは、Google Chrome を例に説明しています。

登録商標

- Apple、iPad、iPadOS、iPhone、Mac、macOS は、米国およびその他の国で登録された Apple Inc.の商標です。
- iOS は、Apple Inc.の OS 名称です。
  IOS は、Cisco Systems, Inc.またはその関連会社の米国およびその他の国における登録商標または商標であり、ライセンスに基づき使用されています。
- iPhone 商標は、アイホン株式会社のライセンスに基づき使用されています。
- App Store は、Apple Inc.のサービスマークです。
- Android、Google Chrome、Google Cloud、Google マップ、Google Play、Google Workspace は、Google LLC の商標です。
- Microsoft、Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Windows の正式名称は、Microsoft Windows Operating System です。 Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- その他記載の会社名、製品名は、各社の登録商標および商標です。

目次

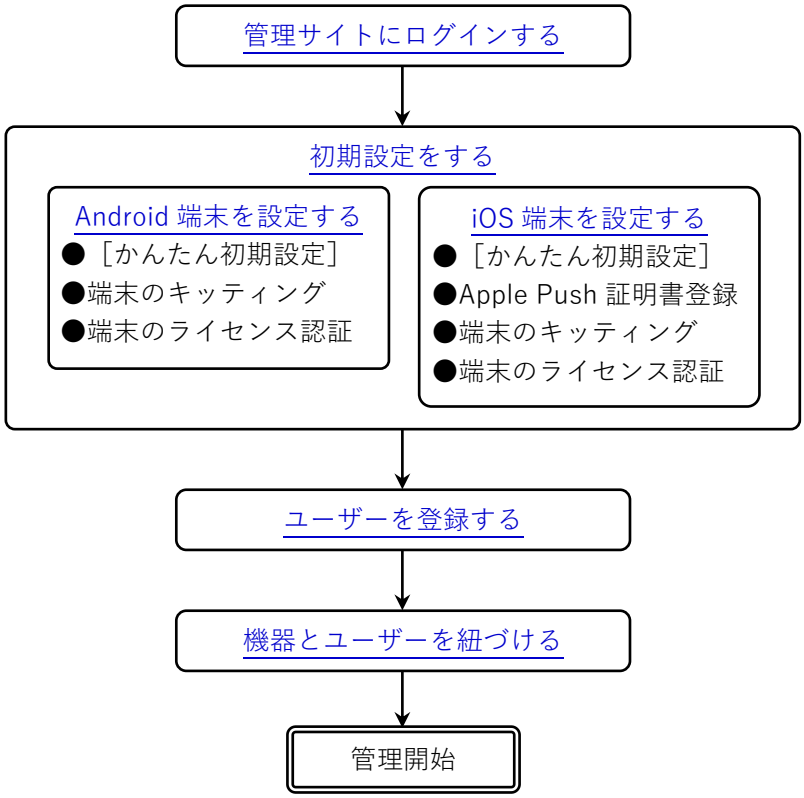
1 端末の管理を開始する

本製品で端末の管理をはじめて行う場合は、以下のフローにしたがって設定します。

端末の管理に必要な最低限の設定が完了し、端末の管理を開始することができます。

本製品を使用するための環境や端末、アカウントなどは事前に準備してください。

Android 端末は、初期化された状態にしてください。



高度な設定やアプリ配信などは、必要に応じて設定してください。

- 『管理サイト リファレンスマニュアル』
- 『Android Enterprise アプリケーション配信 手順書』
- 『iOS アプリケーション配信 手順書』
- 『Android（AMAPI）アプリケーション配信 手順書』

本マニュアルでは、Android 端末と iOS 端末の基本的なキッティング方法の手順を説明しています。監視対象端末など強固なセキュリティで端末をキッティングしたい場合は、以下を参照してください。

- 『Android キッティングマニュアル』
- 『iOS キッティングマニュアル』

Windows 端末、Mac OS 端末、Android（専用デバイス）端末のキッティング手順は、以下を参照してください。

- 『Mac OS キッティングマニュアル』
- 『Windows キッティングマニュアル』
- 『Android（AMAPI）キッティングマニュアル』

1.1 管理サイトにログインする

管理サイトとは、管理下にある端末情報の確認や、その端末に対して各種の設定、制御を行うためのサイトです。ここでは、管理サイトへのログイン方法について説明します。

管理サイトの URL、企業コード、ユーザーID またはメールアドレス、パスワードは、事前に確認してください。

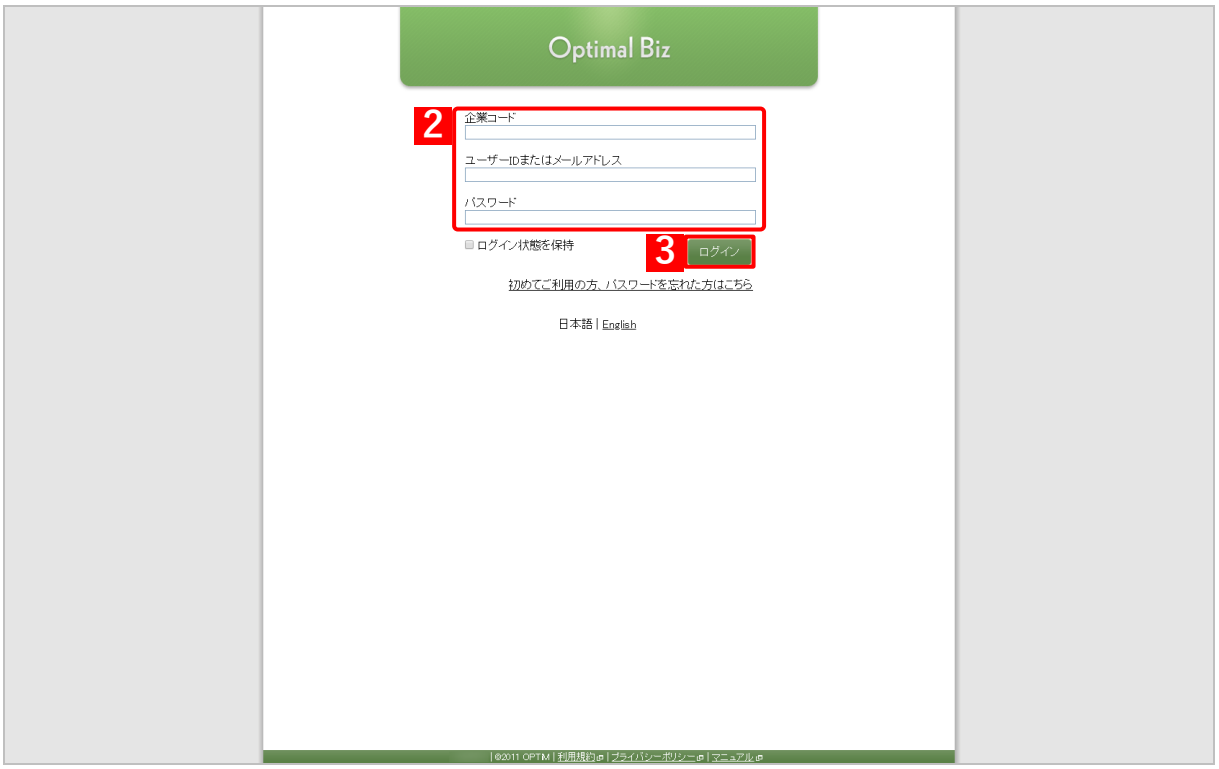
パスワードを新規発行したい場合は、以下を参照してください。

「パスワードを新規発行／再発行する」39 ページ

2 段階認証で管理サイトにログインすることもできます。詳細は以下を参照してください。

「2 段階認証で管理サイトにログインする」

【1】ブラウザーに管理サイトの URL を入力してログイン画面を表示します。
【2】「企業コード」、「ユーザーID またはメールアドレス」、「パスワード」を入力します。
【3】［ログイン］をクリックします。
⇒管理サイトのダッシュボードが表示されます。



1.2 初期設定をする

［かんたん初期設定］を使用して、セキュリティ設定などの初期設定を管理サイトで行い、端末に反映します。

［かんたん初期設定］の手順中に、端末のキッティング、ライセンス認証を行います。［かんたん初期設定］が完了した時点で、初期設定が端末に反映されます。本マニュアルでは、Android 端末と iOS 端末の基本的なキッティング方法の手順を説明します。

「Android 端末を設定する」8 ページ

「iOS 端末を設定する」21 ページ

［かんたん初期設定］で作成された設定セットは、「EasySetup」という設定名で作成されます。設定内容は必要に応じて変更することができます。設定内容については、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「サービス環境設定」―「かんたん初期設定」

