



Optimal Biz

かんたん初期設定マニュアル

最終更新日 2024 年 10 月 20 日

(Web サイト ver.9.22.0)

株式会社オプティム

はじめに

本マニュアルは、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	5
1.1 管理サイトにログインする	6
1.2 初期設定をする	7
1.2.1 Android 端末を設定する	8
1.2.2 iOS 端末を設定する	21
1.3 ユーザーを登録する	34
1.4 機器とユーザーを紐づける	36
2 補足・便利な操作	38
2.1 ログイン／ログアウト	39
2.1.1 パスワードを新規発行／再発行する	39
2.1.2 期限切れパスワードを更新する	42
2.1.3 2段階認証で管理サイトにログインする	44
2.1.3.1 2段階認証を設定してログインする(初回のみ)	44
2.1.3.2 2段階認証でログインする	47
2.1.4 OPTiM ID で管理サイトにログインする	48
2.1.5 管理サイトからログアウトする	51
2.2 組織登録	52
2.3 CSV ファイルの共通操作	54
2.3.1 CSV ファイルをアップロードする	54
2.3.2 インポート用の CSV ファイルの構造	56
2.3.3 CSV ファイルをインポートできる機能	56
2.4 管理方式	57
2.4.1 エージェントとは	57
2.4.2 Android Device Policy とは	57
2.4.3 MDM 構成プロファイルとは	57
2.4.4 構成プロファイルとは	57
2.5 同期	58
2.5.1 同期の仕組み	58
2.5.1.1 Android／Windows	59
2.5.1.2 Android (専用デバイス)	60
2.5.1.3 iOS／Mac OS	61
2.5.2 同期の種類	62
2.5.2.1 定期同期	62
2.5.2.2 手動同期	62

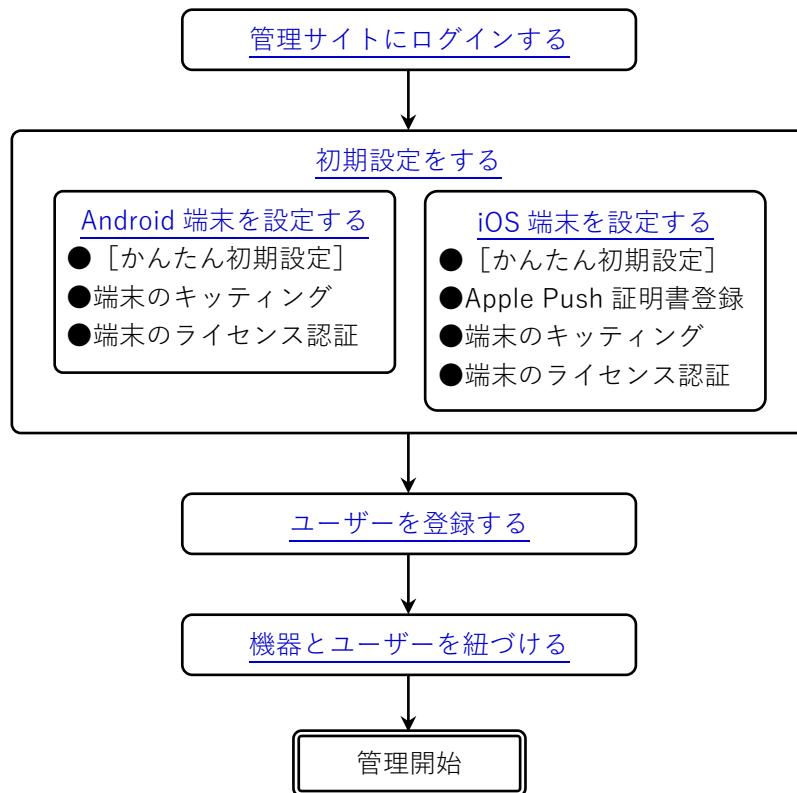
1 端末の管理を開始する

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」

☒ OPTiM ID 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。

☞ 「OPTiM ID で管理サイトにログインする」 48 ページ

[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。

Optimal Biz

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

2

3 ログイン

初めてご利用の方、パスワードを忘れた方はこちら

OPTiM IDでログイン

日本語 | English

©2011 OPTiM | 利用規約 | プライバシーポリシー | マニアル

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」 57 ページ

☞ 「同期」 58 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。

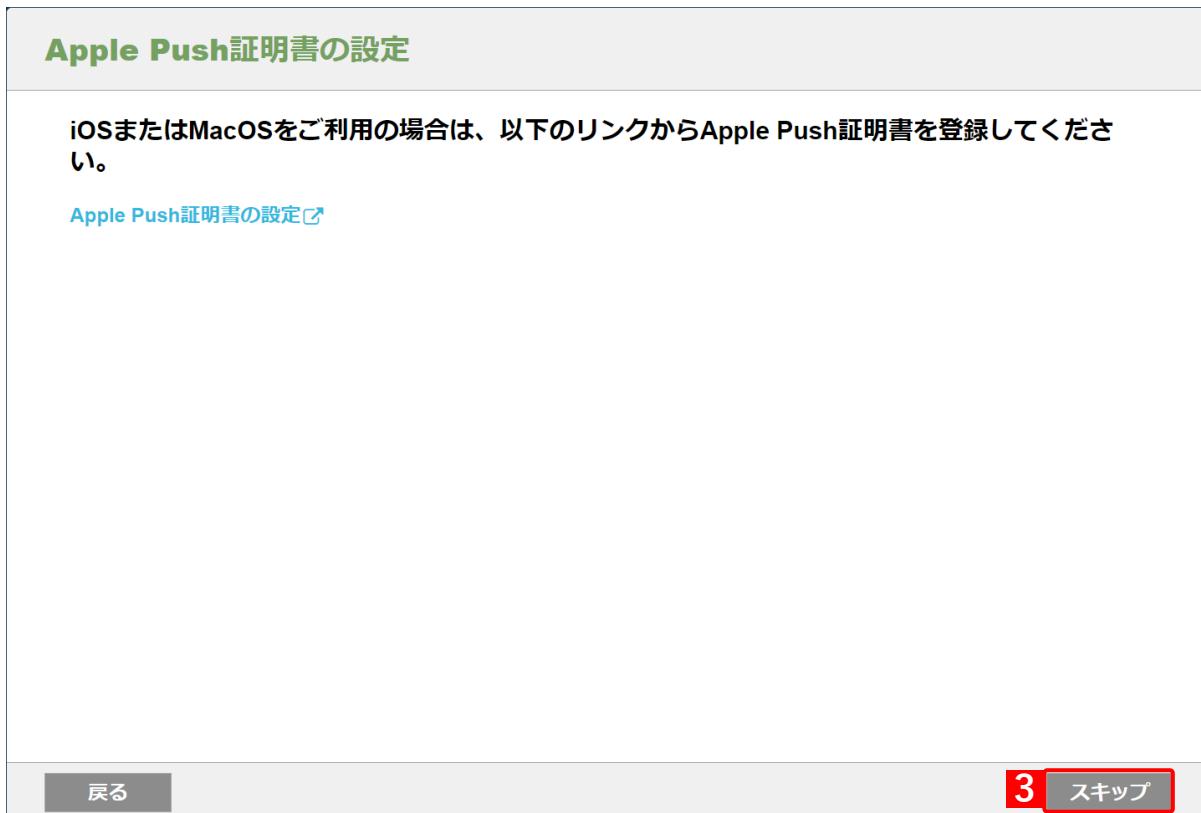
⇒ 「かんたん初期設定の開始」画面が表示されます。

The screenshot shows the Optimal Biz management interface. In the center, there's a section titled 'かんたん初期設定' (Simpler Initial Setup) with a large green button labeled '1 からかんたん初期設定'. This button is highlighted with a red box. Below the button, there's some explanatory text: 'スマートフォンやPCなどの機器の管理を始めるために、おすすめの設定を行います。' (For managing devices like smartphones and PCs, we recommend performing the following settings). At the bottom of the page, there are two buttons: '終了' (End) on the left and '開始' (Start) on the right, which is also highlighted with a red box.

[2] [開始] をクリックします。

This screenshot shows the 'かんたん初期設定の開始' (Simpler Initial Setup Start) screen. It consists of three main steps: 1. 'セキュリティの設定' (Security Settings) featuring icons of a key and a shield; 2. '機器にアプリをインストール' (Install app on device) featuring an icon of a smartphone; 3. '完了!!' (Completed!!) featuring an icon of a smartphone with a numeric keypad. Each step is preceded by a green arrow pointing right. At the bottom left is a '終了' (End) button, and at the bottom right is a large orange '開始' (Start) button, which is also highlighted with a red box.