OS ごとに管理方式や同期の仕組みなどが異なります。詳細は、以下を参照してください。

「管理方式」54 ページ

「同期」55 ページ

1.2.1 Android 端末を設定する

［かんたん初期設定］を使用して、Android 端末を管理サイトに登録します。

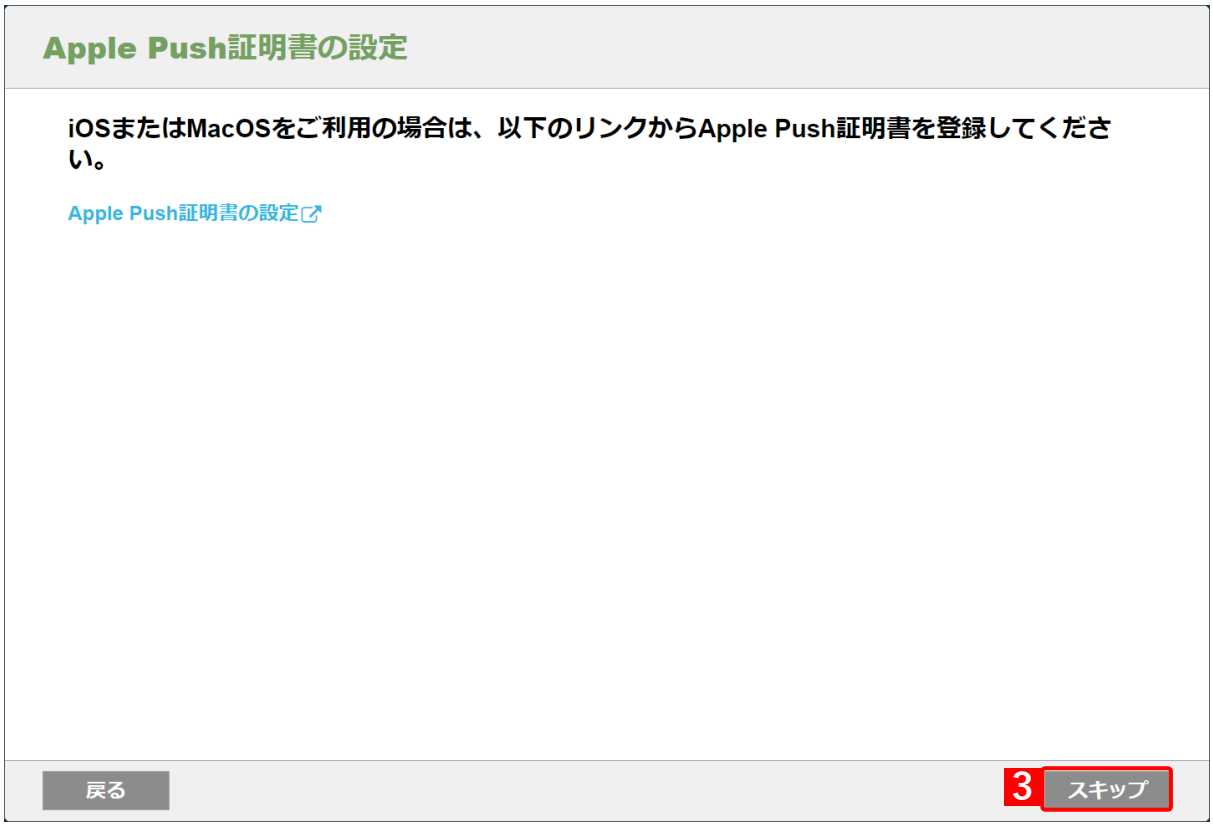
設定をはじめる前に、Android 端末を初期化してください。

【1】［かんたん初期設定］をクリックします。

⇒「かんたん初期設定の開始」画面が表示されます。

【2】［開始］をクリックします。

【3】［スキップ］をクリックします。

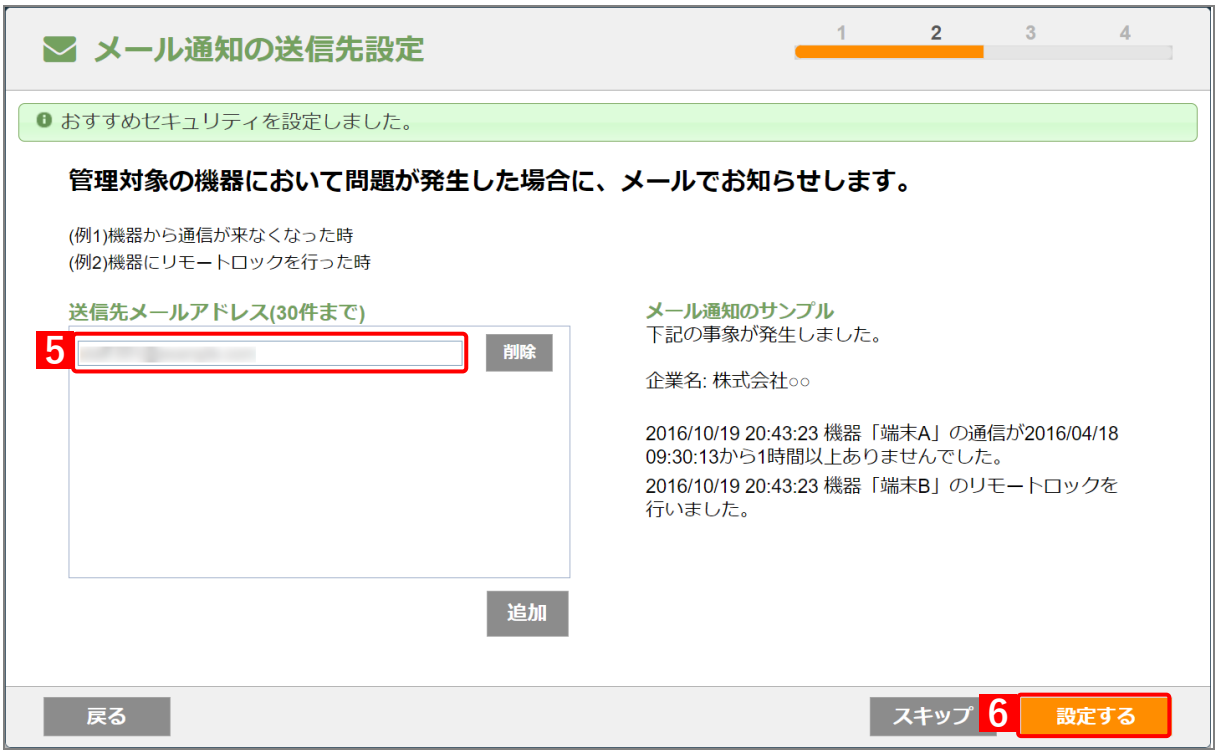


【4】［設定する］をクリックします。

【5】管理者のメールアドレスや端末を管理する部署のメーリングリストを入力します。

端末で問題が発生したときに、通知が受け取れるメールアドレスを入力してください。

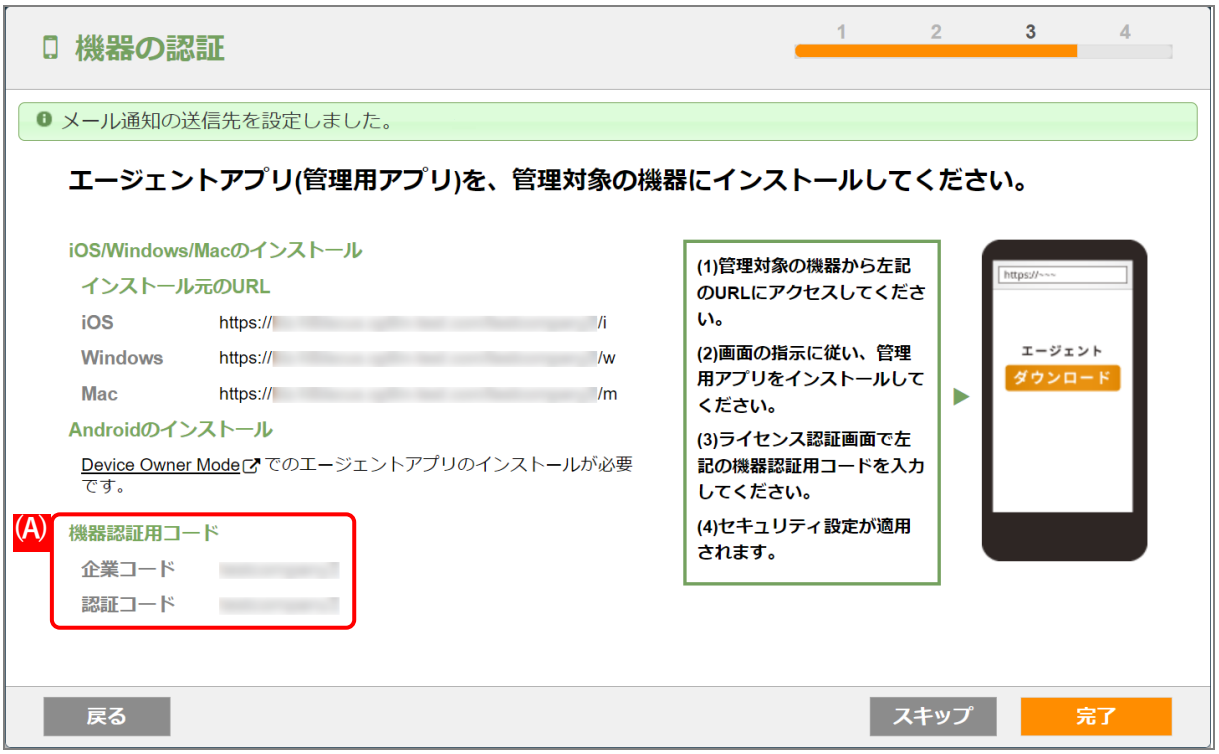
【6】［設定する］をクリックします。



⇒「機器の認証」画面が表示されます。
引き続き Android 端末でキッティングとライセンス認証を行います。

ライセンス認証を完了後に使用しますので、「機器の認証」画面は閉じないでください。

（A）「企業コード」「認証コード」は手順【32】で使用します。



【7】［始める］をタップします。

【8】接続したい Wi-Fi の SSID をタップして、Wi-Fi に接続してください。

⇒ネットワーク接続が開始されます。

必ずネットワークに接続して、以降の手順を進めてください。

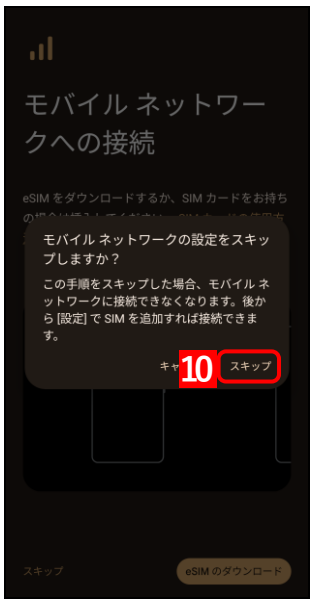
【9】［スキップ］をタップします。

SIM が挿入されている場合は、表示されません。

モバイルネットワークを利用する場合は、(A)［SIM カードの使用方法］を確認して、設定してください。

【10】［スキップ］をタップします。

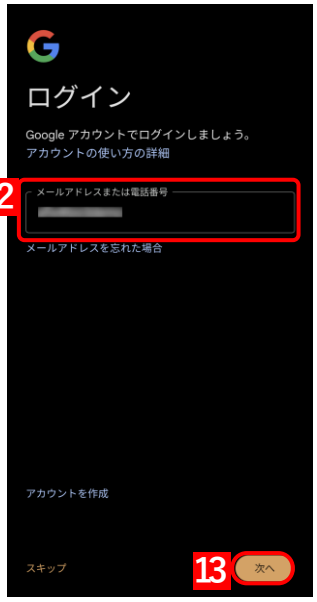
SIM が挿入されている場合は、表示されません。



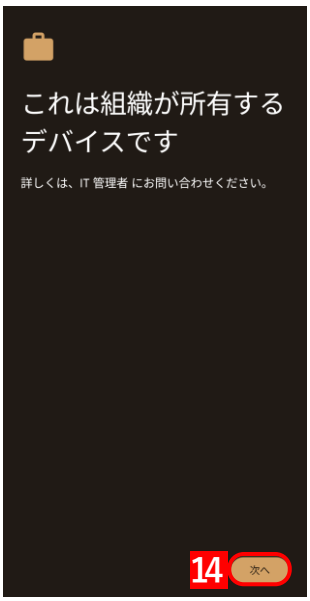
【11】［コピーしない］をタップします。

【12】「メールアドレスまたは電話番号」に「afw#biz3」と入力します。

【13】［次へ］をタップします。

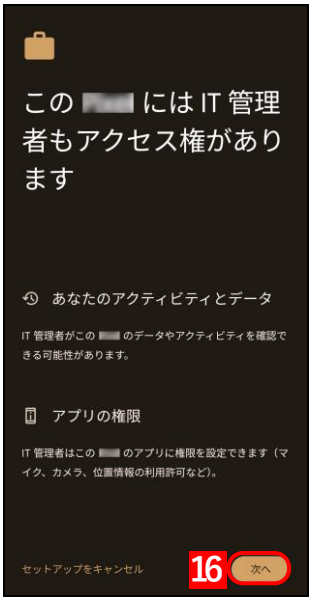


【14】［次へ］をタップします。



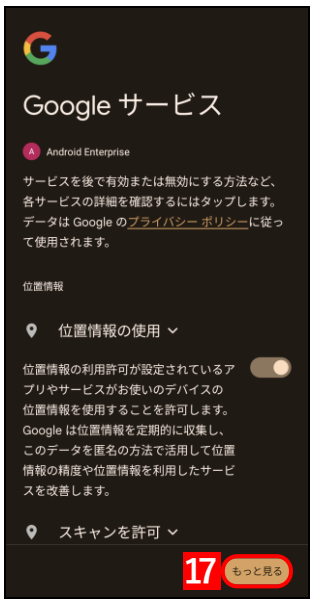
【15】［同意して続行］をタップします。

【16】［次へ］をタップします。

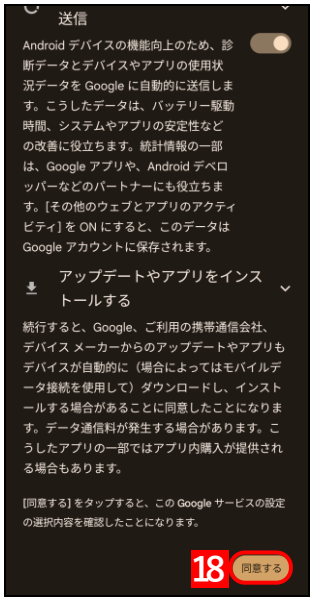


【17】［もっと見る］をタップします。

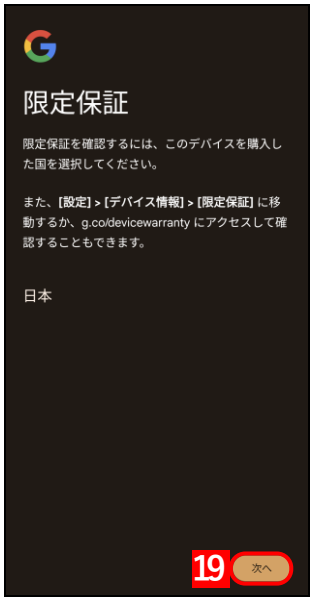
端末によっては［もっと見る］が数回表示されます。［同意する］が表示されるまで、タップします。



【18】［同意する］をタップします。

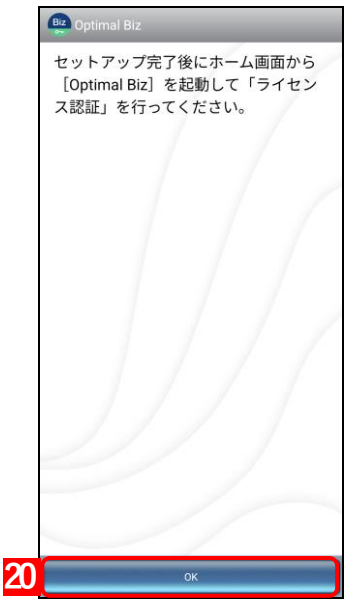


【19】［次へ］をタップします。



【20】［OK］をタップします。

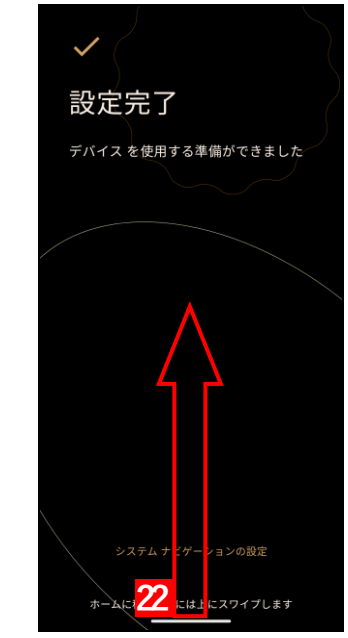
本画面は、機種や OS によって表示されるタイミングが異なる場合があります。



【21】［スキップ］をタップします。

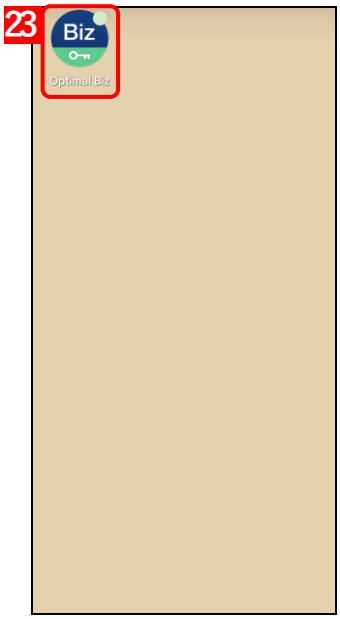
【22】画面下部からスワイプします。

⇒ホーム画面に移動します。



【23】［Optimal Biz］をタップします。

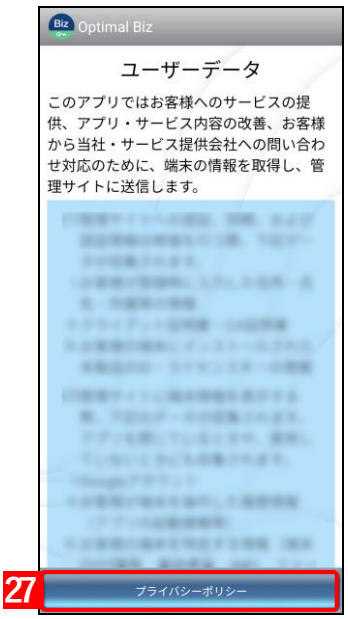
ホーム画面にアイコンが表示されない場合は、アプリ一覧を確認してください。



【24】［ライセンス認証］をタップします。

【25】「利用規約に同意する」にチェックを入れます。
【26】［OK］をタップします。

【27】ユーザーデータについて確認して、［プライバシーポリシー］をタップします。



【28】「プライバシーポリシーに同意する」にチェックを入れます。

【29】［OK］をタップします。

⇒「利用権限の要求」画面が表示されます。

【30】画面の案内に従って設定を行ってください。

Android 11 以上でエージェントバージョン 9.19.0 以上の場合、（A）任意権限に「すべてのファイルへのアクセス」が表示されます。条件を満たしていない場合は、「ストレージ権限」が表示されます。

Android 12 以上でエージェントバージョン 9.14.0 以上の場合、（A）任意権限に「付近のデバイス権限」が表示されます。

Android 13 以上でエージェントバージョン 9.16.0 以上の場合、（A）任意権限に「通知権限」が表示されます。

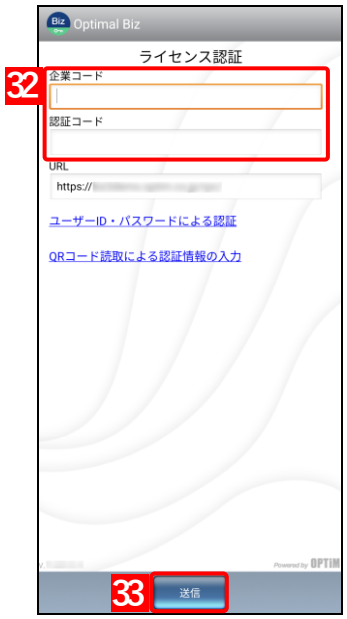
【31】［OK］をタップします。

【32】「企業コード」、「認証コード」を入力します。

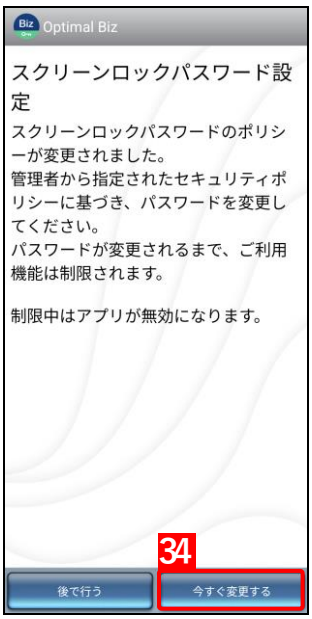
「企業コード」と「認証コード」は、［かんたん初期設定］の「機器の認証」画面に表示されています。

【33】［送信］をタップします。

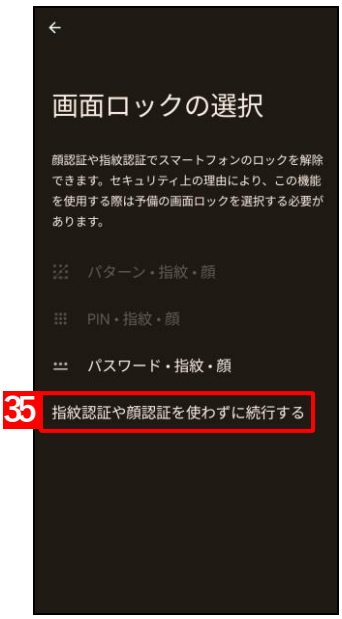
⇒ライセンス認証が完了します。「スクリーンロックパスワード設定」画面が表示されます。



【34】［今すぐ変更する］をタップします。



【35】［指紋認証や顔認証を使わずに続行する］をタップします。



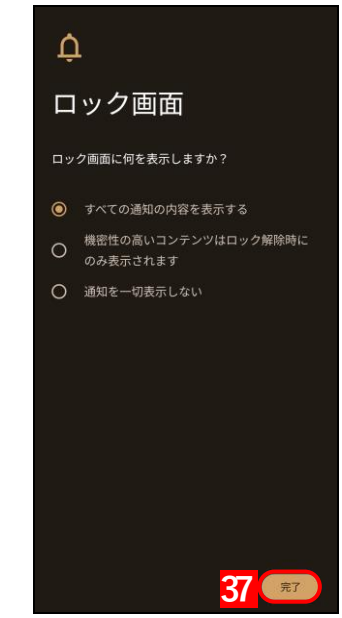
【36】「パスワード」をタップします。

⇒パスワード設定画面が表示されます。画面の指示にしたがい、パスワードを設定してください。

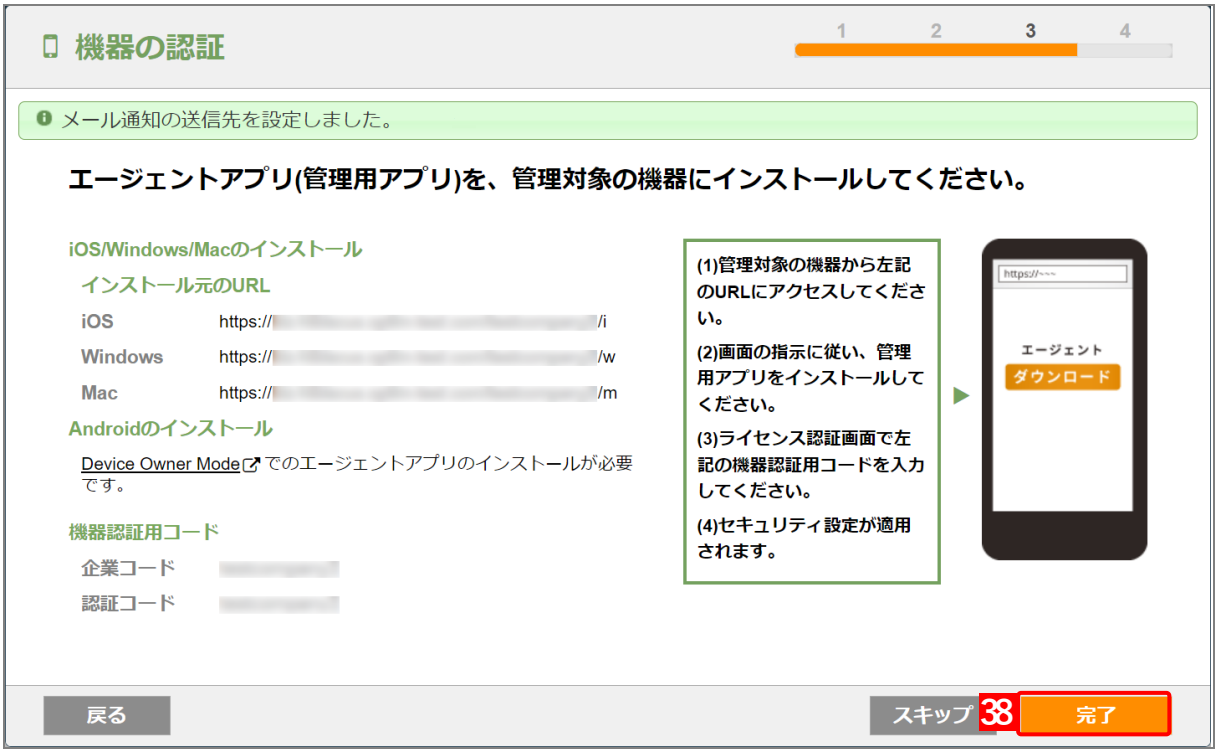
パスワードは、英数字を含む 8 文字以上で設定してください。

【37】［完了］をタップします。

⇒［かんたん初期設定］の「機器の認証」画面に戻ります。

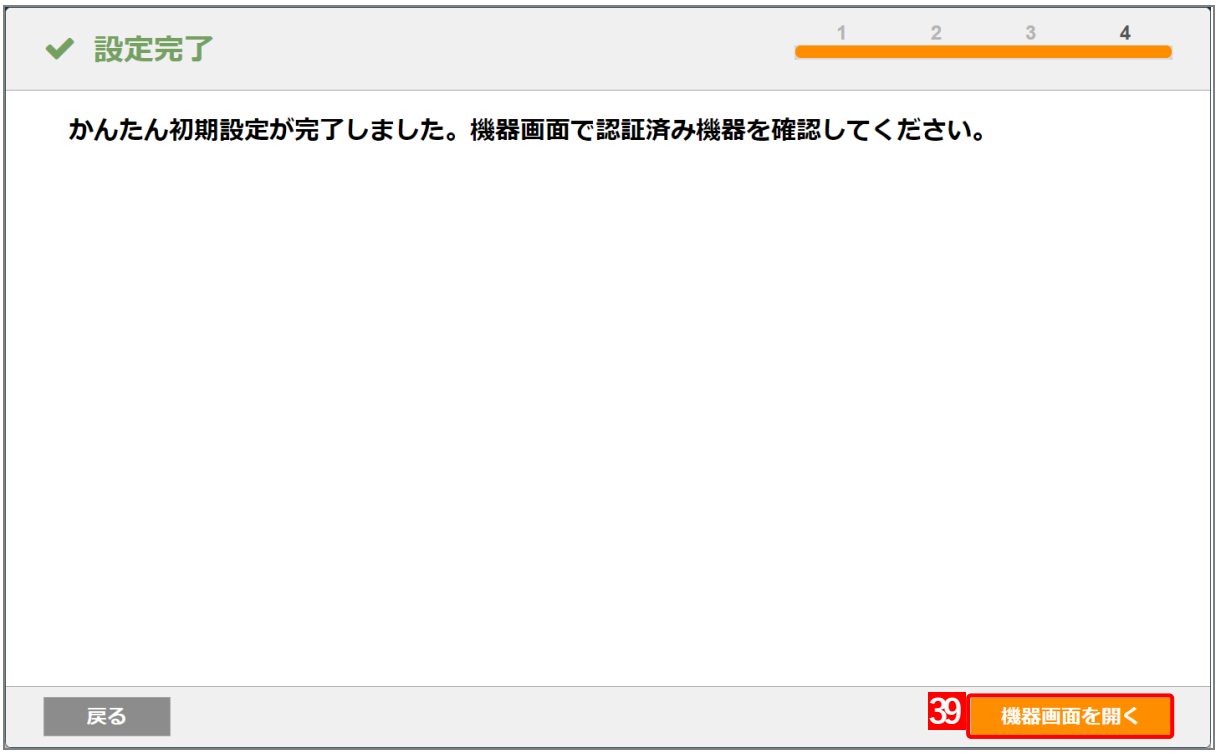


【38】［完了］をクリックします。



【39】［機器画面を開く］をクリックします。

⇒［機器］画面が表示されます。



1.2.2 iOS 端末を設定する

［かんたん初期設定］を使用して、iOS 端末を管理サイトに登録します。

設定をはじめる前に、Apple ID を準備してください。

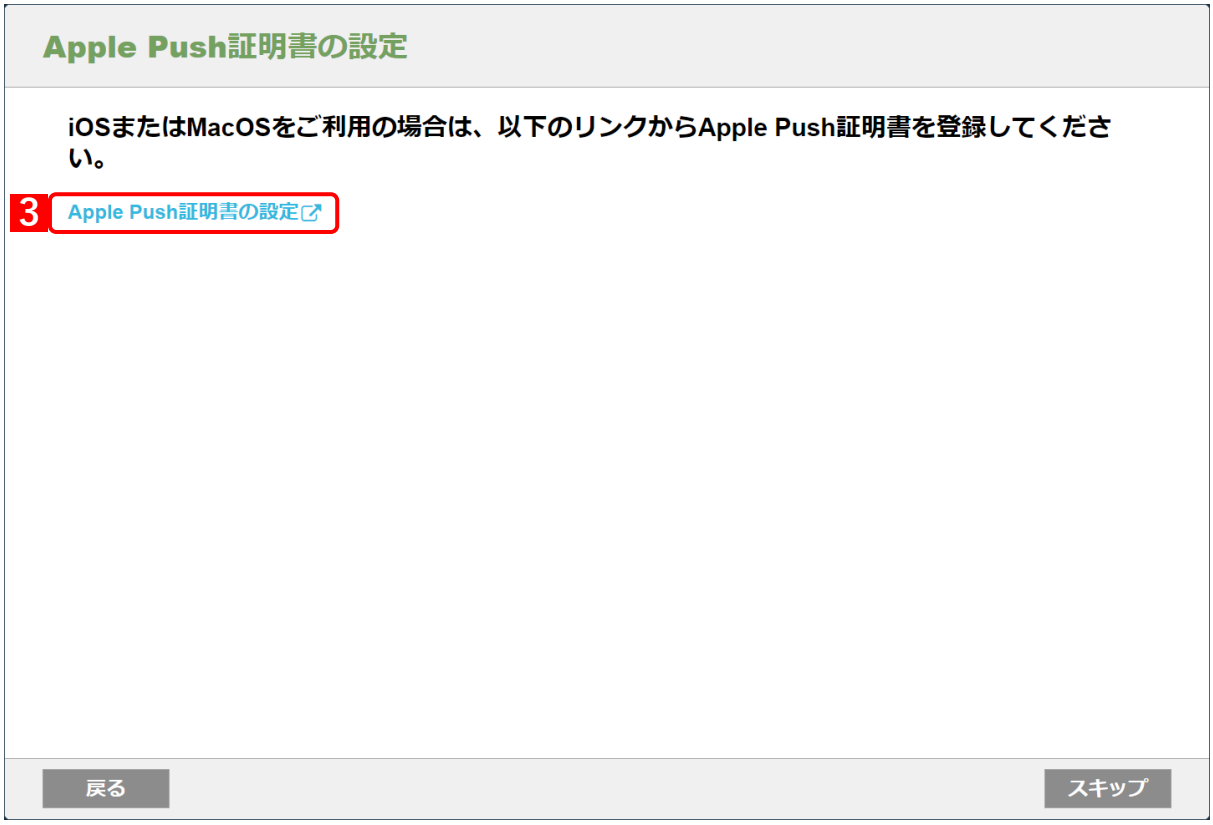
【1】［かんたん初期設定］をクリックします。

⇒「かんたん初期設定の開始」画面が表示されます。

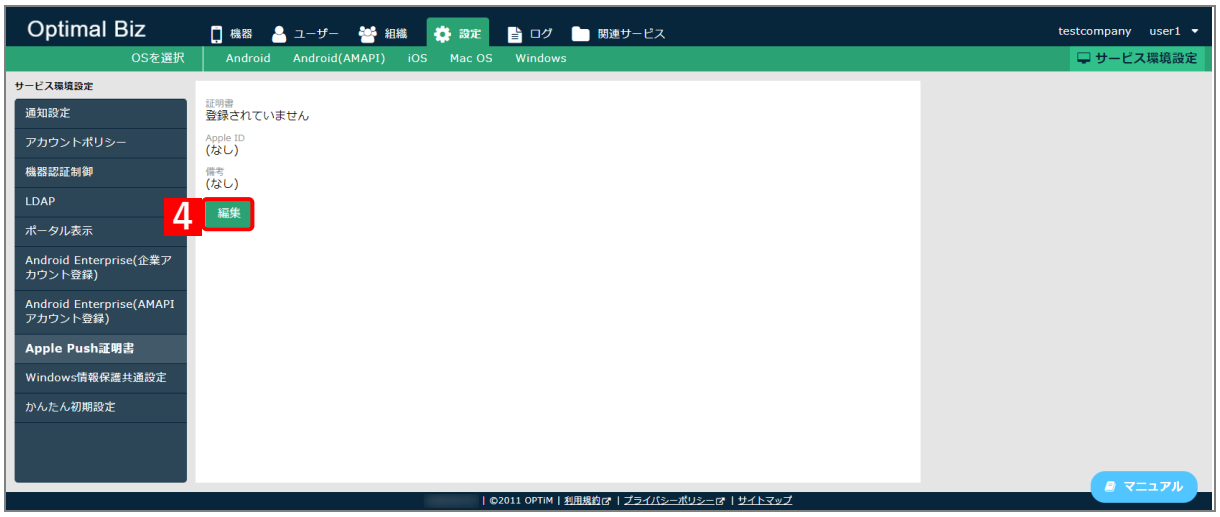
【2】［開始］をクリックします。

【3】［Apple Push 証明書の設定］をクリックします。

⇒［Apple Push 証明書］画面が表示されます。



【4】［編集］をクリックします。



【5】［ダウンロード］をクリックします。

⇒手順【16】で必要となる「署名済みの証明書要求（CSR）ファイル」のダウンロードが開始されます。任意の場所を指定して、ファイルを保存してください。

【6】［https://identity.apple.com/pushcert/］をクリックします。

⇒Apple Push Certificates Portal が表示されます。以降の操作は、Apple Push Certificates Portal のサイトで行います。

【7】管理者用の「Apple ID」を入力します。

【8】→ をクリックします。

⇒「パスワード」入力欄が表示されます。

【9】「パスワード」を入力します。

【10】 をクリックします。

⇒本人確認用の「確認コード」を受け取る電話番号を選択する画面が表示されます。

【11】「確認コード」を受け取る電話番号を選択します。

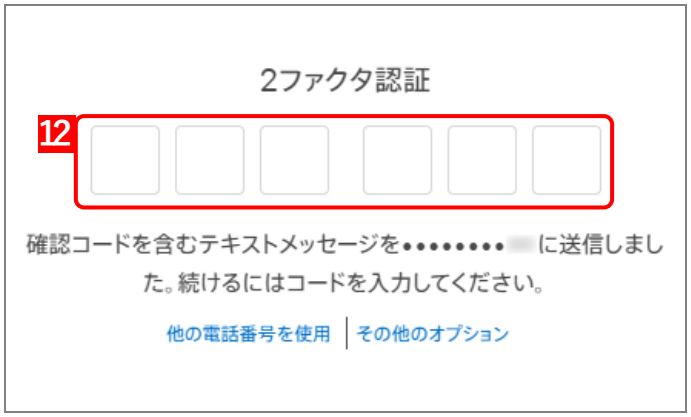
⇒選択した電話番号の端末に「確認コード」が送信されます。

複数の電話番号が登録されている場合は、選択肢が表示されます。

【12】受信したメッセージを確認し、「確認コード」を入力します。

⇒6 桁の入力が終わると、自動的に次の画面に進みます。

「確認コード」に誤りがあるとログインできず、手順【7】の「Apple ID」入力画面に戻ります。

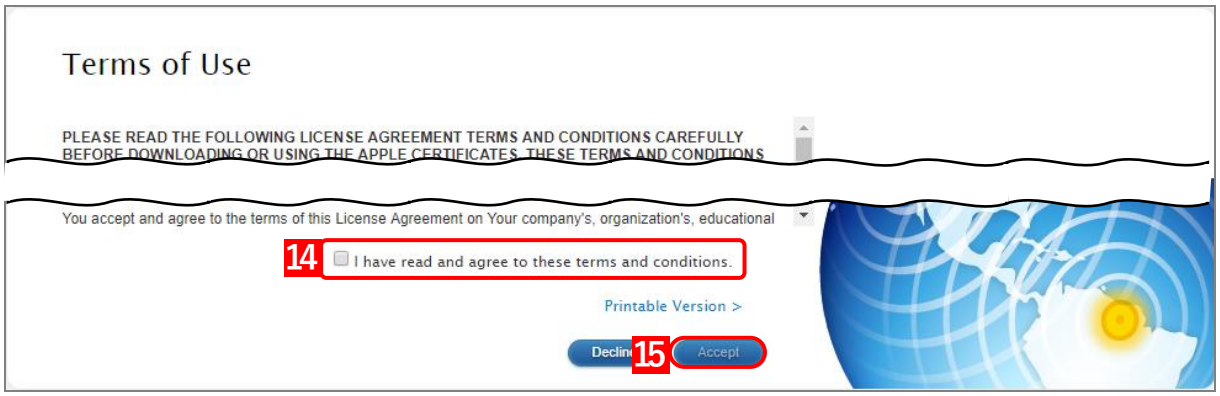


【13】［Create a Certificate］をクリックします。

新規登録とすでに登録されている場合、画面の表示が異なります。

【14】規約を確認し、チェックボックスにチェックを入れます。

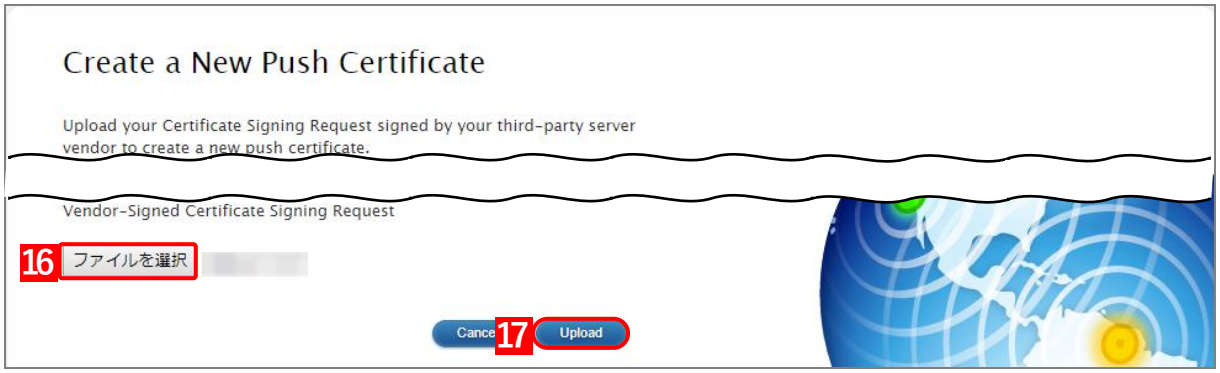
【15】［Accept］をクリックします。



【16】［ファイルを選択］をクリックし、手順【5】でダウンロードした「署名済みの証明書要求（CSR）ファイル」を指定します。

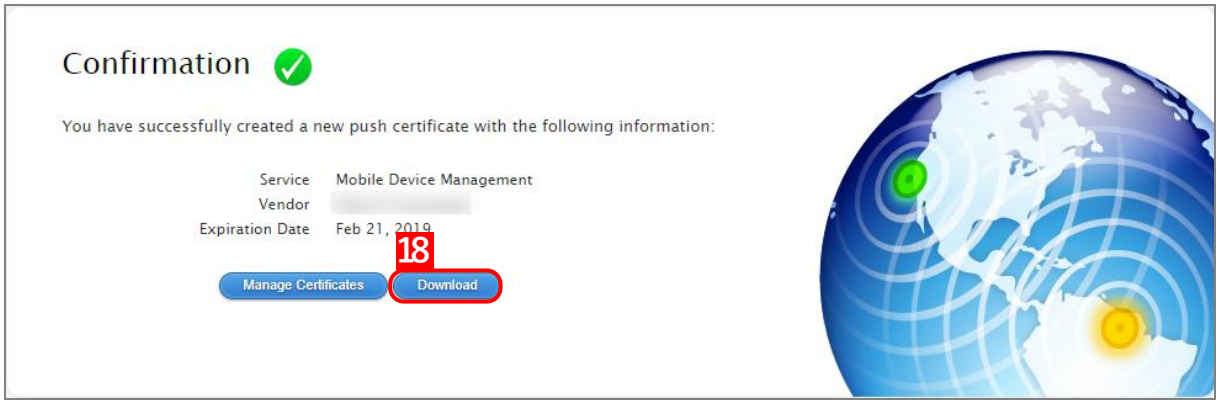
【17】［Upload］をクリックします。

⇒Apple Push 証明書が作成されます。



【18】［Download］をクリックします。

⇒Apple Push 証明書のダウンロードが開始されます。任意の場所を指定して、ファイルを保存してください。管理サイトに戻って、［Apple Push 証明書］の編集画面を表示してください。



【19】［ファイルを選択］をクリックし、手順【18】でダウンロードした Apple Push 証明書を指定します。

⇒（A）選択したファイル名が［ファイルを選択］の右側に表示されます。

【20】「Apple ID」に Apple Push Certificates Portal のサインイン時の Apple ID を入力します。

【21】「備考」を入力します。

Apple Push 証明書の取得日の入力をお勧めします。

【22】［保存］をクリックします。

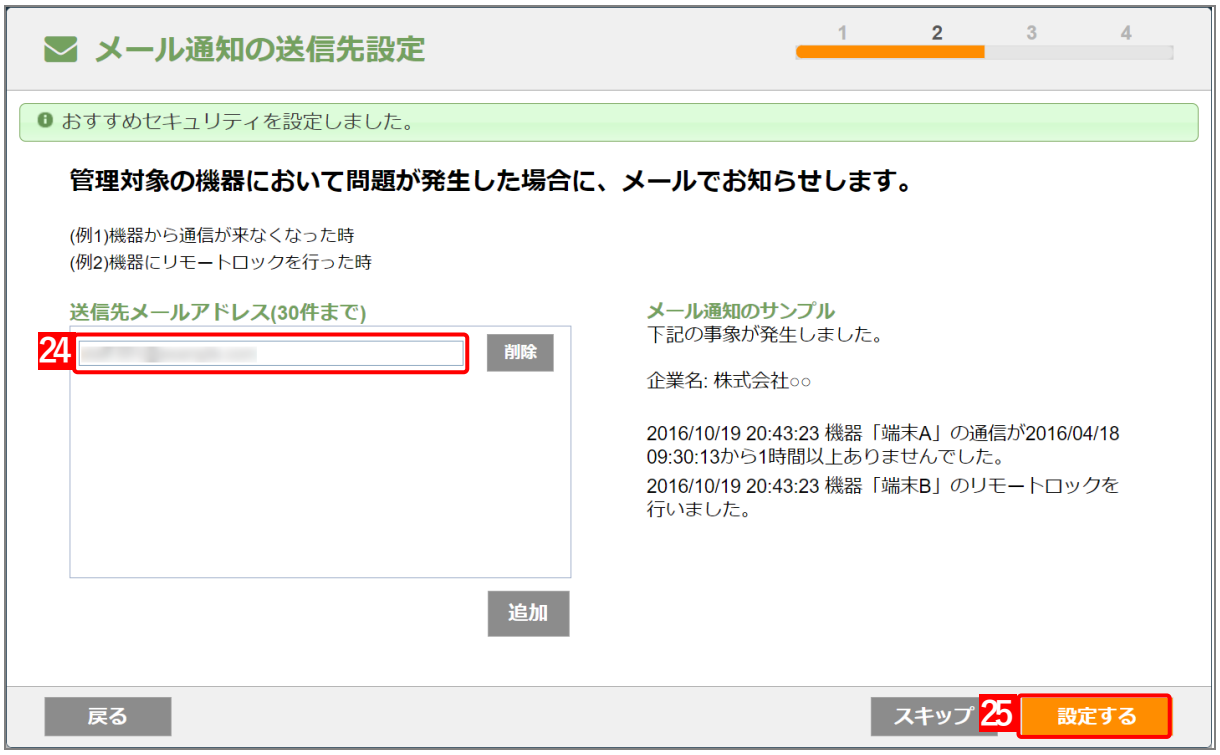
⇒［Apple Push 証明書］画面が表示されます。
［かんたん初期設定］に戻り、「おすすめセキュリティ画面」を表示してください。