【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。

✉ メール通知の送信先設定

❶ おすすめセキュリティを設定しました。

管理対象の機器において問題が発生した場合に、メールでお知らせします。

(例1)機器から通信が来なくなった時
(例2)機器にリモートロックを行った時

送信先メールアドレス(30件まで)

5 [redacted] 削除

追加

メール通知のサンプル
下記の事象が発生しました。
企業名: 株式会社○○
2016/10/19 20:43:23 機器「端末A」の通信が2016/04/18 09:30:13から1時間以上ありませんでした。
2016/10/19 20:43:23 機器「端末B」のリモートロックを行いました。

戻る スキップ 6 設定する

⇒ 「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。

□ 機器の認証

❶ メール通知の送信先を設定しました。

エージェントアプリ(管理用アプリ)を、管理対象の機器にインストールしてください。

iOS/Windows/Macのインストール

インストール元のURL

iOS https://[redacted]/i
Windows https://[redacted]/w
Mac https://[redacted]/m

Androidのインストール

Device Owner Mode のエージェントアプリのインストールが必要です。

(A) 機器認証用コード
企業コード [redacted]
認証コード [redacted]

(1)管理対象の機器から左記のURLにアクセスしてください。
(2)画面の指示に従い、管理用アプリをインストールしてください。
(3)ライセンス認証画面で左記の機器認証用コードを入力してください。
(4)セキュリティ設定が適用されます。



戻る スキップ 完了

[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。

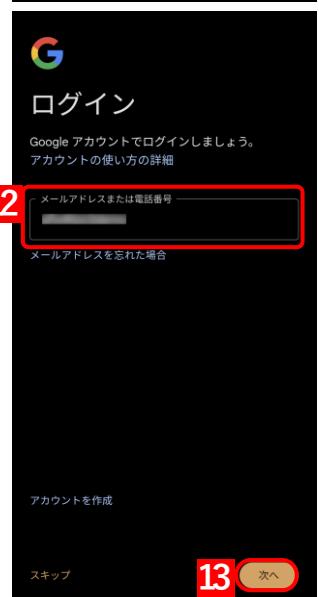


[11] [コピーしない] をタップします。

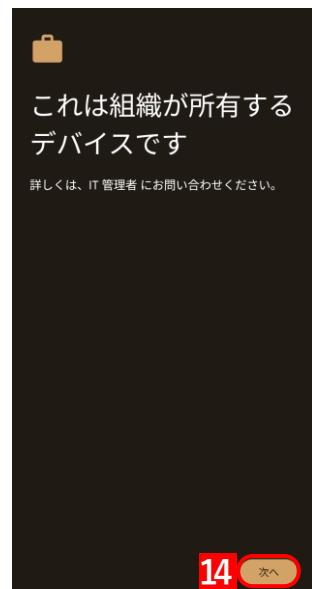


[12] 「メールアドレスまたは電話番号」に「afw#biz3」と入力します。

[13] [次へ] をタップします。



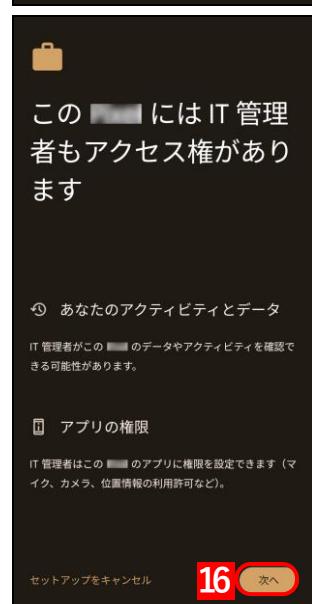
【14】 [次へ] をタップします。



【15】 [同意して続行] をタップします。



【16】 [次へ] をタップします。

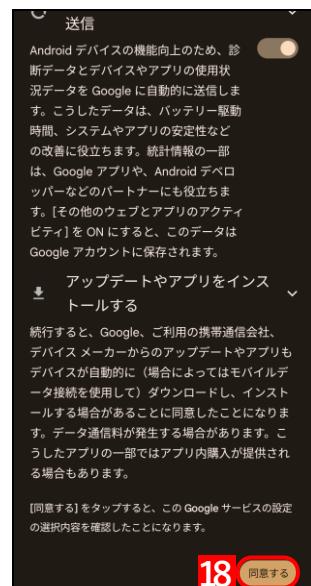


[17] [もっと見る] をタップします。

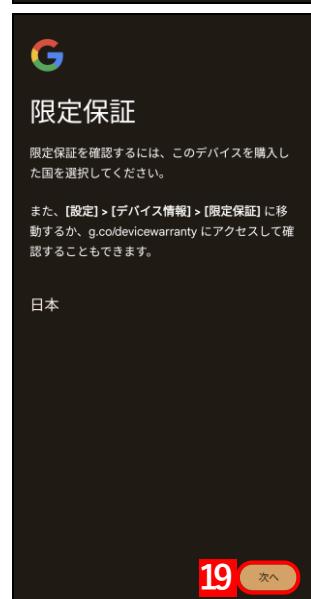
④ 端末によっては「[もっと見る]」が数回表示されます。[同意する]が表示されるまで、タップします。



[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。

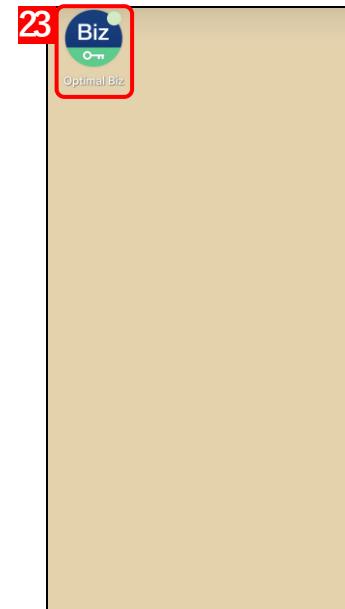
**[21] [スキップ] をタップします。****[22] 画面下部からスワイプします。**

⇒ ホーム画面に移動します。

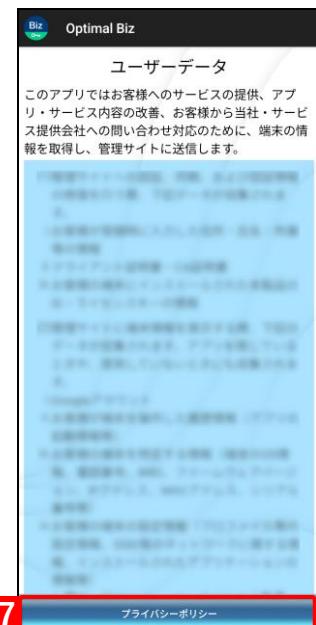


[23] [Optimal Biz] をタップします。

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。

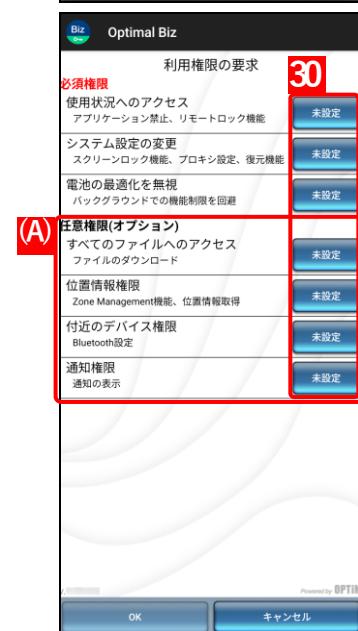


[30] 画面の案内に従って設定を行ってください。

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。

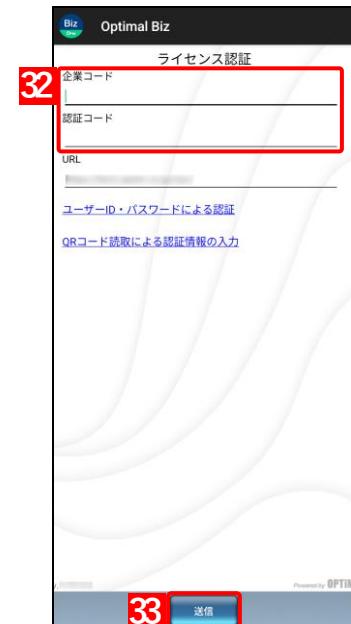


[32] 「企業コード」、「認証コード」を入力します。

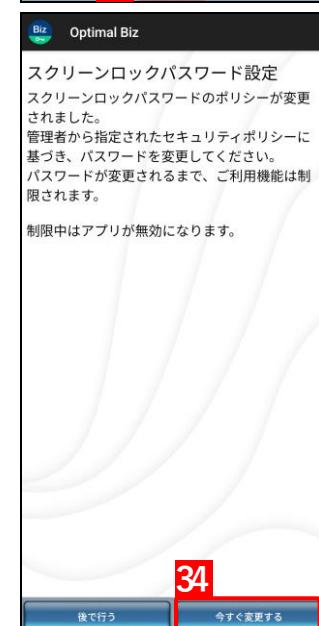
「企業コード」と「認証コード」は、[かんたん初期設定] の「機器の認証」画面に表示されています。