【23】［設定する］をクリックします。

【24】管理者のメールアドレスや端末を管理する部署のメーリングリストを入力します。

端末で問題が発生したときに、通知が受け取れるメールアドレスを入力してください。

【25】［設定する］をクリックします。

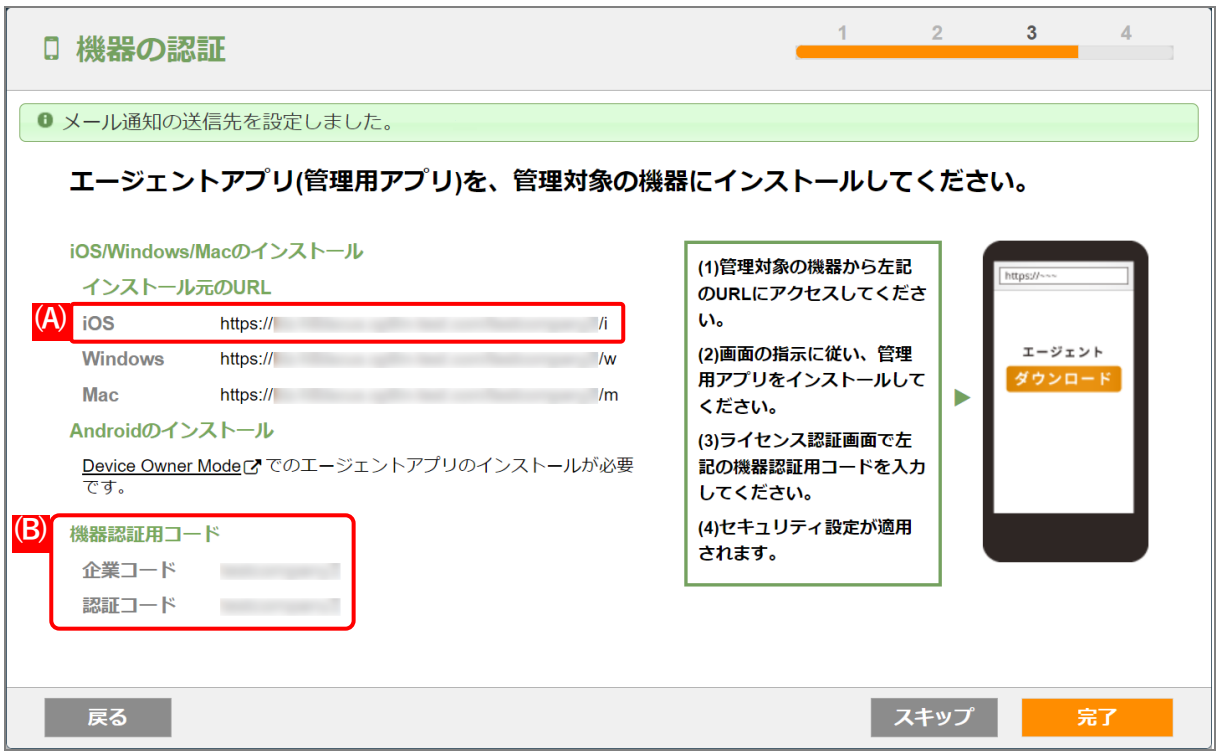


⇒「機器の認証」画面が表示されます。
引き続き iOS 端末でキッティングとライセンス認証を行います。

ライセンス認証を完了後に使用しますので、「機器の認証」画面は閉じないでください。

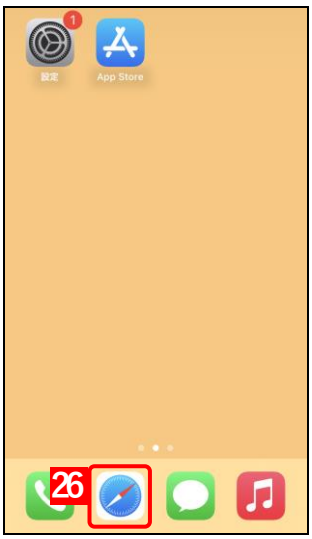
（A）「URL」は手順【27】で使用します。

（B）「企業コード」「認証コード」は手順【29】で使用します。



【26】ホーム画面の［Safari］をタップします。

使用できるブラウザーは、Safari のみです。



【27】「URL」を入力します。

「URL」は、［かんたん初期設定］の「機器の認証」画面に表示されています。

【28】［利用規約］をタップし、利用規約を確認します。

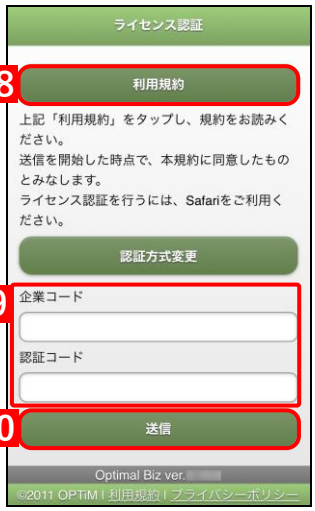
手順【30】で［送信］をタップすることにより、本規約に同意したものとみなします。

【29】「企業コード」、「認証コード」を入力します。

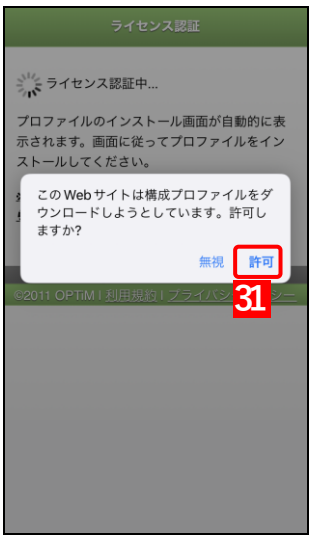
「企業コード」と「認証コード」は、［かんたん初期設定］の「機器の認証」画面に表示されています。

【30】［送信］をタップします。

⇒ライセンス認証が開始されます。



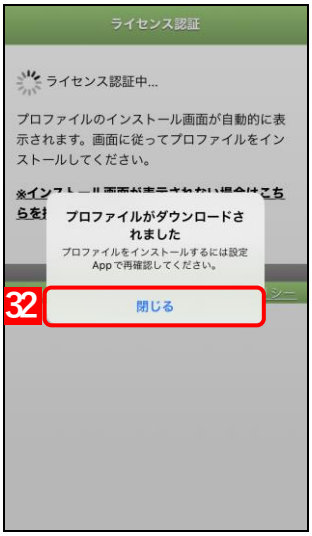
【31】［許可］をタップします。



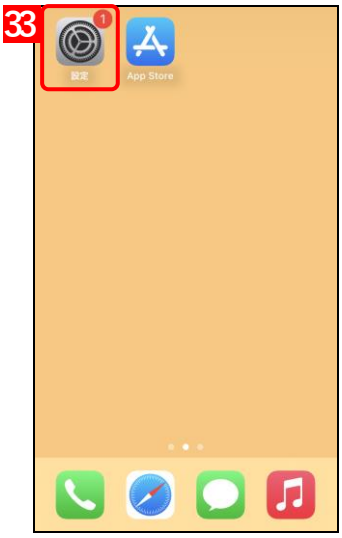
【32】［閉じる］をタップします。

⇒プロファイルのダウンロードが完了します。

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



【33】ホーム画面の［設定］をタップします。



【34】［ダウンロード済みのプロファイル］をタップします。

iOS のバージョンにより［ダウンロード済みのプロファイル］は、表記が異なる場合があります。

【35】［インストール］をタップします。

【36】［インストール］をタップします。

【37】［インストール］をタップします。

⇒インストールが開始され、リモート管理について確認を求められます。

【38】［信頼］をタップします。

⇒「インストール完了」画面に切り替わるまで、しばらくお待ちください。

【39】［完了］をタップします。

⇒ホーム画面に「パスコード要求」画面が表示されます。

【40】［今すぐ変更］をタップします。

【41】パスコードを入力します。

パスコードは、英数字を含む 8 文字以上で設定してください。

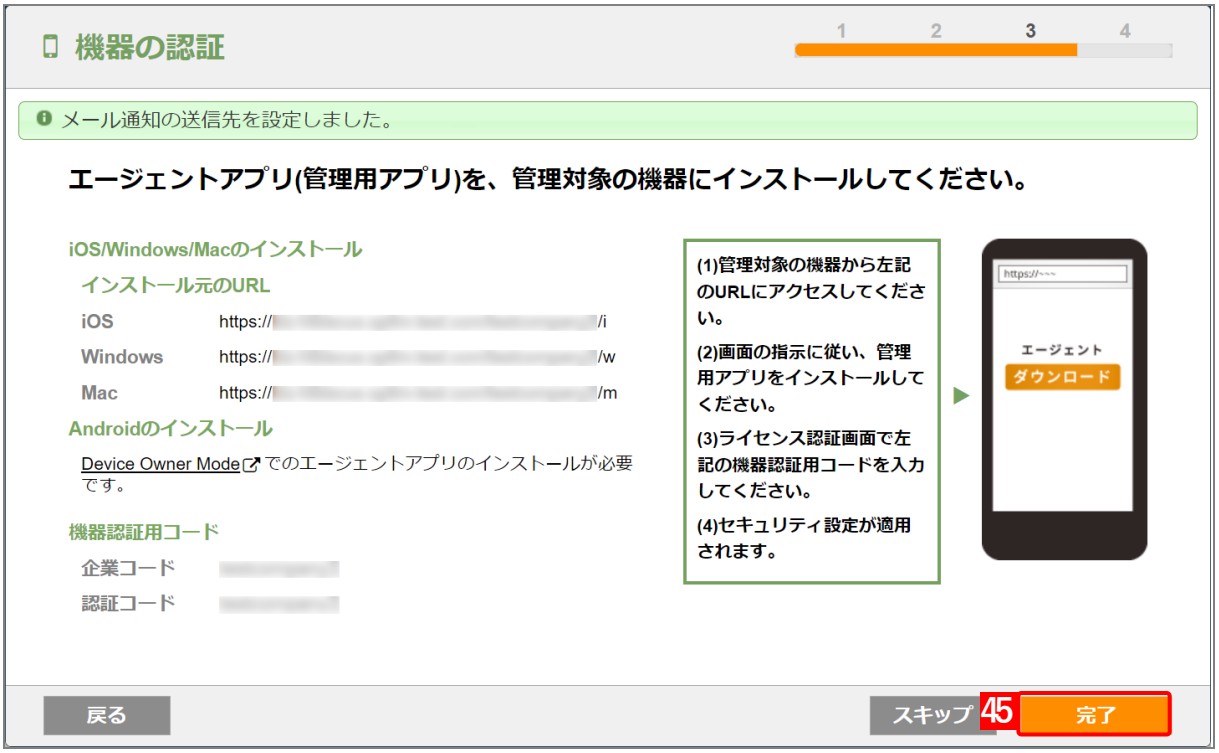
【42】［続ける］をタップします。

【43】手順【41】で入力したパスコードを、再度入力します。

【44】［パスコードを設定］をタップします。

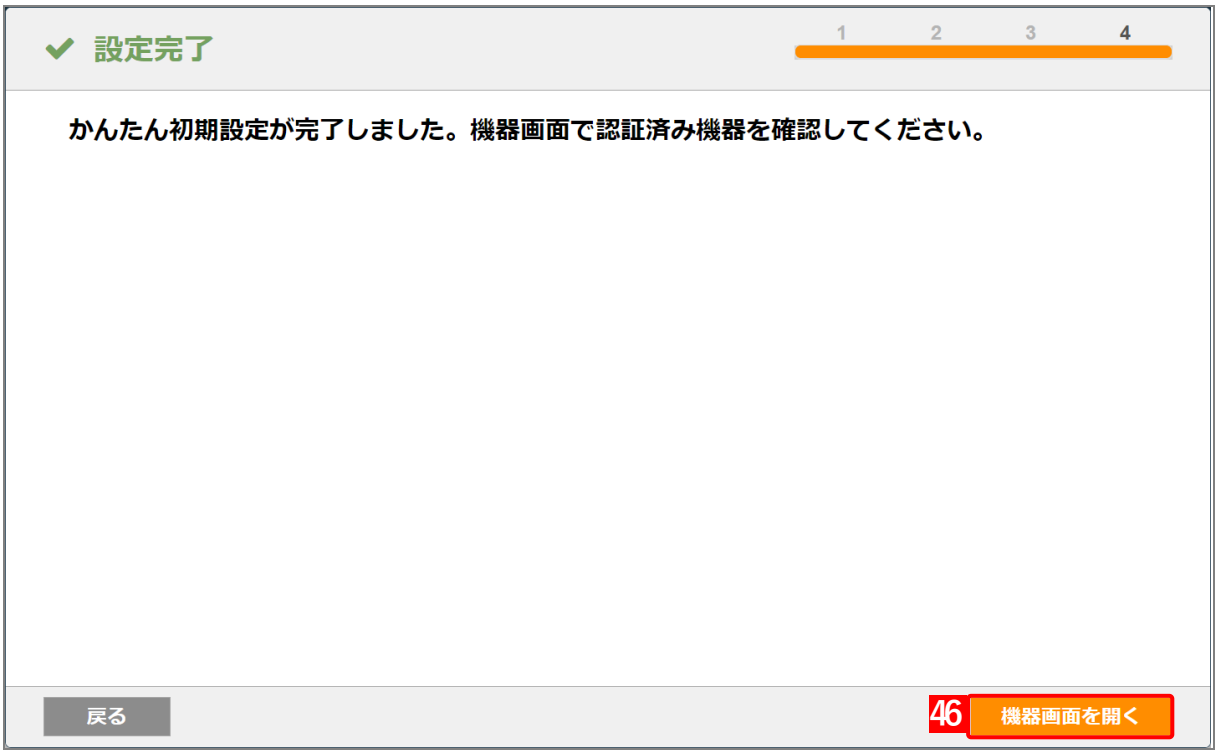
⇒［かんたん初期設定］の「機器の認証」画面に戻ります。

【45】［完了］をクリックします。



【46】［機器画面を開く］をクリックします。

⇒［機器］画面が表示されます。



1.3 ユーザーを登録する

管理サイトに登録した端末に紐づけるためのユーザーを登録します。

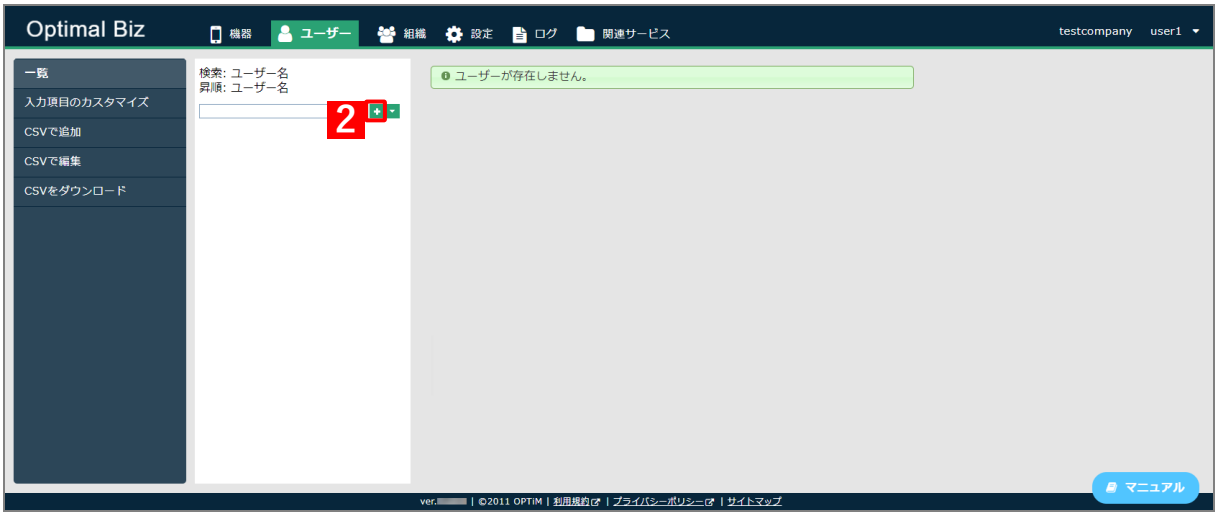
複数のユーザーを登録する場合は、CSV ファイルを利用して一括で登録することができます。詳細は、以下を参照してください。

「CSV ファイルの共通操作」51 ページ

【1】［ユーザー］をクリックします。

⇒［ユーザー］画面が表示されます。

【2】＋ をクリックします。



【3】「名前」を入力します。

【4】「ユーザー種別」を選択します。

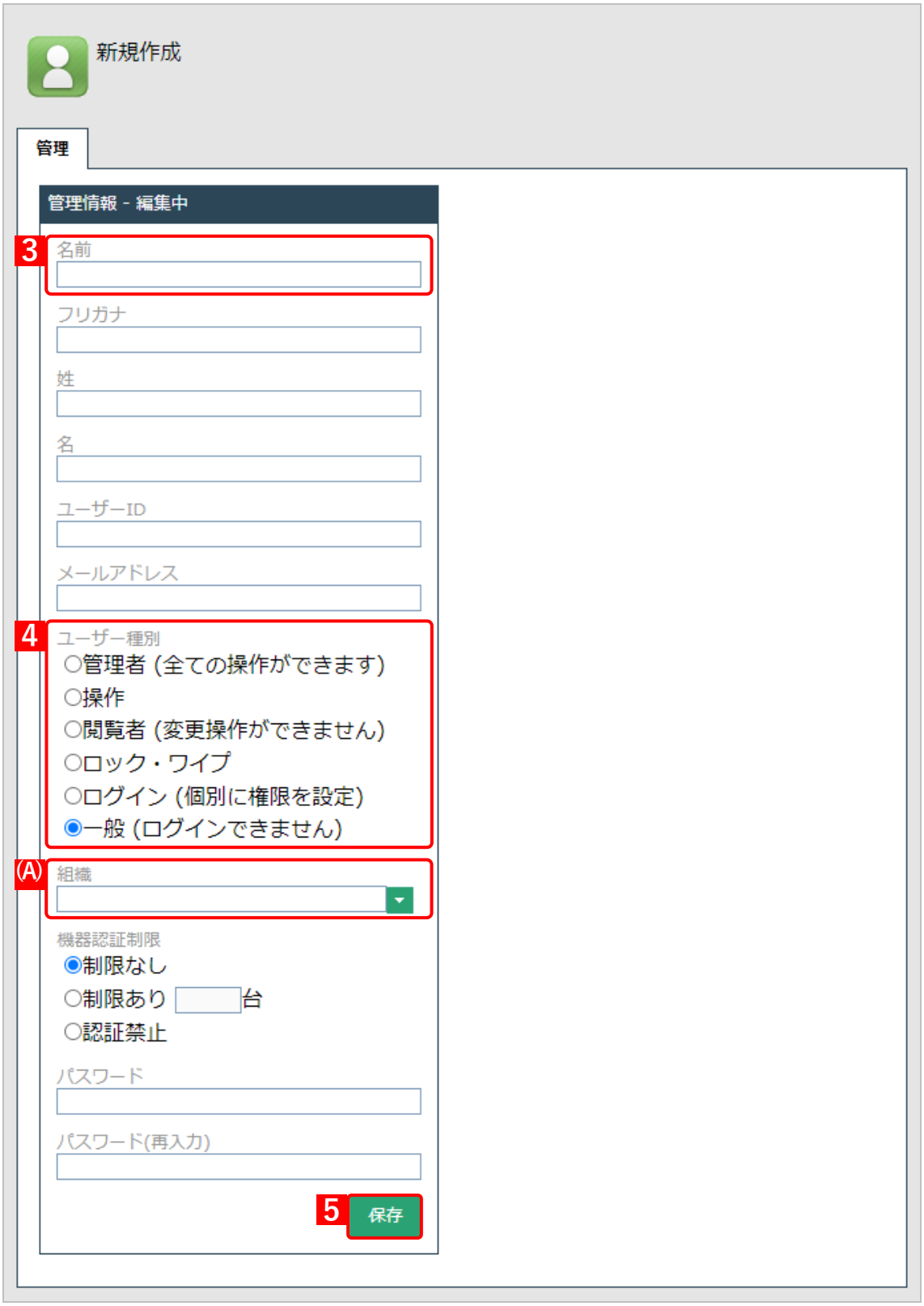
その他の項目の入力、選択は任意です。項目の詳細は以下を参照してください。

『管理サイト リファレンスマニュアル』の「ユーザー」－「一覧」－「[管理］タブ」

ユーザーに（A）組織を紐づけたい場合は、以下を参照して組織を作成してください。

「組織登録」49 ページ

【5】［保存］をクリックします



1.4 機器とユーザーを紐づける

管理サイトに登録した端末とユーザーを紐づけます。端末とユーザーを紐づけると端末の管理がしやすくなります。

Android Enterprise を利用する場合は、1 ユーザーに紐づけできる機器は 10 台までです。1 ユーザーに 11 台以上の機器を紐づけると、端末に配信した Google アカウントが無効になります。Google Play ストアの閲覧やアプリのインストールができなくなります。

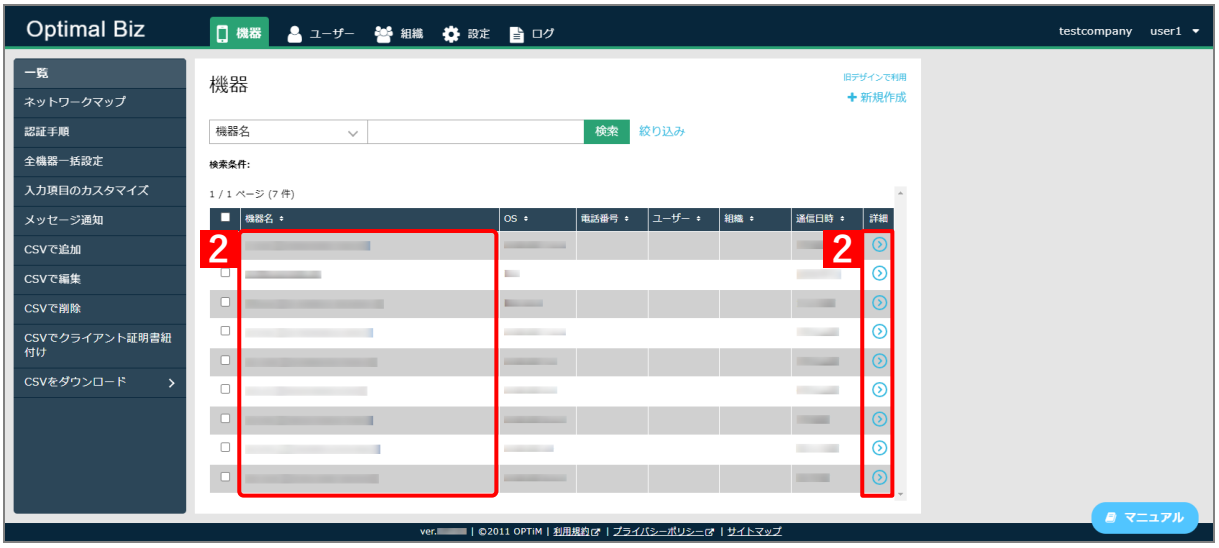
複数の機器に紐づける場合は、CSV ファイルを利用して一括で紐づけることができます。詳細は、以下を参照してください。

「CSV ファイルの共通操作」51 ページ

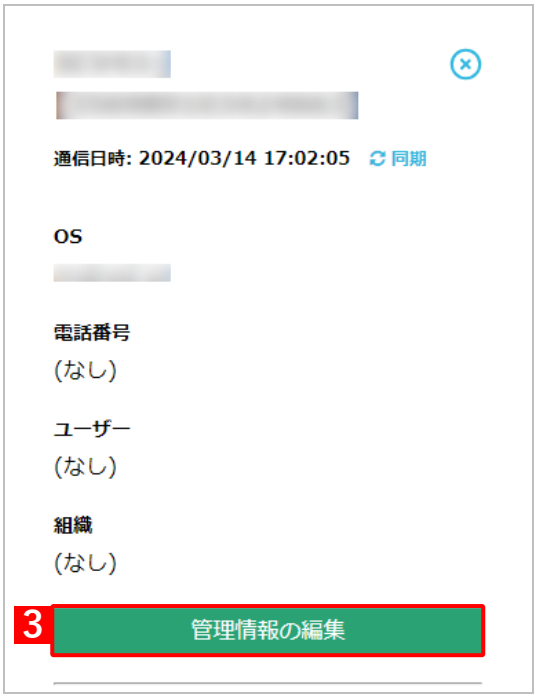
【1】［機器］をクリックします。

⇒機器画面が表示されます。

【2】対象の機器名または「詳細」の ⓘ をクリックします。



【3】［機器情報の編集］をクリックします。



【4】ユーザーの▼をクリックして、表示されるユーザーを選択します。

機器と（A）組織を紐づけたい場合は、以下を参照して、組織を作成してください。

「組織登録」49 ページ

【5】［保存］をクリックします。

2 補足・便利な操作

「端末の管理を開始する」の設定にかかわる補足、知っていると便利な操作などを説明します。

2.1 ログイン／ログアウト

パスワードの発行や更新、2 段階認証でのログイン、ログアウトの手順について説明します。

管理サイトの URL、企業コード、ユーザーID またはメールアドレス、パスワードは、事前に確認してください。

2.1.1 パスワードを新規発行／再発行する

管理サイトにログインするパスワードを変更したい場合や、パスワードを忘れてしまった場合は、パスワードを発行、再発行します。

管理サイトで「パスワードリマインダー」が［無効］に設定されている場合は、パスワードの発行はできません。

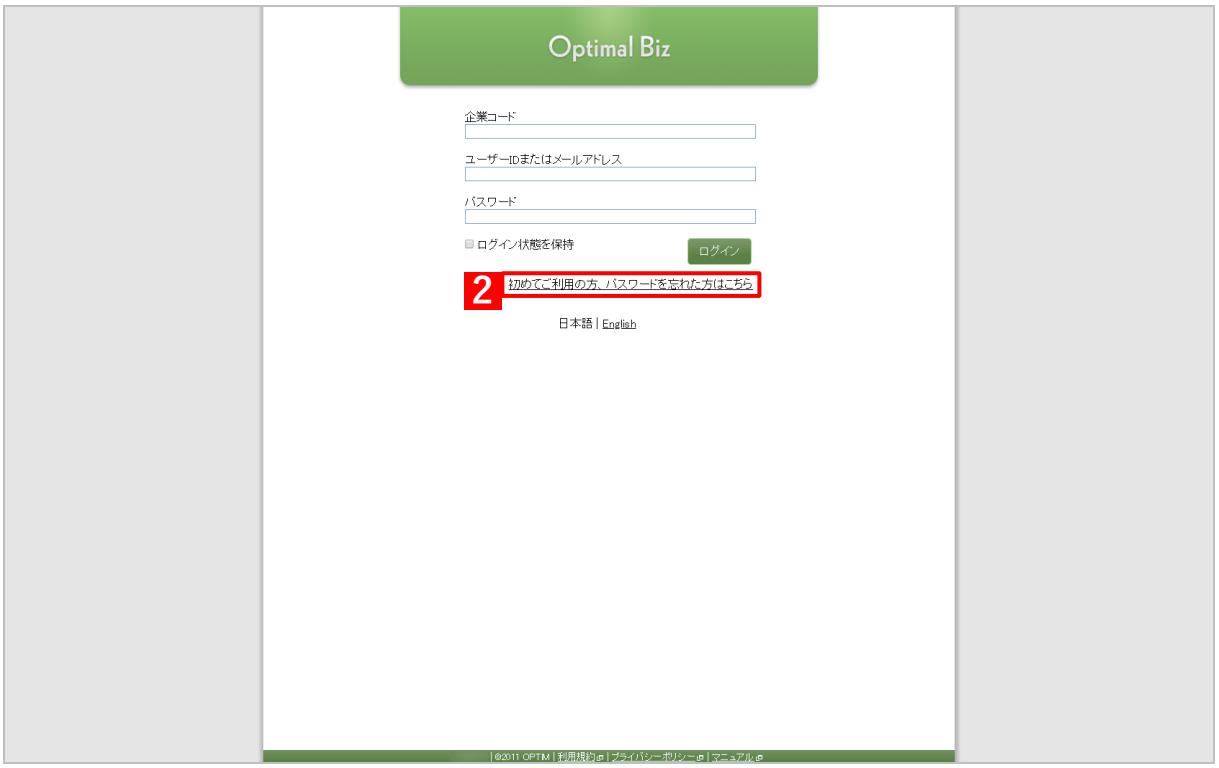
『管理サイト リファレンスマニュアル』の「サービス環境設定」－「アカウントポリシー」

【1】ブラウザーに管理サイトの URL を入力してログイン画面を表示します。

【2】［初めてご利用の方、パスワードを忘れた方はこちら］をクリックします。

⇒「メール送信」画面が表示されます。

企業コードを取得する前のログイン画面は、「パスワードリマインダー」の設定にかかわらず［初めてご利用の方、パスワードを忘れた方はこちら］は表示されます。



【3】「企業コード」と「メールアドレス」を入力します。

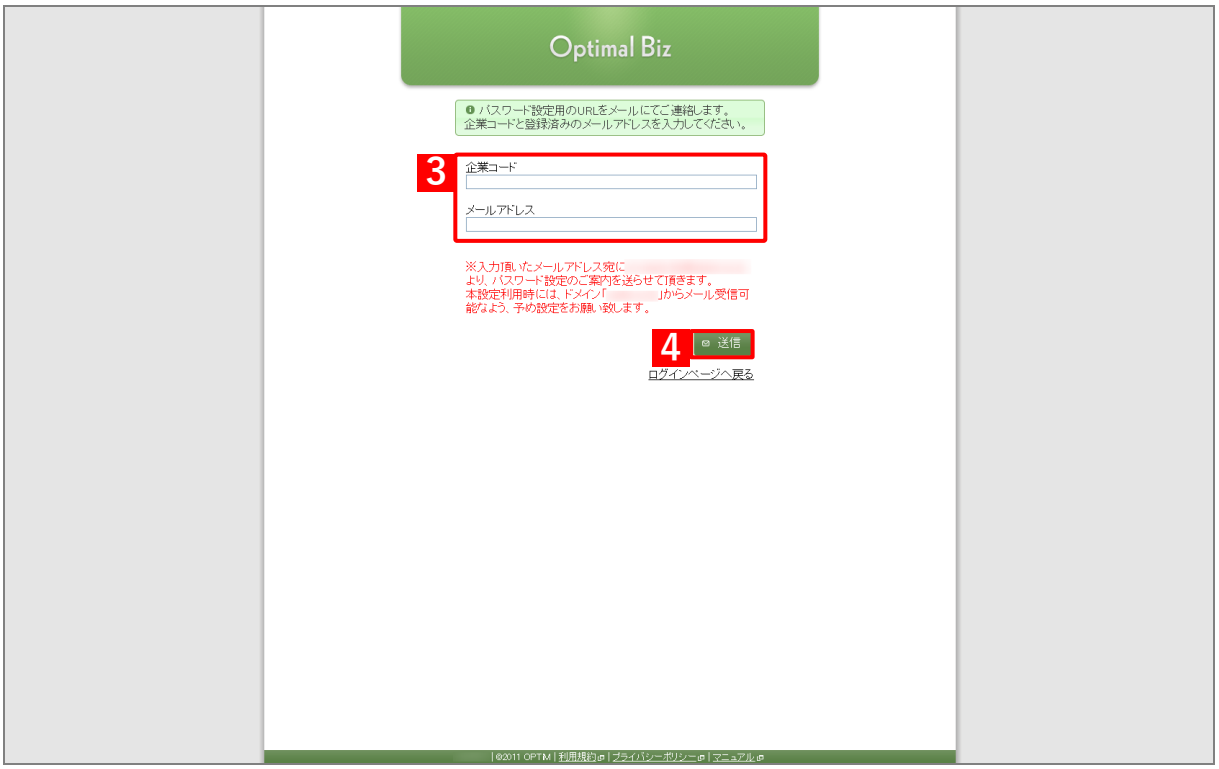
「企業コード」は、すでに入力済みの場合があります。

【4】［送信］をクリックします。

⇒指定したメールアドレスに、パスワード設定の案内メールが送信されます。

メールが届かない場合は、企業コードとメールアドレスを確認のうえ、本製品の購入元に問い合わせてください。

使用しているメールアプリに迷惑メールフィルターなどが設定されている場合、メールが正しく受信できない場合があります。メールが届かない場合、メール設定を確認してください。