[33] [送信] をタップします。

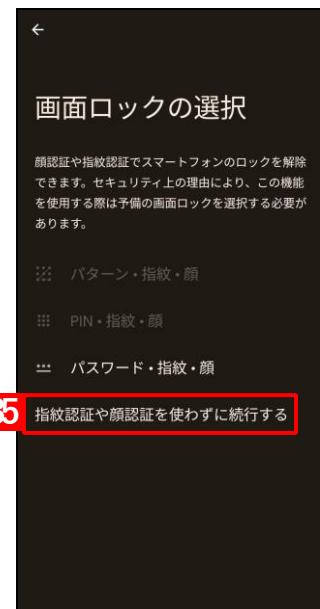
⇒ ライセンス認証が完了します。「スクリーンロックパスワード設定」画面が表示されます。



[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。

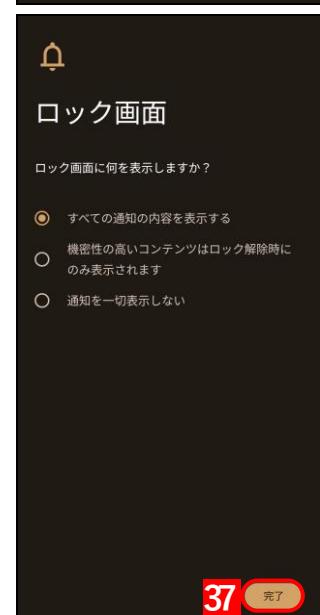
⇒ パスワード設定画面が表示されます。画面の指示にしたがい、
パスワードを設定してください。

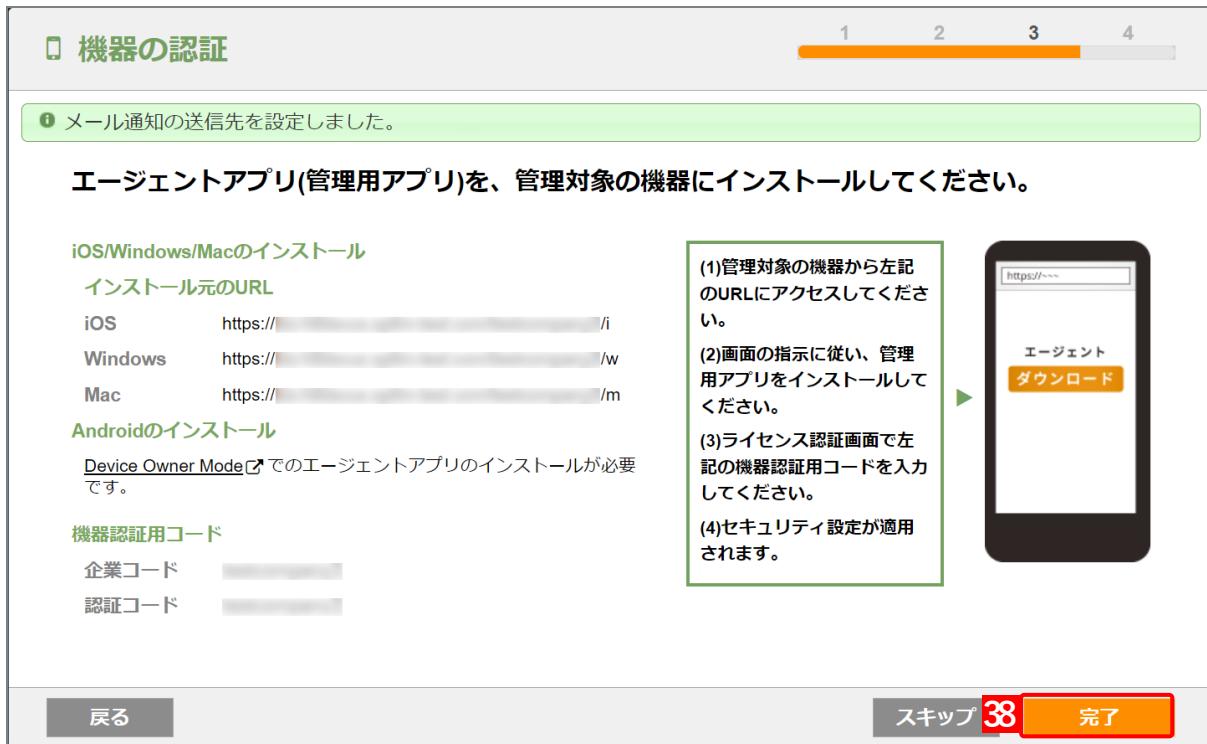
パスワードは、英数字を含む 8 文字以上で設定してください。



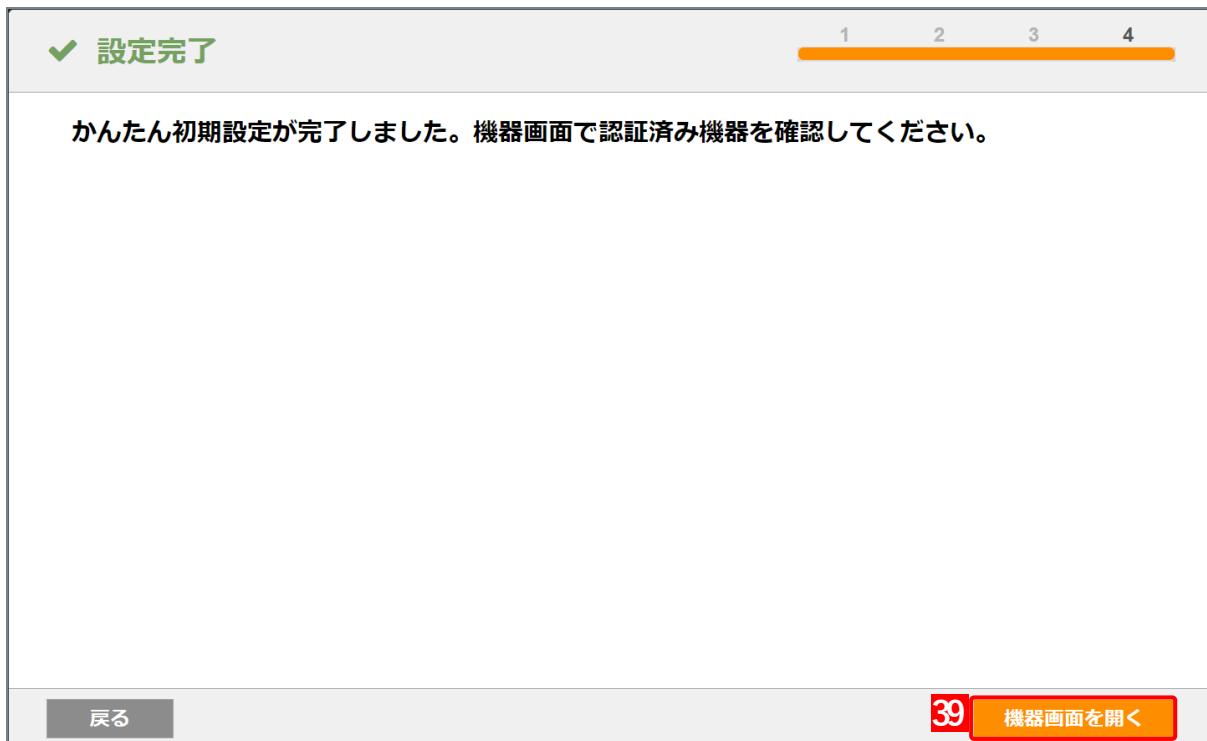
[37] [完了] をタップします。

⇒ [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。

The screenshot shows the Optimal Biz management interface. In the center, there is a large button labeled 'ここからかんたん初期設定' (Start Easy Initial Setup) with a red box and the number '1' over it. To the left of this button, there is another button labeled '未設定' (Not Set). The top navigation bar includes links for '機器' (Devices), 'ユーザー' (Users), '組織' (Organizations), '設定' (Settings), 'ログ' (Logs), and '関連サービス' (Related Services). On the right side, there is a '利用状況' (Usage Status) section with various metrics like '0/10' and '0/10'.

[2] [開始] をクリックします。

The screenshot shows the 'Easy Initial Setup' start screen. It displays three sequential steps: 1. 'セキュリティの設定' (Security Settings) with icons of a key and shield; 2. '機器にアプリをインストール' (Install app on device) with an icon of a smartphone; 3. '完了!!' (Done!!) with an icon of a smartphone displaying a numeric keypad. At the bottom left is a '終了' (Exit) button, and at the bottom right is a large orange '開始' (Start) button with the number '2' over it.

[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。

Apple Push証明書の設定

iOSまたはMacOSをご利用の場合は、以下のリンクからApple Push証明書を登録してください。

3 Apple Push証明書の設定

戻る **スキップ**

[4] [編集] をクリックします。

Optimal Biz

OSを選択: Android, Android(AMAPI), iOS, Mac OS, Windows

サービス環境設定

- 通知設定
- アカウントポリシー
- 機器認証制御
- LDAP
- ポータル表示
- Android Enterprise(企業アカウント登録)
- Android Enterprise(AMAPIアカウント登録)
- Apple Push証明書** (Red box)
- Windows情報保護共通設定
- かんたん初期設定

4 编集

マニュアル

[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。

1. 署名済みの証明書要求(CSR)ファイルの生成とダウンロード

署名済みの証明書要求(CSR)ファイルをダウンロードしてください。

5 ダウンロード**2.** 証明書ファイルの取得

以下のリンクより「Apple Push Certificates Portal」にログインし証明書を取得してください。
証明書ファイルは、署名済みの証明書要求(CSR)をアップロードすることで取得できます。

6 <https://identity.apple.com/pushcert/>

※Internet ExplorerではApple Push Certificates Portalサイトを表示できないため、Safari、Google Chrome、Firefox等のブラウザで開いてください。

※証明書を1年に1回更新する必要があります。証明書の有効期限が切れた場合、本製品はご利用いただけなくなります。

3. 証明書ファイルの登録

2.より作成した証明書ファイルを指定してください。

[ファイルを選択] 選択されていません

Apple ID (証明書発行の際に使用されたApple IDを以下に記載してください。)

備考

取消

保存

[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。

Apple IDを使ってサインイン

7 Apple ID**8**  Apple IDをブラウザに保存[Apple IDまたはパスワードをお忘れですか？](#)[Apple IDをお持ちでないですか？
作成はこちら](#)

【9】「パスワード」を入力します。

【10】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。

The screenshot shows the 'Apple IDを使ってサインイン' (Sign in with Apple ID) screen. A red box highlights the '9 パスワード' (9 Password) input field and the '10' button with a right-pointing arrow. Below the input fields is a checkbox for saving the Apple ID to the browser. At the bottom, there are links for forgot Apple ID or password.

Apple IDを使ってサインイン

9 パスワード 10 →

Apple IDをブラウザに保存

Apple IDまたはパスワードをお忘れですか? [↗](#)

Apple IDをお持ちでないですか? [作成はこちら > ↗](#)

【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。

The screenshot shows the '本人確認' (Person confirmation) screen. A red box highlights a list of three phone numbers, each followed by an 'SMS' label and a right-pointing arrow. Below the list is a note about selecting a delivery recipient and a link for access issues.

本人確認

11

.....
SMS

.....
SMS

.....
SMS

確認コードの送信先に使用する電話番号を選択してください。

これらの電話番号にアクセスできませんか?

【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。

The screenshot shows the '2ファクタ認証' (2-factor authentication) screen. A red box highlights a row of six input boxes. Below the boxes is a note about sending the code via text message and links for other phone numbers or options.

2ファクタ認証

12

確認コードを含むテキストメッセージを..... に送信しました。
た。続けるにはコードを入力してください。

[他の電話番号を使用](#) | [その他のオプション](#)

[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。

〔筆〕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。

1. 署名済みの証明書要求(CSR)ファイルの生成とダウンロード
署名済みの証明書要求(CSR)ファイルをダウンロードしてください。
ダウンロード

2. 証明書ファイルの取得
以下のリンクより「Apple Push Certificates Portal」にログインし証明書を取得してください。
証明書ファイルは、署名済みの証明書要求(CSR)をアップロードすることで取得できます。
<https://identity.apple.com/pushcert/>
※Internet ExplorerではApple Push Certificates Portalサイトを表示できないため、Safari、Google Chrome、Firefox等のブラウザで開いてください。
※証明書を1年に1回更新する必要があります。証明書の有効期限が切れた場合、本製品はご利用いただけなくなります。

3. 証明書ファイルの登録
(A) 2.より作成した証明書ファイルを選択してください。
19 ファイルを選択

20 Apple ID (証明書発行の際に使用されたApple IDを以下に記載してください。)
21 備考

22 取消 保存

【23】 [設定する] をクリックします。

おすすめセキュリティ 1 2 3 4

以下のセキュリティ機能を管理対象の機器に設定します。

○ パスワード	○ 暗号化	○ バックアップ	○ ウイルス対策機能
パスワードの入力 必須 パスワードの文字数 8文字以上 □ ツクまでの時間 5分	機器の暗号化 する	機器のバックアップ する バックアップの周期 毎週月曜日	ウイルススキャン する リアルタイムスキャン する スキャン時刻 毎週金曜日12時

※Androidのみ対応

※Androidのみ対応

戻る **スキップ** **23 設定する**

【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。

メール通知の送信先設定

❶ おすすめセキュリティを設定しました。

管理対象の機器において問題が発生した場合に、メールでお知らせします。

(例1)機器から通信が来なくなった時
(例2)機器にリモートロックを行った時

送信先メールアドレス(30件まで)

24 [redacted] 削除 追加

メール通知のサンプル
下記の事象が発生しました。
企業名: 株式会社○○
2016/10/19 20:43:23 機器「端末A」の通信が2016/04/18 09:30:13から1時間以上ありませんでした。
2016/10/19 20:43:23 機器「端末B」のリモートロックを行いました。

戻る スキップ 25 設定する

⇒ 「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。

機器の認証

❶ メール通知の送信先を設定しました。

エージェントアプリ(管理用アプリ)を、管理対象の機器にインストールしてください。

iOS/Windows/Macのインストール

インストール元のURL

(A) iOS https://[redacted]/i
Windows https://[redacted]/w
Mac https://[redacted]/m

Androidのインストール

Device Owner Mode のエージェントアプリのインストールが必要です。

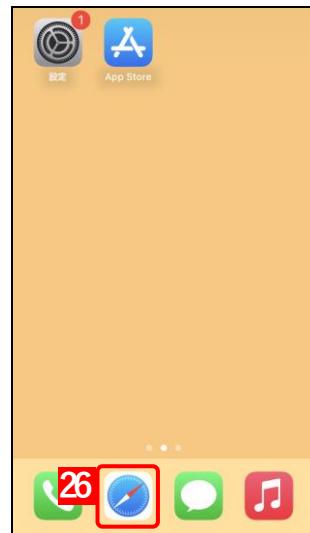
(B) 機器認証用コード
企業コード [redacted]
認証コード [redacted]

(1)管理対象の機器から左記のURLにアクセスしてください。
(2)画面の指示に従い、管理用アプリをインストールしてください。
(3)ライセンス認証画面で左記の機器認証用コードを入力してください。
(4)セキュリティ設定が適用されます。

戻る スキップ 完了

[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。

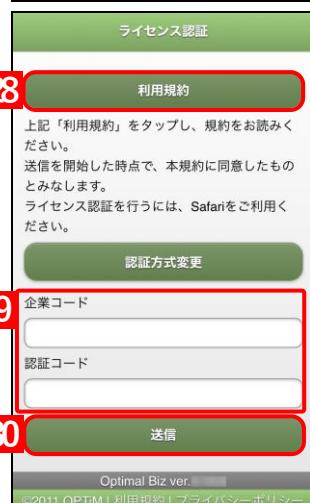
手順【30】で「送信」をタップすることにより、本規約に同意したものとみなします。

[29] 「企業コード」、「認証コード」を入力します。

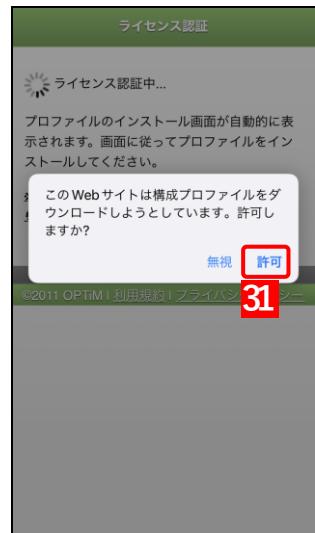
「企業コード」と「認証コード」は、[かんたん初期設定] の「機器の認証」画面に表示されています。