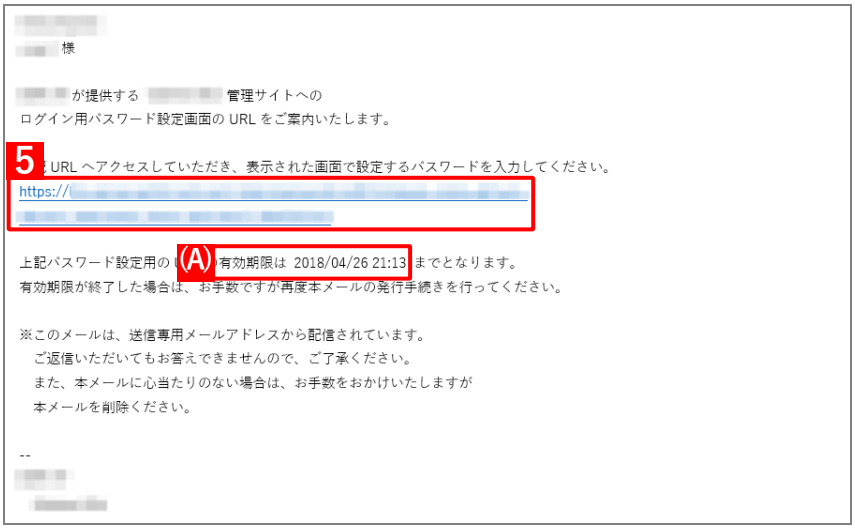


【5】受信したメールの内容を確認し、URL をクリックします。

⇒パスワード再設定画面が表示されます。

(A)「有効期限」に表示されている期間が過ぎると、パスワードの発行、再発行ができなくなります。パスワードの設定、再設定は有効期限内に行ってください。

メールの件名、本文、送信元メールアドレスは、サービス企業の設定により異なります。

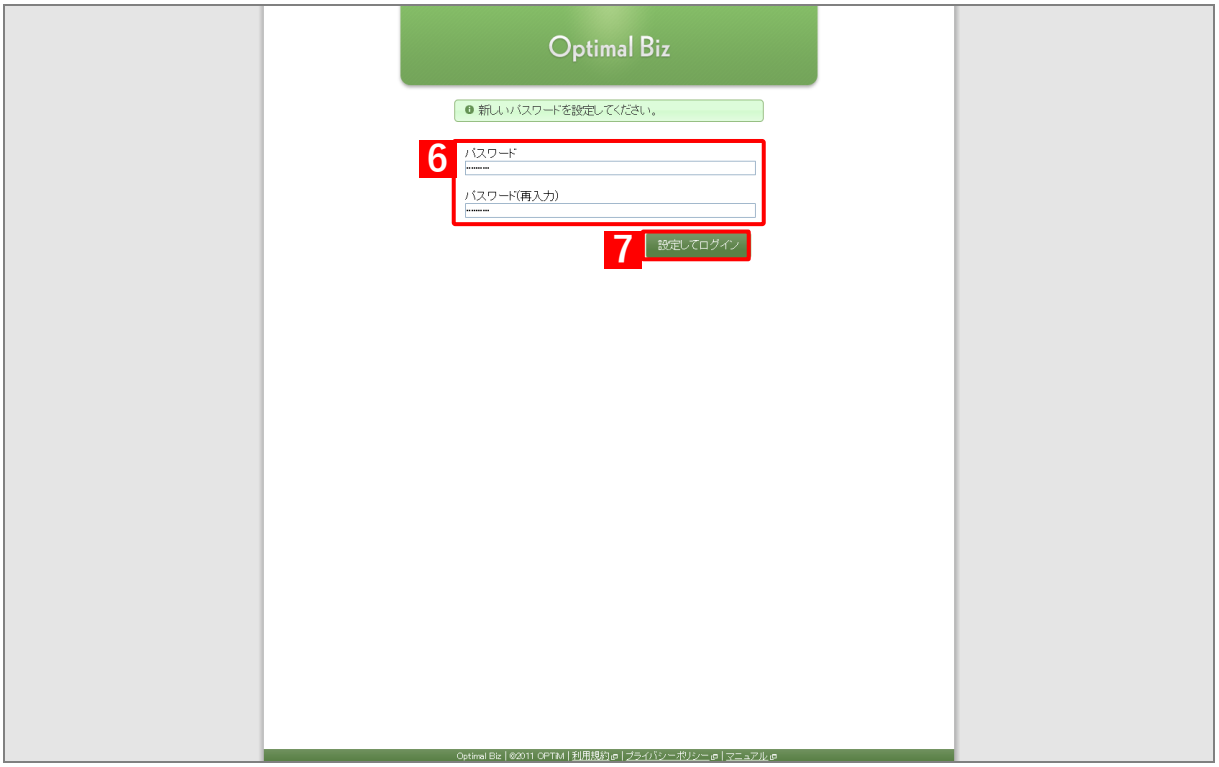


【6】「パスワード」、「パスワード(再入力)」に新しいパスワードを入力します。

設定したパスワードは忘れないように管理してください。

【7】［設定してログイン］をクリックします。

⇒管理サイトのダッシュボードが表示されます。

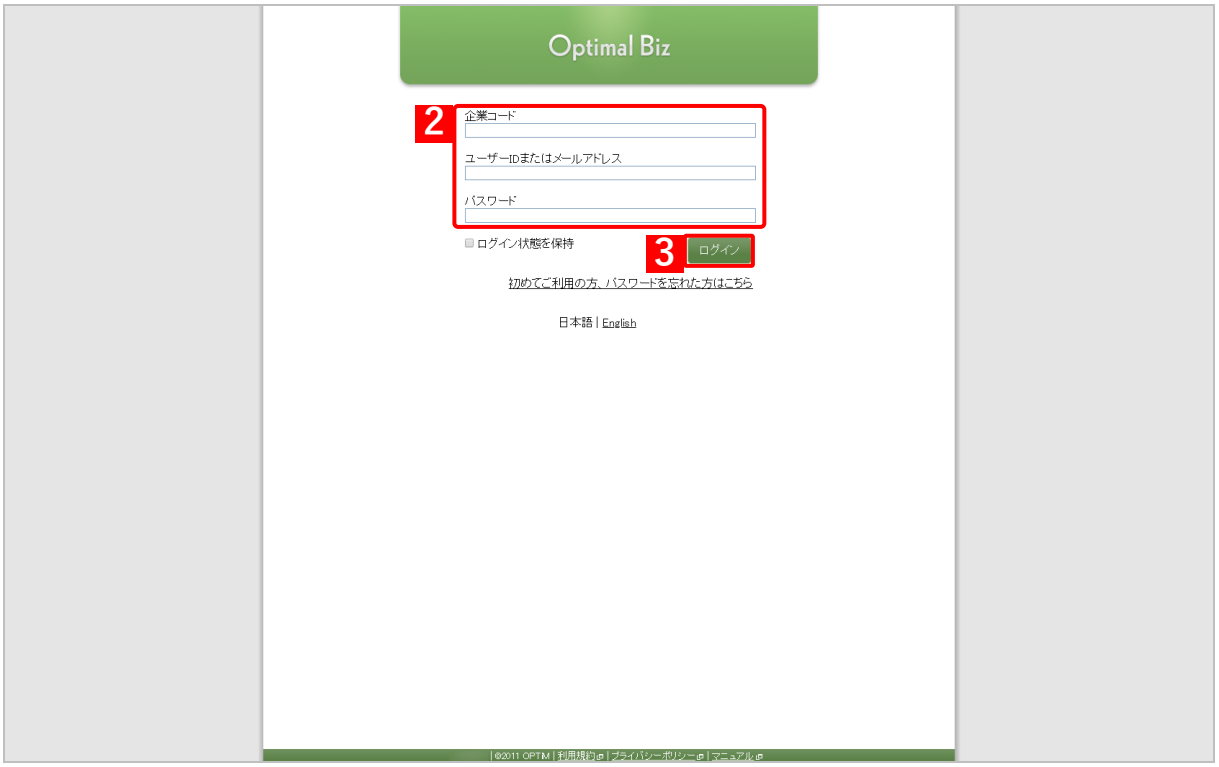


2.1.2 期限切れパスワードを更新する

管理サイトの［アカウントポリシー］の設定で「パスワードの有効期間」を設定している場合は、有効期間が過ぎると管理サイトにログインできなくなります。その場合は、新しいパスワードを設定して管理サイトにログインします。

『管理サイト リファレンスマニュアル』の「サービス環境設定」－「アカウントポリシー」

【1】ブラウザーに管理サイトの URL を入力してログイン画面を表示します。
【2】「企業コード」、「ユーザーID またはメールアドレス」、「パスワード」を入力します。
【3】［ログイン］をクリックします。
⇒パスワード更新画面が表示されます。



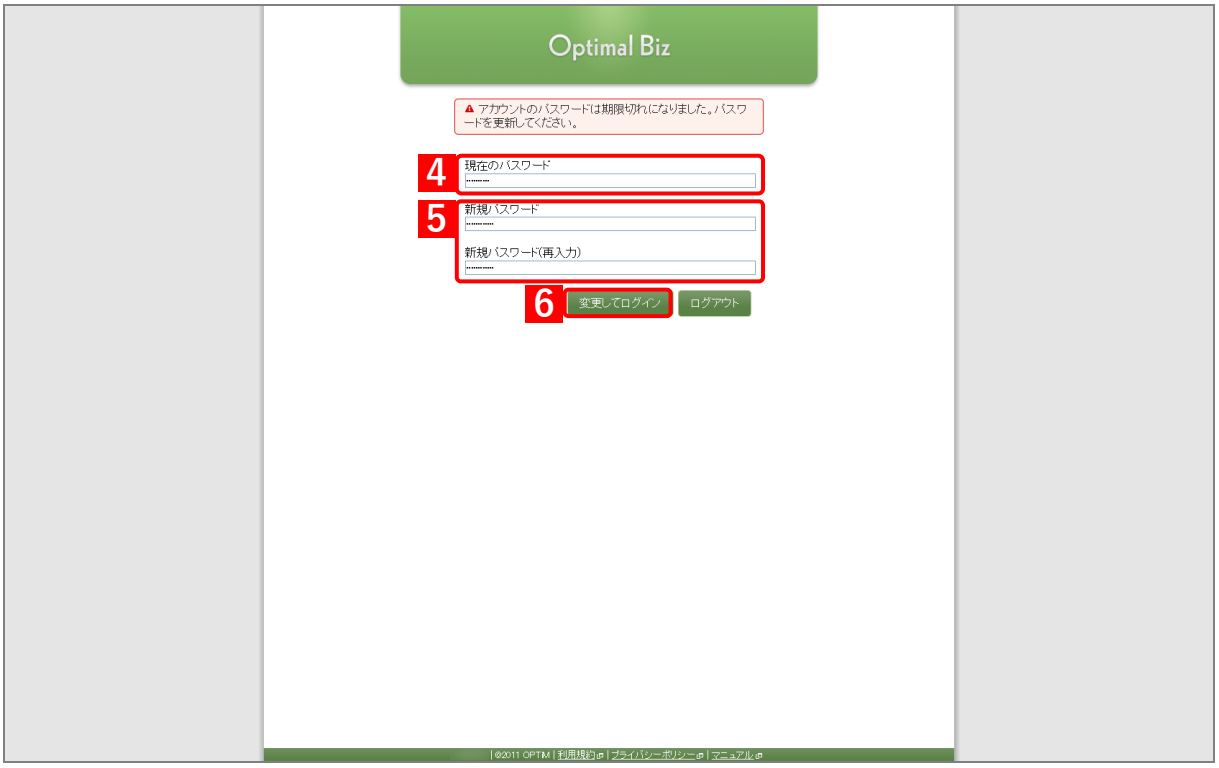
【4】「現在のパスワード」を入力します。

【5】「新規パスワード」と「新規パスワード(再入力)」を入力します。

入力した新規パスワードは忘れないように管理してください。

【6】［変更してログイン］をクリックします。

⇒管理サイトのダッシュボードが表示されます。



2.1.3 2 段階認証で管理サイトにログインする

管理サイトの［アカウントポリシー］の設定で「2 段階認証」を［有効］に設定している場合は、管理サイトにログインするときに認証が 2 回必要になります。

『管理サイト リファレンスマニュアル』の「サービス環境設定」－「アカウントポリシー」

ここでは、はじめて 2 段階認証で管理サイトにログインする手順と 2 回目以降にログインする手順について説明します。

「2 段階認証を設定してログインする(初回のみ)」44 ページ

「2 段階認証でログインする」47 ページ

2 段階認証を行うには、Android 端末または iOS 端末に以下のアプリを Google Play ストアや App Store などからインストールしてください。

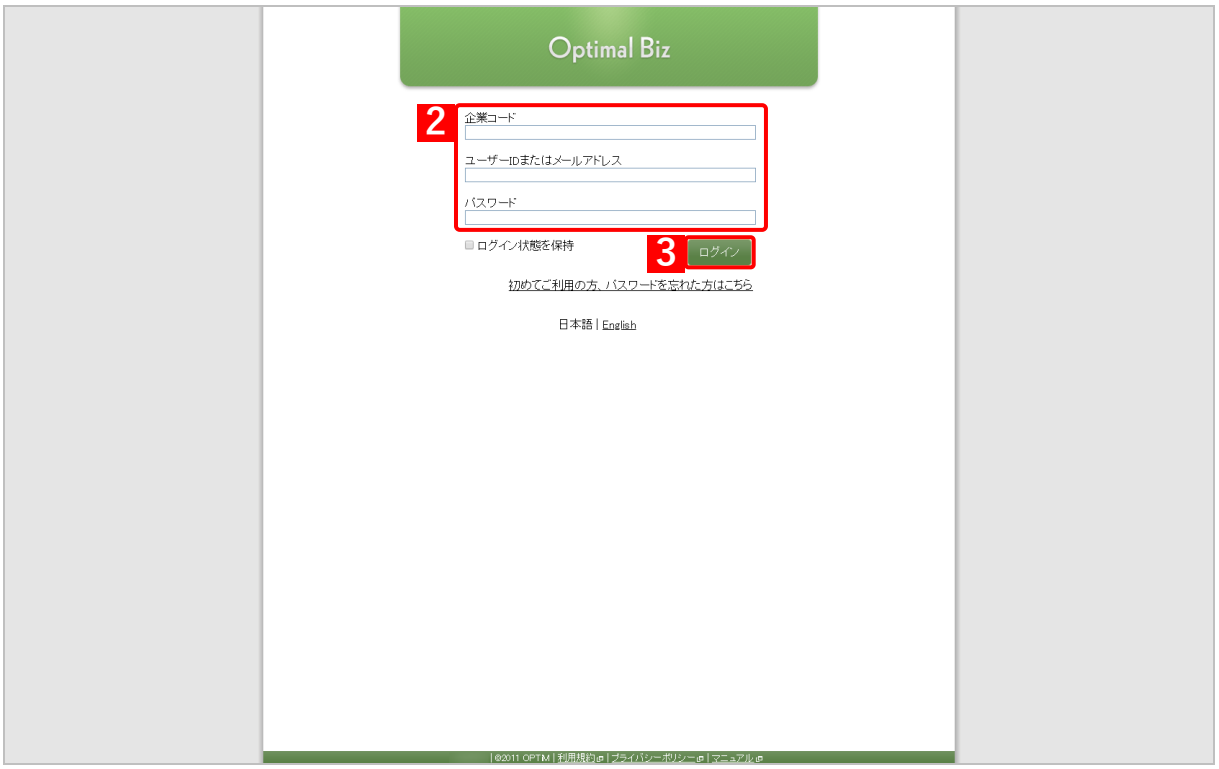
- Google Authenticator
- Microsoft Authenticator

本マニュアルでは、iOS 端末に Microsoft Authenticator をインストールした画面で説明します。端末、アプリによって操作手順、表示画面が異なります。詳細はアプリの提供元に問い合わせてください。

2.1.3.1 2 段階認証を設定してログインする(初回のみ)

管理サイトの［アカウントポリシー］の設定で「2 段階認証」を［有効］に設定し、はじめて管理サイトにログインするときは、2 段階認証の設定を行います。

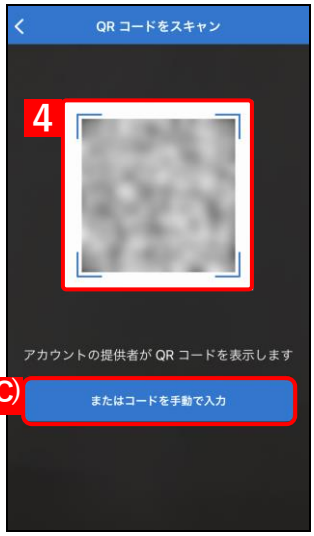
【1】ブラウザーに管理サイトの URL を入力してログイン画面を表示します。
【2】「企業コード」、「ユーザーID またはメールアドレス」、「パスワード」を入力します。
【3】［ログイン］をクリックします。
⇒「2 段階認証の設定」画面が表示されます。



【4】端末にインストールしたアプリで、QR コードのスキャン画面を表示し、（A）QR コードを読み取ります。

⇒端末に 6 桁の数字が表示されます。

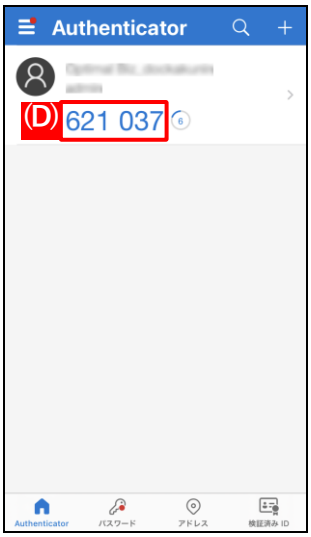
QR コードが読み取れなかった場合、(C)［またはコードを手動入力］をタップしてアカウント入力画面を表示し、(B) アカウントキーを入力してください。入力項目名などはアプリによって異なります。詳細はアプリの提供元に問い合わせてください。



【5】端末に表示された（D）6 桁の数字を「セキュリティコード」に入力します。

【6】［認証する］をクリックします。

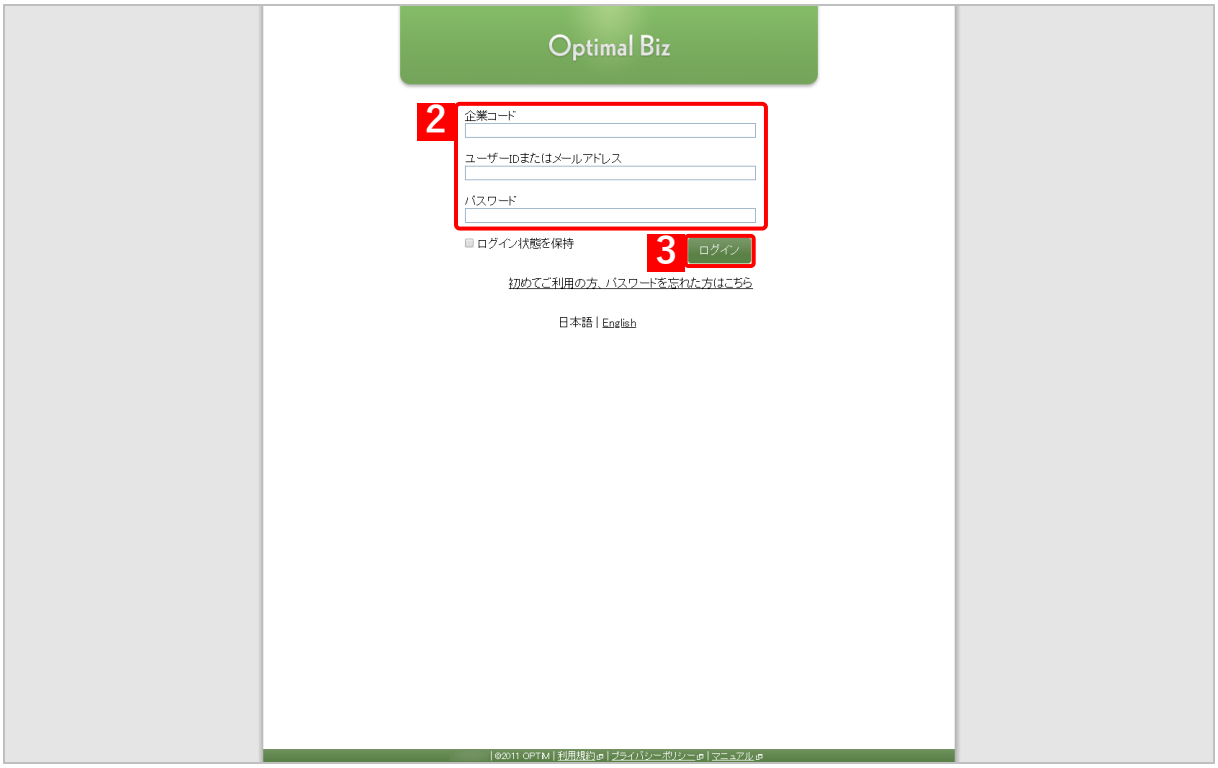
⇒管理サイトのダッシュボードが表示されます。



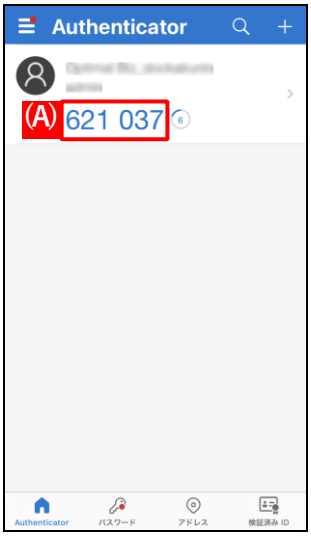
2.1.3.2 2 段階認証でログインする

2 回目以降に 2 段階認証でログインする場合は、通常のログイン手順のあとに、端末に表示される数字を「2 段階認証」画面で入力します。

【1】ブラウザーに管理サイトの URL を入力してログイン画面を表示します。
【2】「企業コード」、「ユーザーID またはメールアドレス」、「パスワード」を入力します。
【3】［ログイン］をクリックします。
⇒「2 段階認証」画面が表示されます。