[30] 「送信」をタップします。

⇒ ライセンス認証が開始されます。



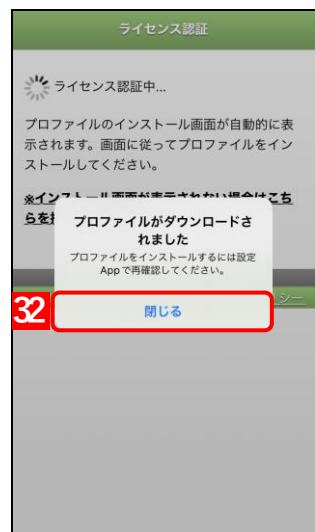
[31] [許可] をタップします。



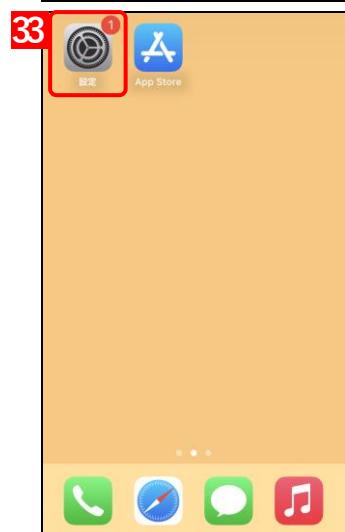
[32] [閉じる] をタップします。

⇒ 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。

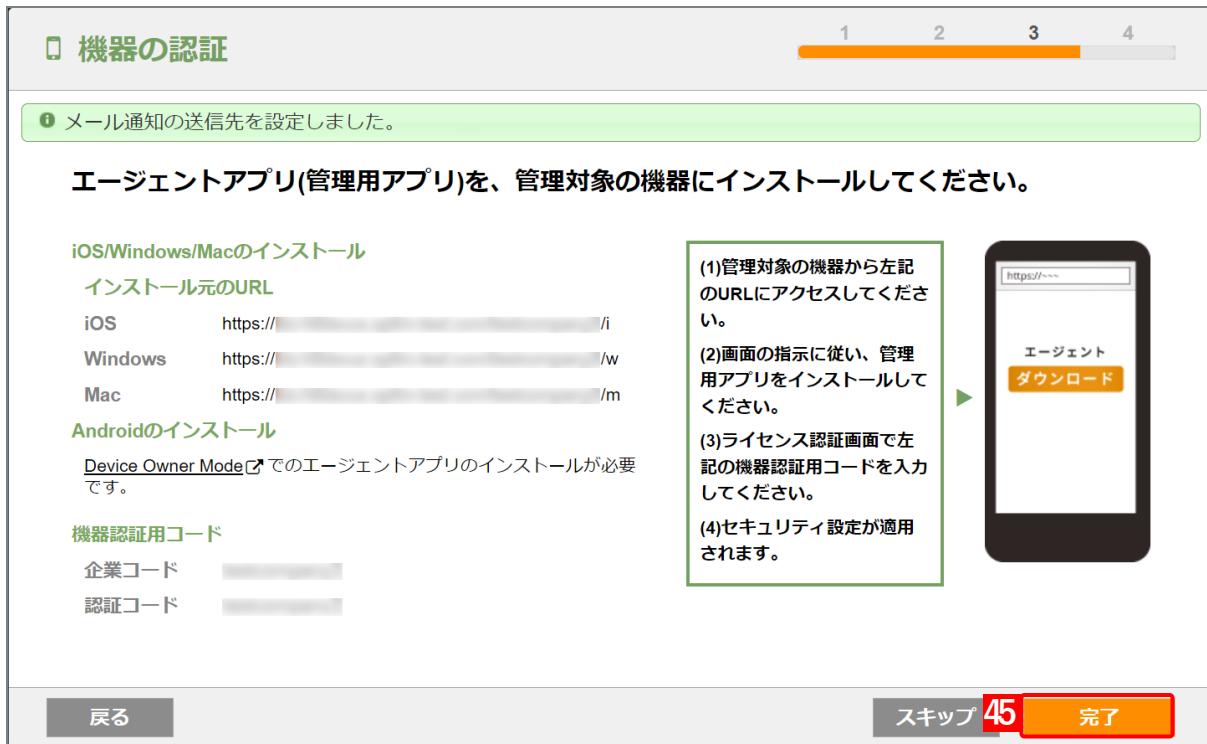


【43】 手順 【41】 で入力したパスコードを、再度入力します。

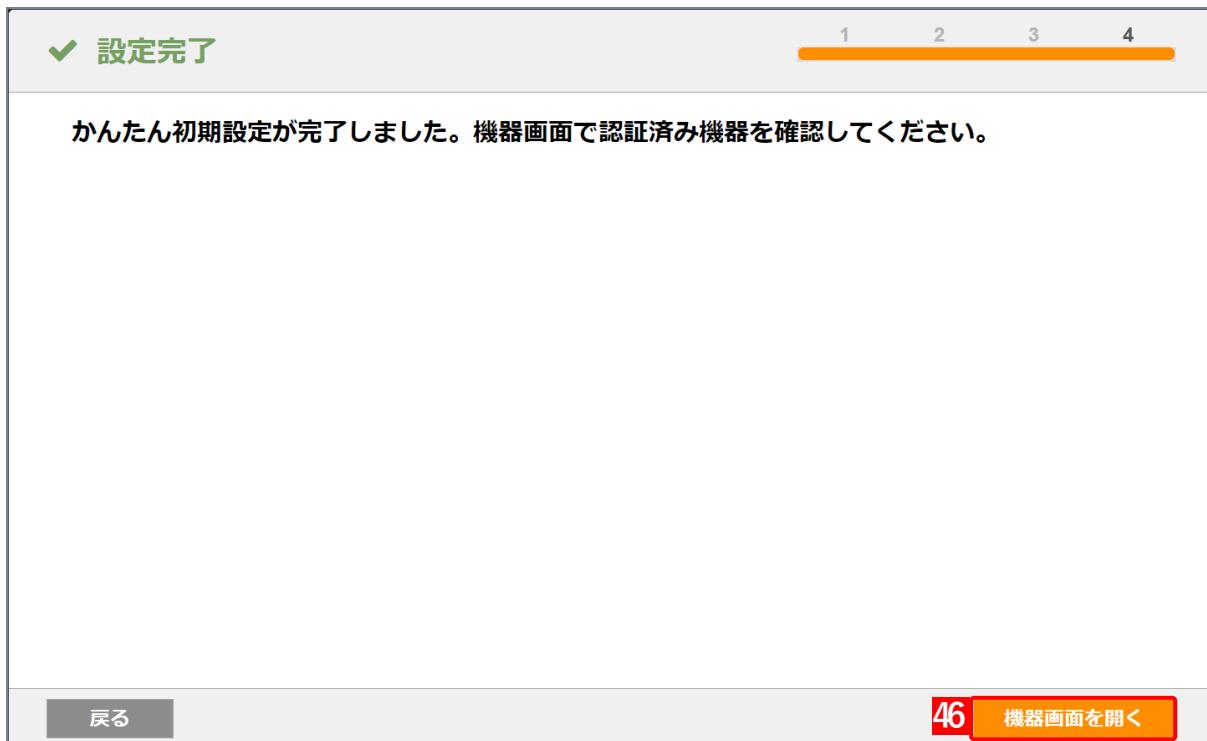
【44】 [パスコードを設定] をタップします。

⇒ [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」 54 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」 52 ページ

[5] [保存] をクリックします

The screenshot shows the 'New User Creation' form in the 'Management Information - Edit集中' section. The form includes fields for Name, Katakana, Last Name, First Name, User ID, Email Address, User Type, Organization, and Device Authentication Limit. A note at the bottom right indicates that steps 3 and 4 are optional.

3 名前

4 ユーザー種別

管理者 (全ての操作ができます)

操作

閲覧者 (変更操作ができません)

ロック・ワープ

ログイン (個別に権限を設定)

一般 (ログインできません)

(A) 組織

機器認証制限

制限なし

制限あり 台

認証禁止

パスワード

パスワード(再入力)

5 保存

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」 54 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。

通信日時: 2024/03/14 17:02:05

OS
[Redacted]

電話番号
(なし)

ユーザー
(なし)

組織
(なし)

3

[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」 52 ページ

[5] [保存] をクリックします。

通信日時: 2024/03/14 17:02:05

機器名
[Redacted]

所属

4 ユーザー
 組織

5

2 補足・便利な操作

「端末の管理を開始する」の設定にかかる補足、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。

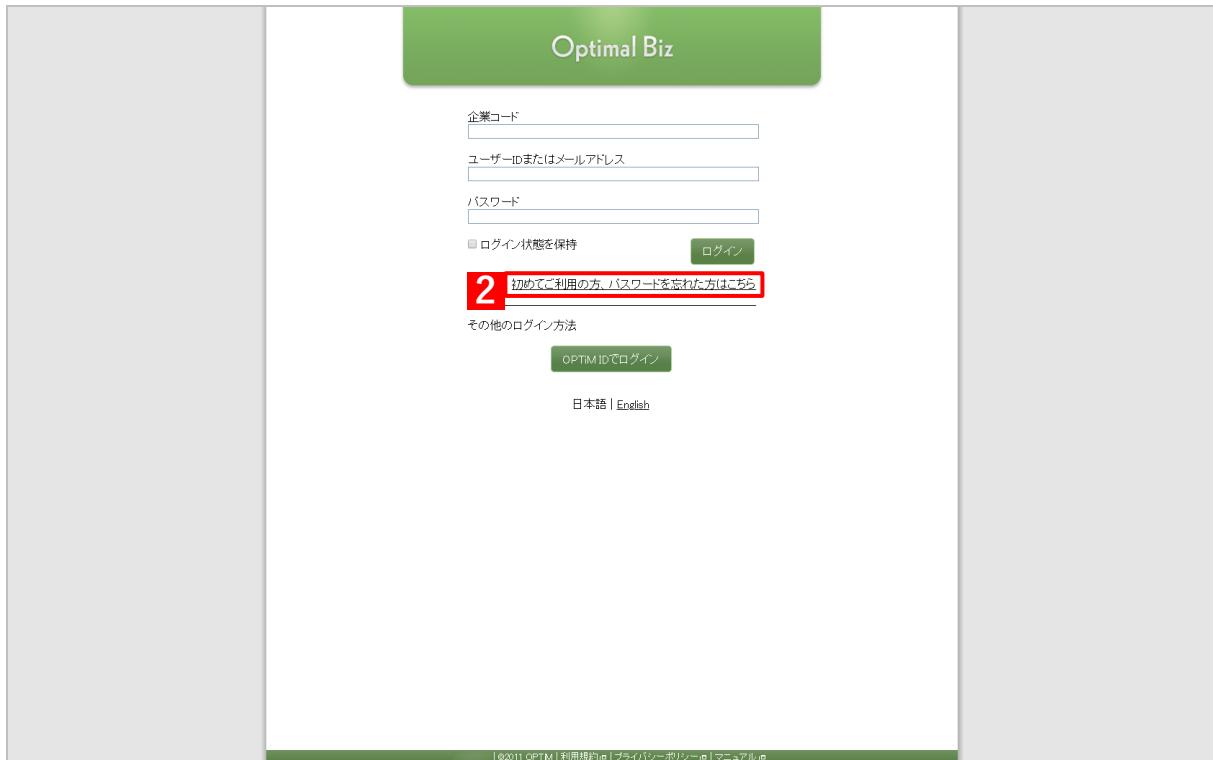
 『管理サイト リファレンスマニュアル』の「サービス環境設定」 - 「アカウントポリシー」

【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。

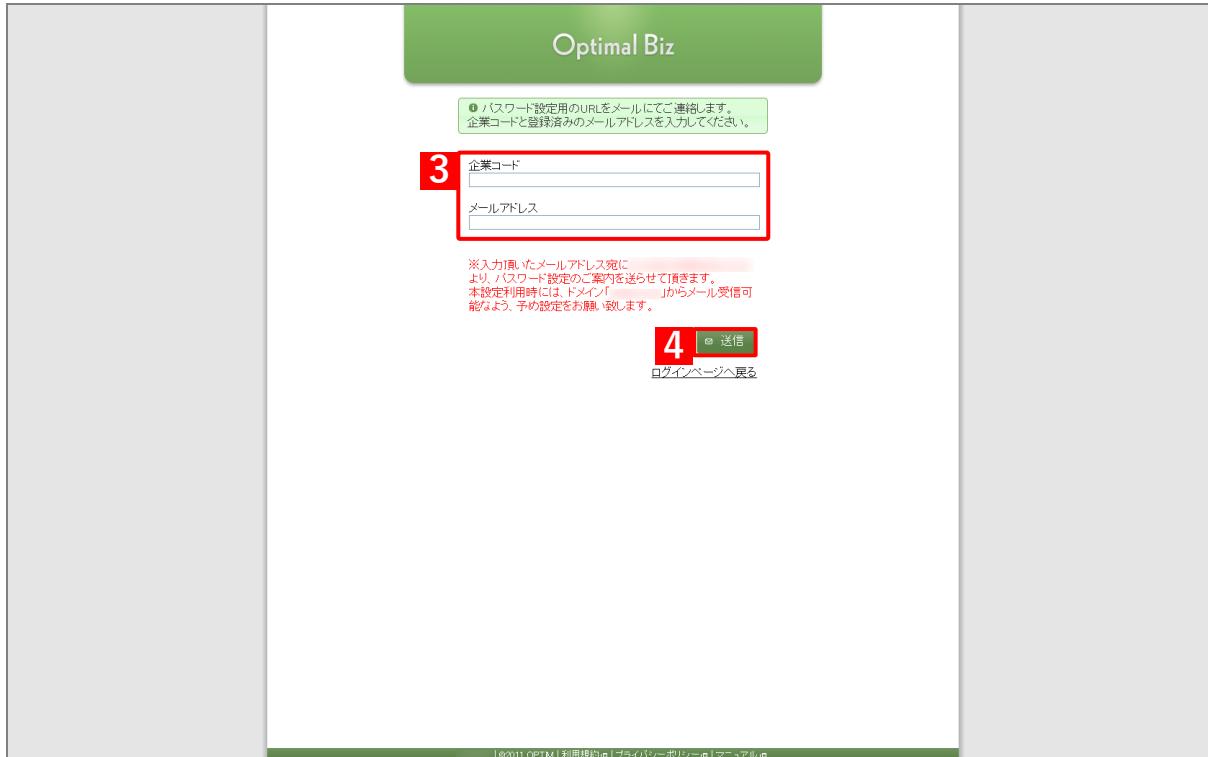
「企業コード」は、すでに入力済みの場合があります。

【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。

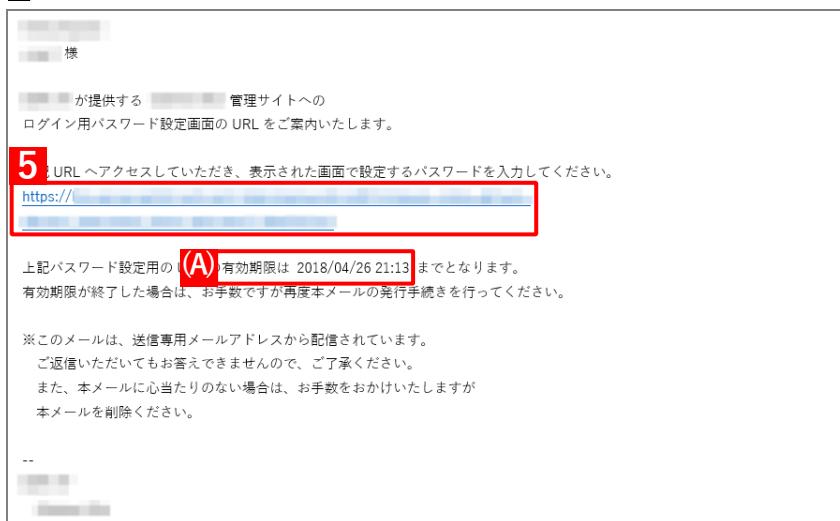


【5】受信したメールの内容を確認し、URL をクリックします。

⇒ 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。

The screenshot shows the Optimal Biz dashboard. At the top, there is a green header bar with the text "Optimal Biz". Below it, a message in a green box says "● 新しいパスワードを設定してください。". The main content area has two input fields: "パスワード" and "パスワード(再入力)", both of which are highlighted with a red box. A large red number "6" is positioned to the left of the first input field. A large red number "7" is positioned to the left of the "設定してログイン" button. At the bottom of the page, there is a footer bar with the text "Optimal Biz | ©2011 OPTIM | 利用規約 | プライバシーポリシー | マニアブル" and a small logo.

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。

The screenshot shows the Optimal Biz login interface. At the top, there is a green header bar with the text "Optimal Biz". Below it is a white login form area. The form fields are labeled with red numbers: "2" above the "企業コード" (Enterprise Code) input field, "2" above the "ユーザーIDまたはメールアドレス" (User ID or Email Address) input field, and "3" above the "ログイン" (Login) button. The "ログイン" button is highlighted with a red border. Below the form, there is a link for "初めてご利用の方、パスワードを忘れた方(はこちら)" (First-time users, password forgotten (here)) and another for "他のログイン方法" (Other login methods). At the bottom of the page, there is a footer bar with links for "OPTIM-IDでログイン" (Log in with OPTIM-ID), "日本語 | English", and copyright information: "©2011 OPTIM | 利用規約 | プライバシーポリシー | マニフェスト".