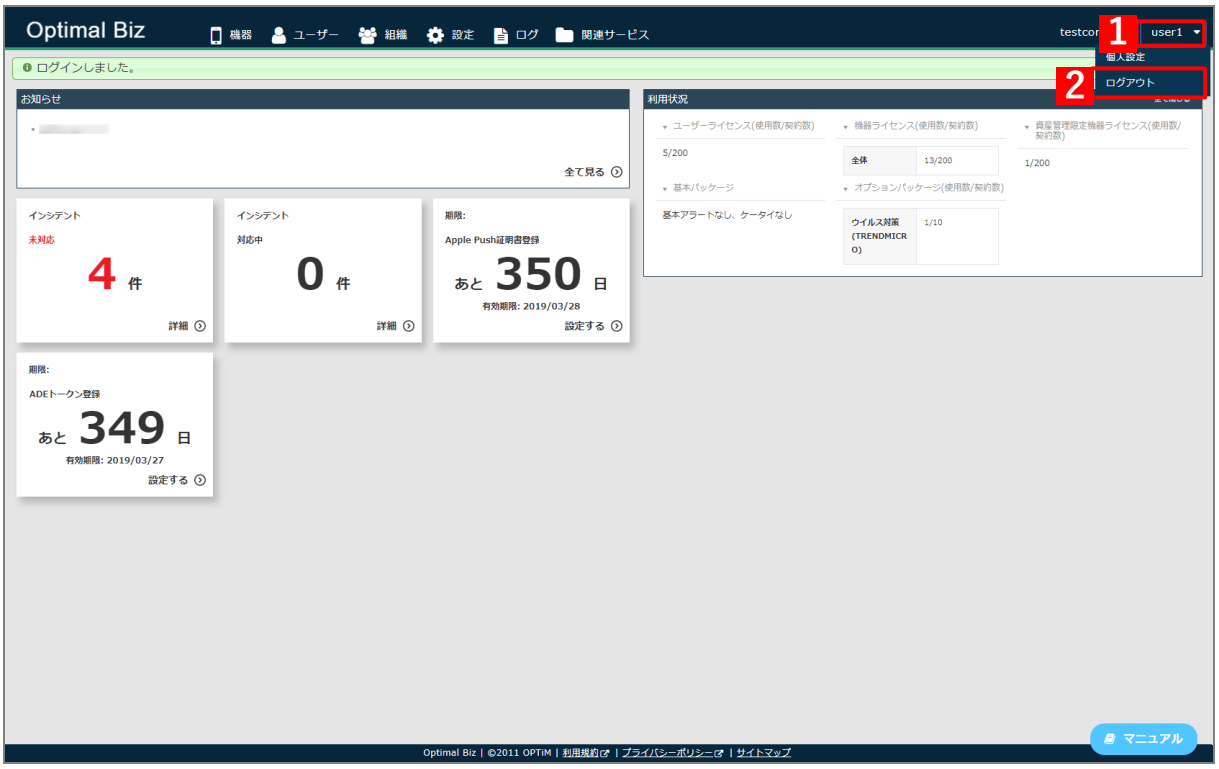


【4】端末にインストールしたアプリに表示されている（A）6 桁の数字を「セキュリティコード」に入力します。
【5】［認証する］をクリックします。
⇒管理サイトのダッシュボードが表示されます。

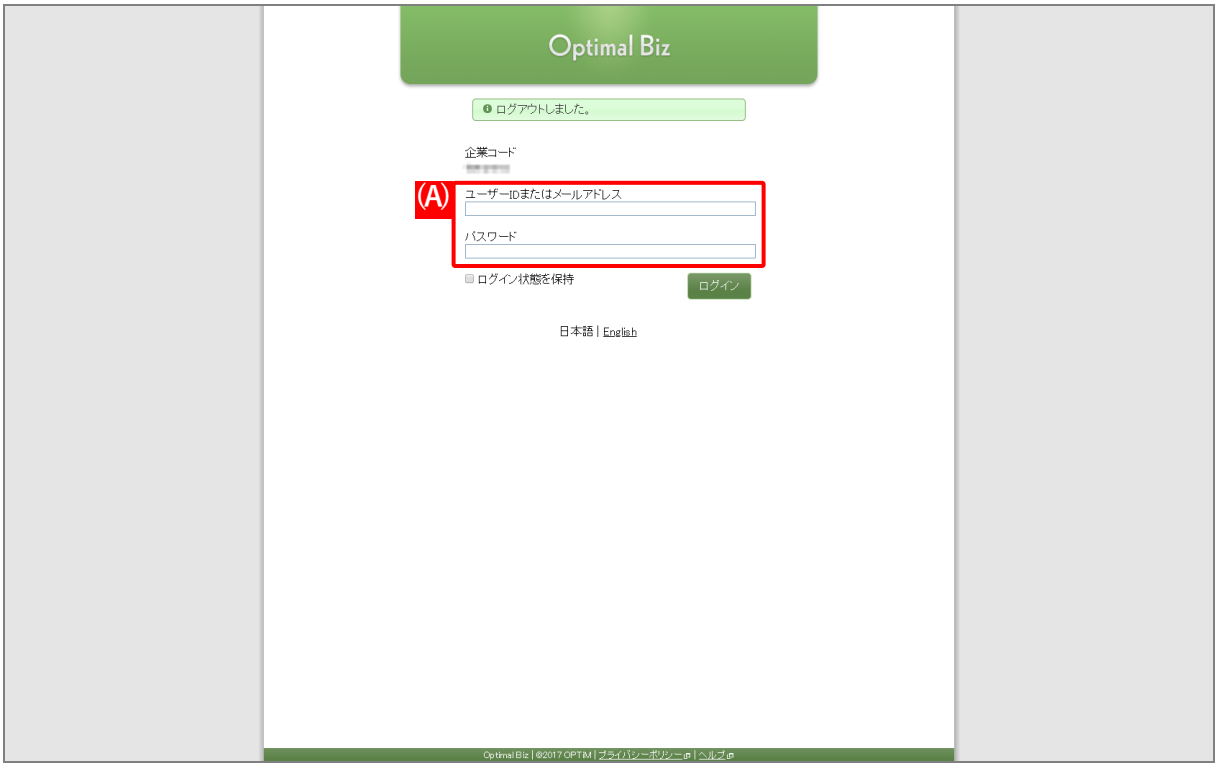


2.1.4 管理サイトからログアウトする

【1】ログイン情報の［ユーザー名］をクリックします。
【2】［ログアウト］をクリックします。



⇒ログイン画面が表示されます。
　ログアウトしたあとは、(A) ユーザーID またはメールアドレス、パスワードでログインできます。



2.2 組織登録

登録した端末やユーザーを紐づけるための「組織」を登録することができます。

「組織」を登録すると、ユーザーと同様に端末を直接紐づけすることもできますが、端末を紐づけしたユーザーを紐づけすることもできるため、より高度な管理をすることができます。

ここでは、新規に組織を登録する手順について説明します。

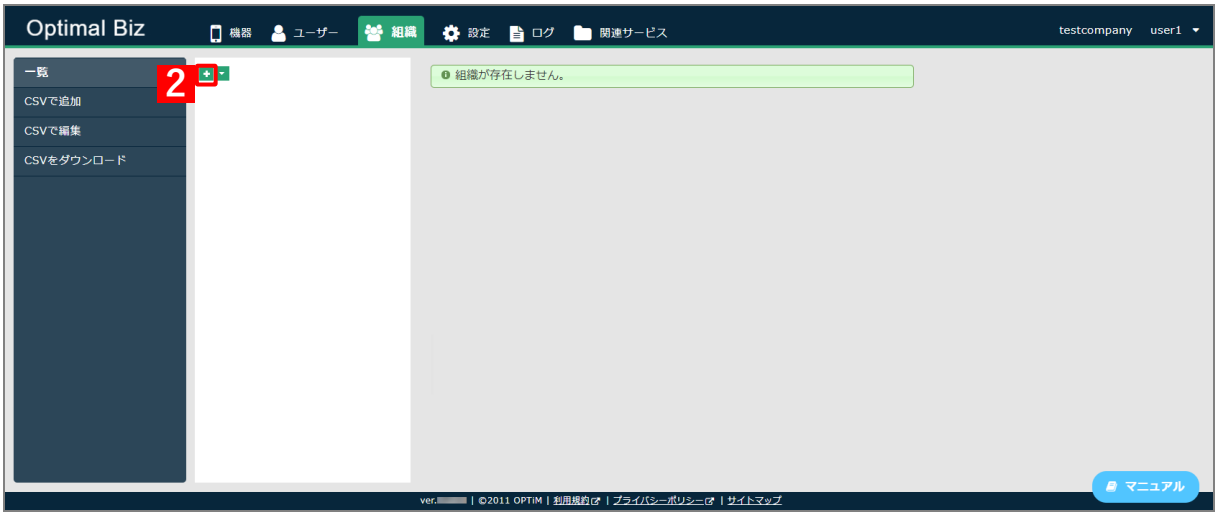
複数の組織を登録する場合は、CSV ファイルを利用して一括で登録することができます。詳細は、以下を参照してください。

「CSV ファイルの共通操作」51 ページ

【1】［組織］をクリックします。

⇒組織画面が表示されます。

【2】＋ をクリックします。

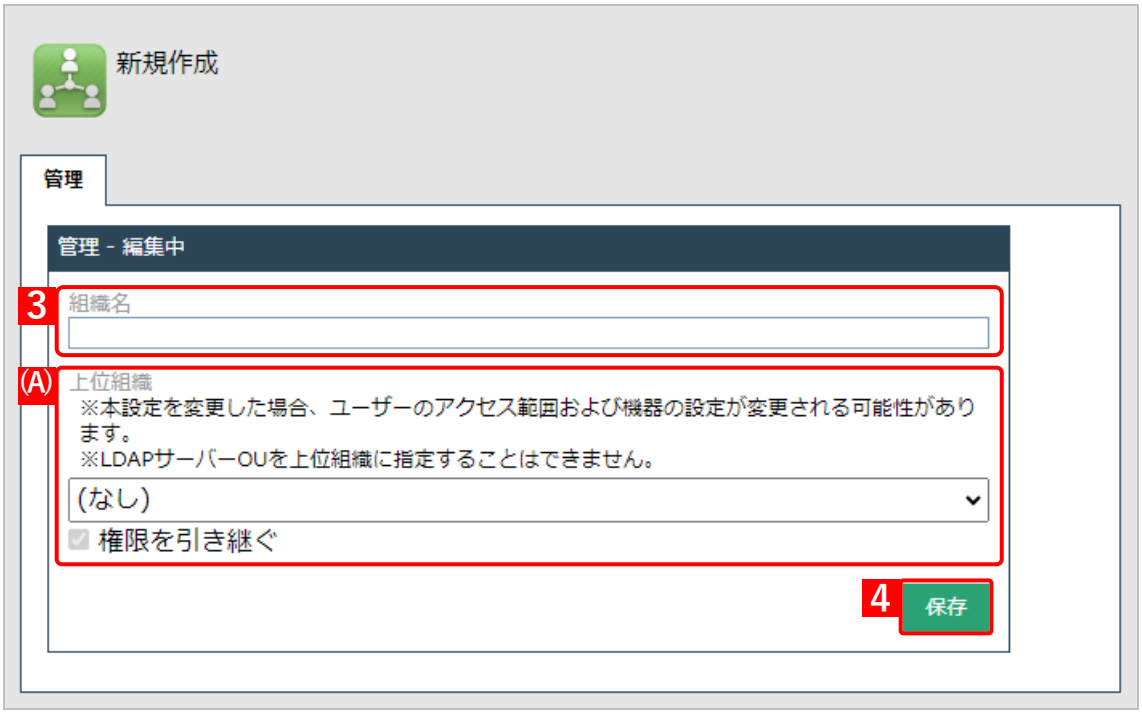


【3】「組織名」を入力します。

（A）上位組織がある場合は、設定してください。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「組織」－「一覧」－「[管理］タブ」

【4】［保存］をクリックします



2.3 CSV ファイルの共通操作

CSV ファイルを利用して、複数の情報を一括で管理サイトに登録できます。

CSV ファイルを利用できる機能は、以下を参照してください。

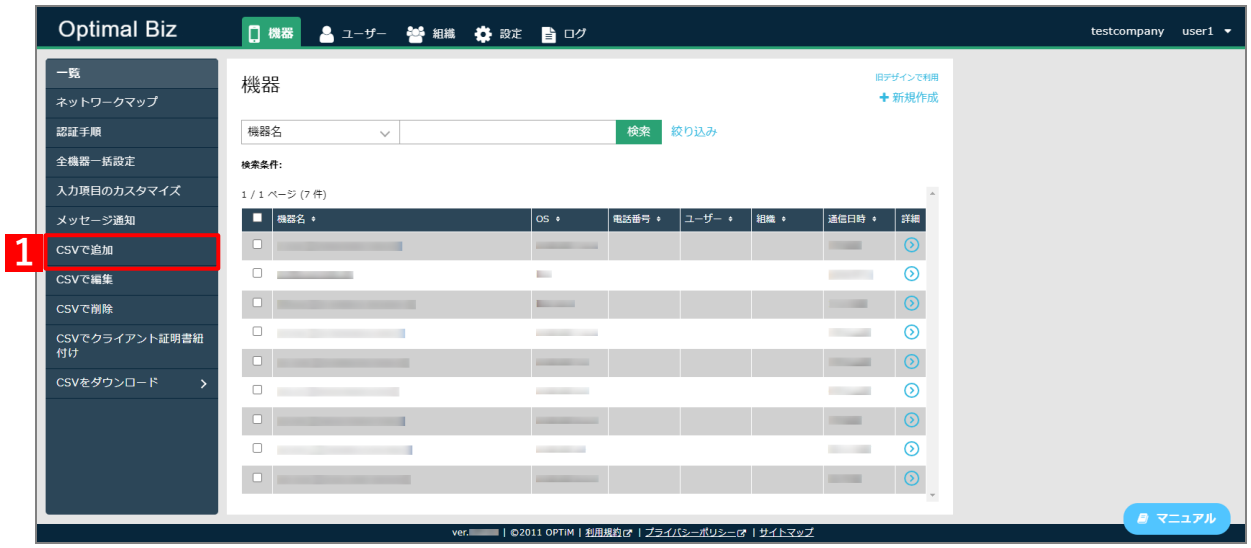
「CSV ファイルをインポートできる機能」53 ページ

2.3.1 CSV ファイルをアップロードする

ダウンロードした CSV ファイルを編集し、アップロードします。

ここでは、［機器］の［CSV で追加］を例にしています。

【1】［機器］→［CSV で追加］をクリックします。



【2】［ダウンロード］をクリックします。

⇒CSV ファイルがダウンロードされます。

CSV ファイルの構造は、以下を参照してください。

「インポート用の CSV ファイルの構造」53 ページ

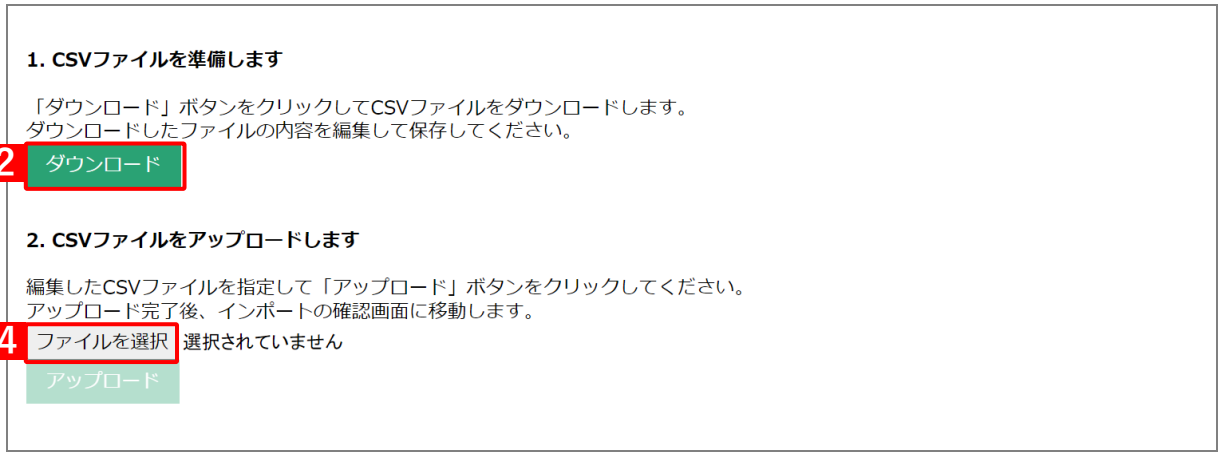
【3】手順【2】でダウンロードした CSV ファイルを編集して、インポート用の CSV ファイルを作成します。