- [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。

The screenshot shows a web page titled "Optimal Biz". At the top, there is a red warning box containing the text: "▲ アカウントのパスワードは期限切れになりました。パスワードを更新してください。". Below this, there are three input fields labeled 4, 5, and 6, each with a red border:

- 4 現在のパスワード
- 5 新規パスワード
- 5 新規パスワード(再入力)

Below these fields is a green button labeled "6 変更してログイン". To the right of the button is a smaller green button labeled "ログアウト".

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。

The screenshot shows the login page for 'Optimal Biz'. At the top, there is a green header bar. Below it, the main login form has three input fields: '企業コード' (Enterprise Code), 'ユーザーIDまたはメールアドレス' (User ID or Email Address), and 'パスワード' (Password). A red box highlights the '企業コード' field, and another red box highlights the 'ログイン' (Login) button. To the right of the 'ログイン' button, the number '3' is enclosed in a red box. Below the input fields, there is a checkbox labeled 'ログイン状態を保持' (Keep login status) and a link '初めてご利用の方、パスワードを忘れた方はこちら' (For first-time users and password遗忘者). At the bottom of the form, there is a link 'OPTIM IDでログイン' (Log in with OPTIM ID) and language selection links '日本語 | English'. The footer contains small text and links.

【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 行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。

2段階認証の設定
2段階認証の初期設定を行い認証します。設定と認証は以下の手順で行ってください。

STEP1 アプリをインストールする
端末に「Google Authenticator」または「Microsoft Authenticator」をインストールしてください。

▼ 「Google Authenticator」をインストールする場合：
[Android端末](#) [iOS端末](#)

▼ 「Microsoft Authenticator」をインストールする場合：
[Android端末](#) [iOS端末](#)

STEP2 アプリを設定する
「Google Authenticator」または「Microsoft Authenticator」を起動し、端末でQRコードを読み取ってください。
QRコードが読み取れない場合は、「アカウントキー」（※）に表示されている文字列を入力してください。

(A)

(B) アカウントキー

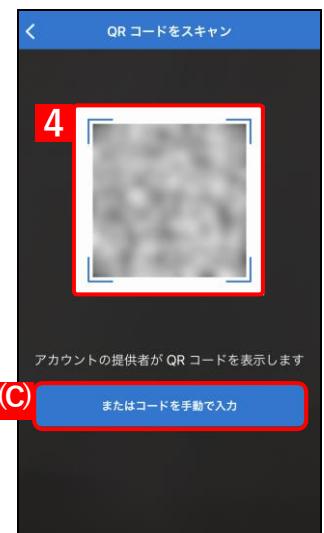
※アカウントキーとは？
アプリを設定するための24桁の文字列（英数字）です。

STEP3 セキュリティコードで認証する
「Google Authenticator」または「Microsoft Authenticator」に表示されている6桁の数字を入力し、[認証する] をクリックしてください。

セキュリティコード

認証する

[ログイン画面に戻る](#)



[5] 端末に表示された (D) 6 行の数字を「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。

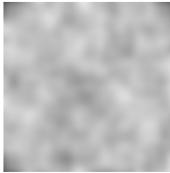
2段階認証の設定
2段階認証の初期設定を行い認証します。設定と認証は以下の手順で行ってください。

STEP1 アプリをインストールする
端末に「Google Authenticator」または「Microsoft Authenticator」をインストールしてください。

▼ 「Google Authenticator」をインストールする場合：
[Android端末](#) [iOS端末](#)

▼ 「Microsoft Authenticator」をインストールする場合：
[Android端末](#) [iOS端末](#)

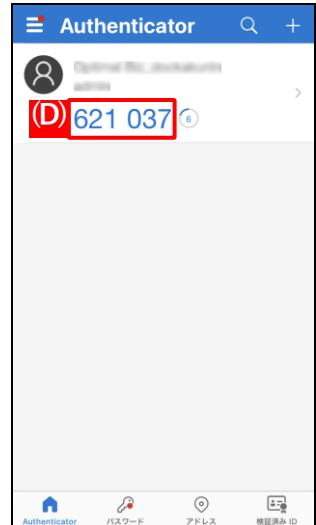
STEP2 アプリを設定する
「Google Authenticator」または「Microsoft Authenticator」を起動し、端末でQRコードを読み取ってください。
QRコードが読み取れない場合は、「アカウントキー」(※)に表示されている文字列を入力してください。

アカウントキー

※アカウントキーとは？
アプリを設定するための24桁の文字列（英数字）です。

STEP3 セキュリティコードで認証する
「Google Authenticator」または「Microsoft Authenticator」に表示されている6行の数字を入力し、「認証する」をクリックしてください。

5 6

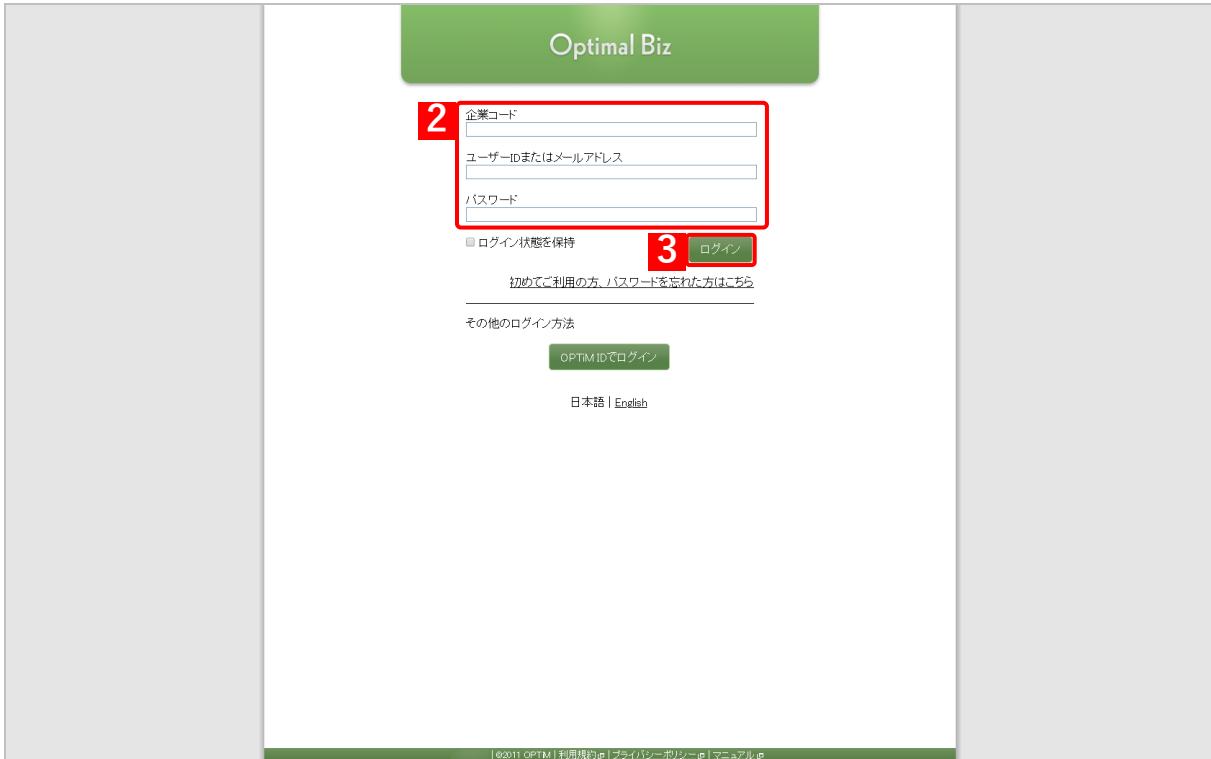
[ログイン画面に戻る](#)



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段階認証

「Google Authenticator」または「Microsoft Authenticator」に表示されている6桁の数字を入力し、[認証する]をクリックしてください。

4 セキュリティコード

5 認証する

[ログイン画面に戻る](#)

Authenticator

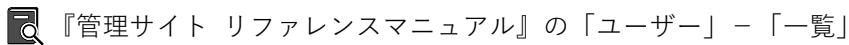
(A) 621 037

Authenticator パスワード アドレス 検証済み ID

2.1.4 OPTiM ID で管理サイトにログインする

OPTiM Contract や OPTiM Assetなどのサービスを契約している場合は、OPTiM ID で管理サイトにログインできます。

【OPTiM ID で管理サイトにログインする】には、ユーザーにメンバーID の設定が必要です。



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

[2] [OPTiM ID でログイン] をクリックします。

→ OPTiM ID のログイン画面が表示されます。

【すでに OPTiM ID にログインしている場合は、管理サイトのダッシュボードが表示されます。】

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

□ ログイン状態を保持

2 OPTiM IDでログイン

初めてご利用の方、パスワードを忘れた方はこちら

その他のログイン方法

日本語 | English

【3】OPTiM ID の「メールアドレス」、「パスワード」を入力します。

【4】[ログイン] をクリックします。

⇒ OPTiM ID で初めてログインする場合は、手順 【5】【6】 の画面が表示されます。2回目以降は、管理サイトのダッシュボードが表示されます。



The screenshot shows the OPTiM ID login page. At the top left is the OPTiM logo. The main title is 'OPTiM ID'. Below it is a form with two input fields: 'メールアドレス' (Email Address) and 'パスワード' (Password), both outlined in red. To the right of the password field is a link 'パスワードをお忘れの場合' (Forgot Password). Below the inputs are two small checkboxes: 'ログイン状態を保持する' (Remember login status) and 'パスワードをお忘れの場合' (Forgot Password). A large blue 'ログイン' (Login) button is at the bottom, also outlined in red. At the bottom of the page, there's a dark footer bar with language links '日本語 English', a privacy policy link 'プライバシーポリシー', a terms of service link '利用規約', and a copyright notice '© OPTiM Corp. All Rights Reserved.'.