CSV ファイルは、Excel やメモ帳などで編集してください。

アスタリスク「*」だけで構成された文字列は使用しないでください。

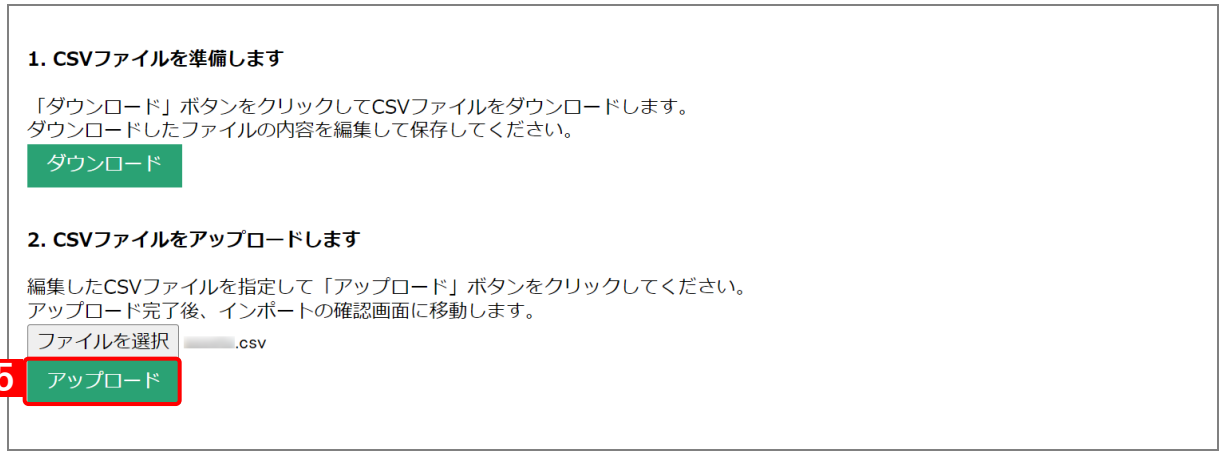
【4】［ファイルを選択］をクリックし、手順【3】で作成した CSV ファイルを選択します。

アップロードできる CSV ファイルのファイルサイズは 10MB までです。



【5】［アップロード］をクリックします。

⇒インポート用の CSV ファイルがアップロードされます。アップロードが完了すると、インポート画面が表示されます。



【6】手順【5】でアップロードした CSV ファイルの内容が一覧で表示されます。内容を確認します。

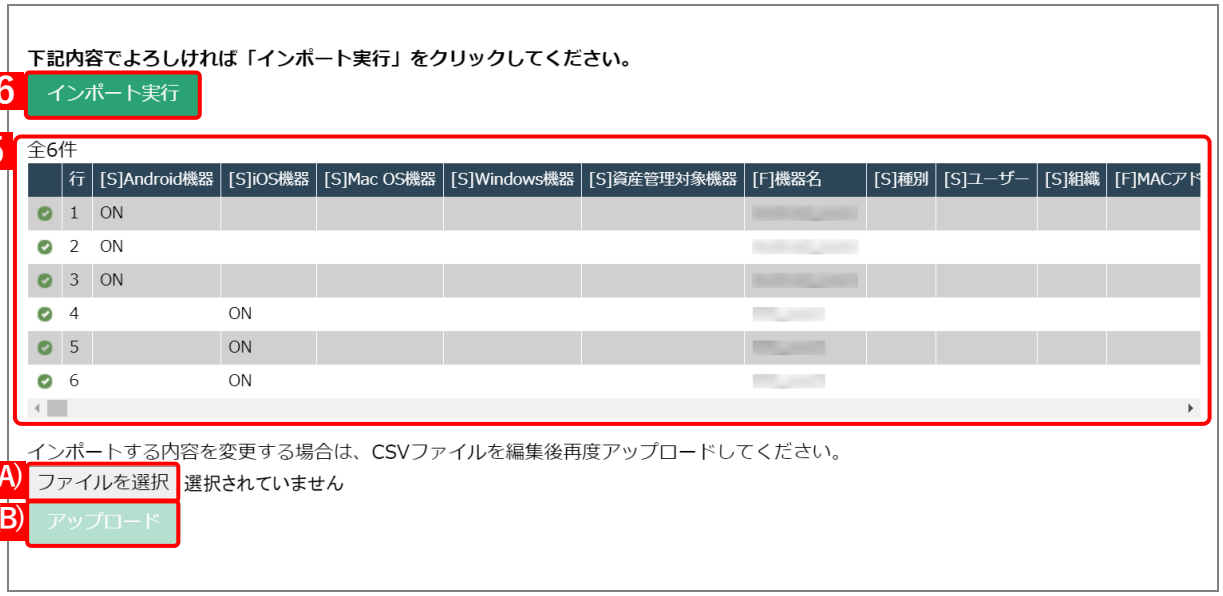
内容に誤りがある場合は、一覧の最終列「備考」にエラー内容が表示されます。

内容を変更する場合は、インポート用の CSV ファイルを再編集し、(A)［ファイルを選択］をクリックして CSV ファイルを選択して、(B)［アップロード］をクリックしてください

【7】［インポート実行］をクリックします。

⇒インポートが開始されます。インポートが完了すると「インポートに成功しました。」とメッセージが表示され、インポート結果が表示されます。

CSV ファイルでインポートした情報は、次回の同期時に端末に反映されます。



2.3.2 インポート用の CSV ファイルの構造

形式	●CSV ファイルは、改行コードで区切った複数のレコードで構成されています。 ●各レコードは、カンマ（%x2C）で区切った複数のフィールドで構成されています。 フィールドの値に以下の制御文字が含まれる場合は、フィールドの値全体をダブルクオートで囲むことで、エスケープすることができます。 ・ダブルクオート（%x22） ・カンマ（%x2C） ・CR（%x0D） ・LF（%x0A） インポートできる CSV ファイルのフォーマットは、カンマ（,）で定義されています。 ・エスケープされたフィールドを含まない場合 GUID,[F]名前,[F]フリガナ,[F]ユーザーID,[F]メールアドレス,[F]パスワード,[M]ロール user1,ユーザー1,ユーザー1,user1,user1@example,********,ロール 1 user2,ユーザー2,ユーザー2,user2,user2@example,********,ロール 2 ・エスケープされたフィールドを含む場合 GUID,[F]名前,[F]フリガナ,[F]ユーザーID,[F]メールアドレス,[F]パスワード,[M]ロール user1,ユーザー1,ユーザー1,user1,user1@example,********,"ロール 1,ロール 2" user2,ユーザー2,ユーザー2,user2,user2@example,********,"ロール 1,ロール 2"
文字コード	●日本語環境 Shift_JIS (CP932) ●日本語以外の環境 UTF-8 Shift_JIS で表示できない文字は「?」に置き換えられて登録されますので、注意してください。
改行コード	CR+LF（インポート時、エクスポート時）

2.3.3 CSV ファイルをインポートできる機能

機能の詳細は、以下を参照してください。

『管理サイト リファレンスマニュアル』

タブ		メニュー		
機器		CSV で追加		
		CSV で編集		
		CSV で削除		
		CSV でクライアント証明書紐付け（iOS のみ）		
ユーザー		CSV で追加		
		CSV で編集		
組織		CSV で追加		
		CSV で編集		
設定	Android	セキュリティ	機能制限	発信先制限
		アプリケーション	アプリケーション禁止	
		便利機能	連絡先	
		証明書管理	クライアント証明書一括削除	
		Device Owner Mode	アプリケーション非表示	
	iOS	証明書管理	クライアント証明書一括削除	
	Windows	証明書管理	クライアント証明書一括削除	

2.4 管理方式

OS を管理する方式としてエージェントや MDM 構成プロファイルなどがあり、OS によって使用する方式が異なります。OS ごとの管理方式は以下になります。

OS	管理方式	参照ページ
Android Windows	エージェント	54
Android（専用デバイス）	Android Device Policy	54
iOS Mac OS	MDM 構成プロファイル	54
	構成プロファイル	54
	エージェント（任意）	54

各 OS の詳細、使用方法などは、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』
- 『Android（AMAPI）クライアント リファレンスマニュアル』
- 『iOS クライアント リファレンスマニュアル』
- 『Mac OS クライアント リファレンスマニュアル』
- 『Windows クライアント リファレンスマニュアル』

2.4.1 エージェントとは

Android 端末、Windows 端末（iOS 端末、Mac OS 端末は任意）を本製品で管理するために、端末にインストールする本製品のアプリです。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です。

2.4.2 Android Device Policy とは

Android（専用デバイス）を本製品で管理するために、管理対象の機器へ自動でインストールされる Google 製のエージェントです。

他 OS のエージェントと異なり、本製品と直接通信を行わず、Google を介して情報の更新や機器の制御・設定を行います。

また、認証はキッティング時に同時に行われるため、別途認証作業を行う必要はありません。

このアプリはアンインストールができないため、本製品との認証が解除された場合は、端末がワイプ（初期化）されます。

2.4.3 MDM 構成プロファイルとは

MDM に関する各種の設定が記述された XML 形式のファイルです。

iOS 端末と Mac OS 端末を本製品で管理するために、端末にインストールします。

2.4.4 構成プロファイルとは

管理サイトや、Apple が提供している Apple Configurator で作成できるプロファイルです。iOS 端末、Mac OS 端末に対する制御や設定ができます。

2.5 同期

同期とは、管理サイトと端末で通信を取ることです。通信を取ることで端末情報の収集や、端末に設定を送ることができます。

2.5.1 同期の仕組み

管理サイトと端末の同期を行うには、以下のサーバーを経由します。

ここでは、どのような仕組みで管理サーバーと各 OS の同期用サーバー、端末間でやり取りが行われるかを OS ごとに図示して説明します。

OS	同期用サーバー	参照ページ
Android Windows	プッシュ配信サーバー（独自 Push 方式）	55
Android（専用デバイス）	Android Management API Cloud Pub/Sub	56
iOS Mac OS	Apple Push Notification Service（APNs）	56

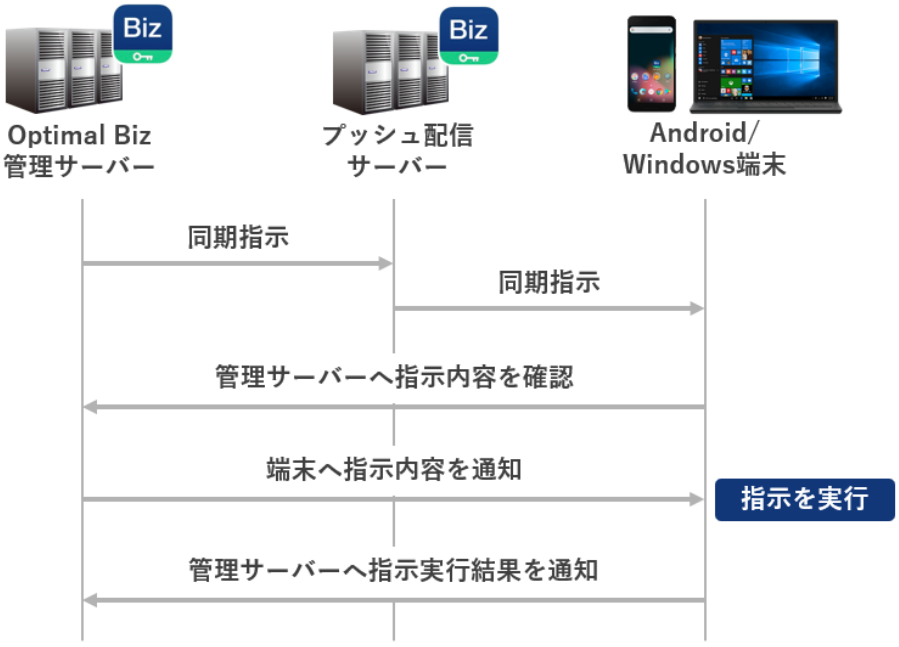
2.5.1.1 Android／Windows

Android 端末や Windows 端末が管理サーバーと同期するには、独自のプッシュ配信サーバーを経由します。

本製品の利用時には、プッシュ配信サーバーと通信できる状態で端末を運用します。

プッシュ配信サーバーは、管理サーバーまたは端末からの同期指示のみを通達します。

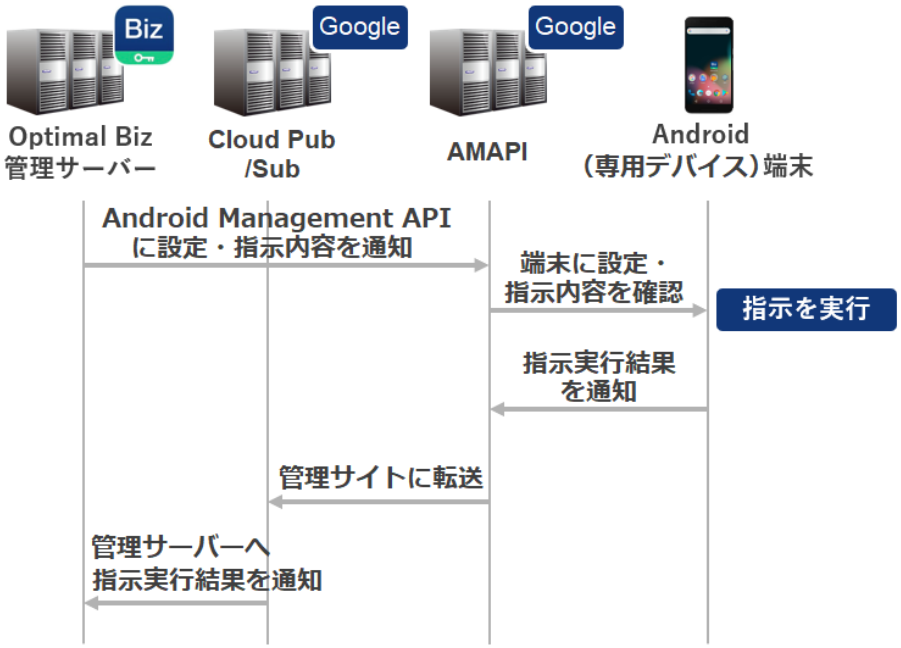
同期指示の通達以降は管理サーバーと端末間で直接通信が行われます。



2.5.1.2 Android（専用デバイス）

Android（専用デバイス）端末が管理サーバーと同期するには、Android Management API、Cloud Pub/Sub を経由します。Android Management API、Cloud Pub/Sub は Google が提供するサービスです。本製品の利用時には、Android Management API、Cloud Pub/Sub と通信できる状態で端末を運用します。

Android Management API は管理サーバーから端末に設定変更や操作指示を通達します。また、端末からの情報を Cloud Pub/Sub に通達します。Cloud Pub/Sub は、端末情報を管理サーバーに通達します。

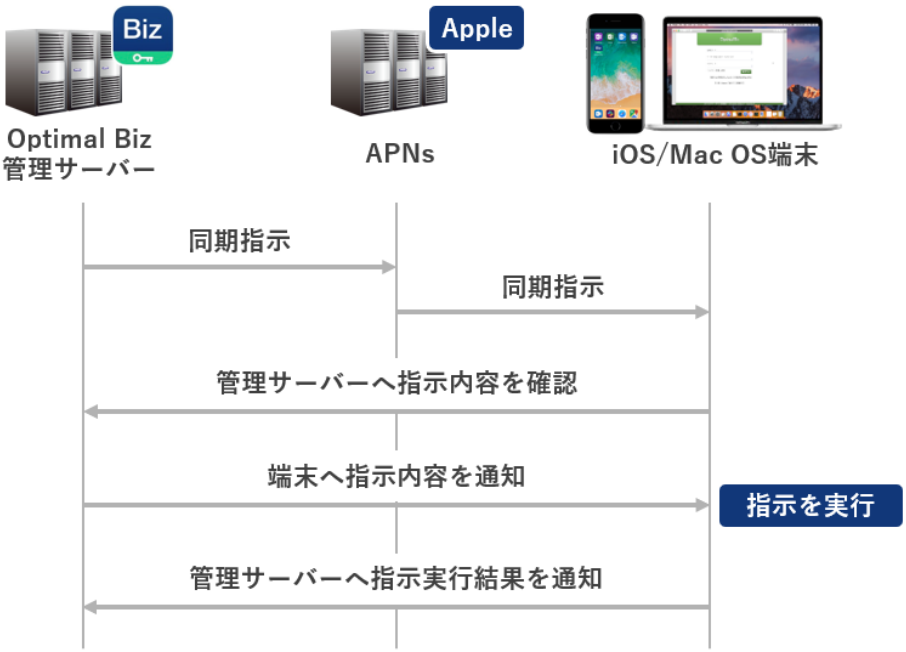


2.5.1.3 iOS／Mac OS

iOS 端末や Mac OS 端末などの Apple 製品が管理サーバーと同期するには、必ず APNs と呼ばれるプッシュ配信サーバーを経由します。APNs は Apple が提供しているサーバーです。本製品の利用時には、APNs と通信できる状態で端末を運用します。

APNs は、管理サーバーまたは端末からの同期指示のみを通達します。

同期指示の通達以降は管理サーバーと端末間で直接通信が行われます。



2.5.2 同期の種類

本製品の同期には、定期的に自動で行われる定期同期と任意のタイミングで行う手動同期があります。

「定期同期」57 ページ
「手動同期」57 ページ

2.5.2.1 定期同期

定期同期は、定期的に自動で同期が行われます。定期同期のタイミングは、以下のとおり OS ごとに異なります。

OS	定期同期タイミング
Android Windows	10 分から月 1 まで選択可能（デフォルト 30 分）
Android（専用デバイス）	24 時間ごと
iOS Mac OS	前回の同期から最短 8 時間後

2.5.2.2 手動同期

管理サイトで行った設定をすぐに端末に反映させたい場合は、手動で同期を行うことができます。

管理サイトの［機器］画面で、反映させたい端末の「詳細」画面に表示される 同期 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」－「機器との同期」

手動同期は、端末からも行えます。詳細は、以下を参照してください。

『Android クライアント リファレンスマニュアル』の「エージェントの基本操作」－「Android 端末から管理サイトと同期する」

『Android（AMAPI）クライアント リファレンスマニュアル』の「専用デバイスの基本操作」－「端末から管理サイトと同期する」

『iOS クライアント リファレンスマニュアル』の「ポータルの使用方法」－「iOS 端末から管理サイトに同期する」

『Mac OS クライアント リファレンスマニュアル』

『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」－「Windows 端末から管理サイトに同期する」

Android 端末、iOS 端末、Windows 端末は、端末を起動したときに同期します。ただし、Windows 端末でスリープ、ハイバネーション、休止状態から起動すると、同期がされない場合があります。