【5】利用規約を確認して、[同意] をクリックします。



The screenshot shows a consent screen titled '利用規約' (Terms of Service). It contains a message box stating '本サービスをご利用いただくためには、利用規約への同意が必要です。' (You must agree to the terms of service to use this service.). Below the message is a large text area containing the actual terms of service text, which is mostly illegible due to its length. At the bottom are two buttons: '拒否' (Reject) and '同意' (Accept), with '同意' also outlined in red. The footer is identical to the one in the previous screenshot.

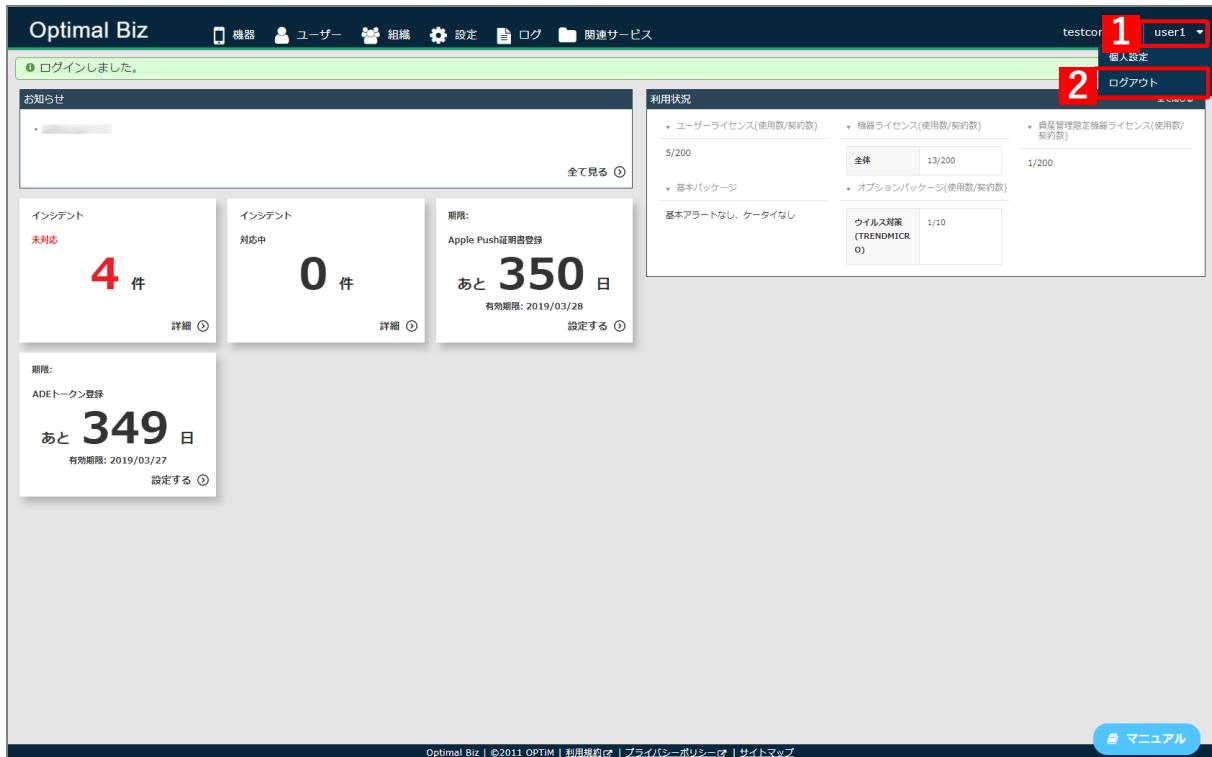
【6】 [許可] をクリックします。

⇒ 管理サイトのダッシュボードが表示されます。



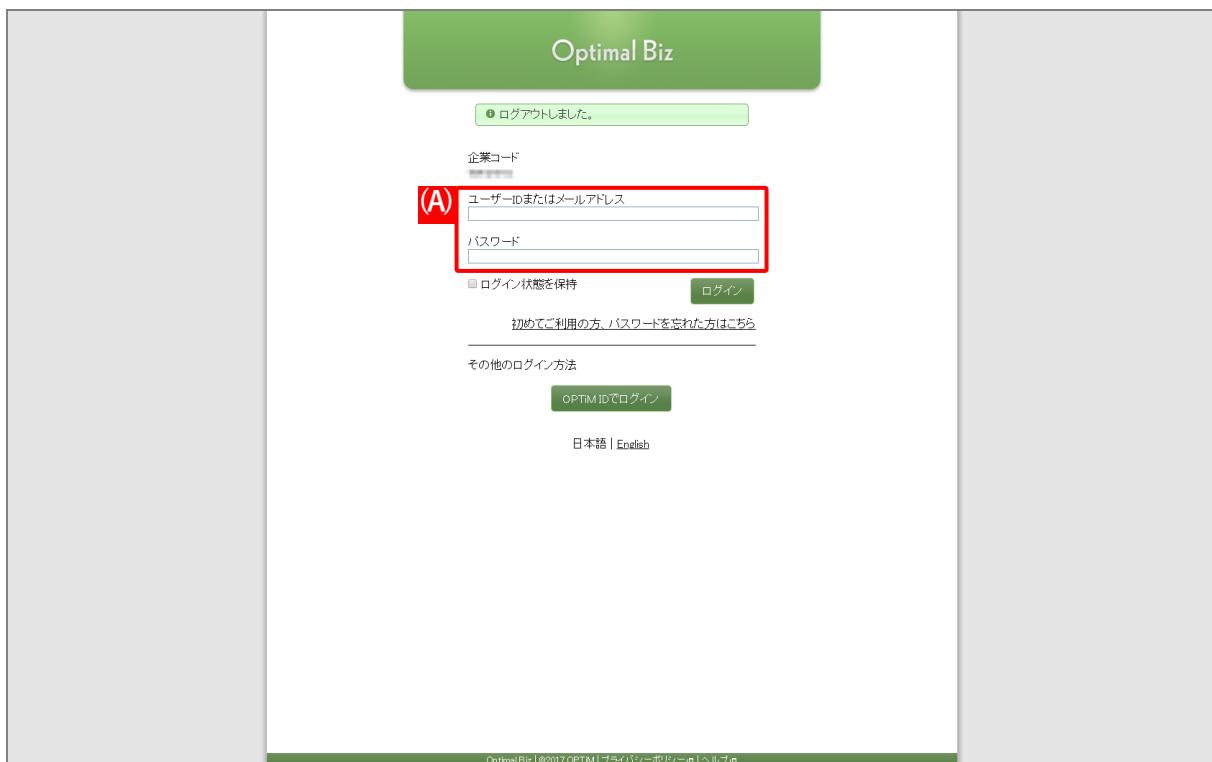
2.1.5 管理サイトからログアウトする

- [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」 54 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

The screenshot shows a user interface for managing organizations. At the top left is a green icon labeled '新規作成' (New Creation). Below it is a navigation bar with the word '管理'. The main area has a dark header bar with the text '管理 - 編集中'. A red box labeled '3' highlights the '組織名' (Organization Name) input field, which is currently empty. Another red box labeled '(A)' highlights the '上位組織' (Parent Organization) section. It contains a note about changing settings affecting access ranges and machine settings, and a note that specifying an LDAP server OU as the parent organization is not possible. It also includes a dropdown menu set to '(なし)' (None) and a checked checkbox for '権限を引き継ぐ' (Inherit permissions). A red box labeled '4' highlights the green '保存' (Save) button at the bottom right.

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 ファイルを利用する機能は、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」 56 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」 56 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。

1. CSVファイルを準備します

「ダウンロード」ボタンをクリックしてCSVファイルをダウンロードします。
ダウンロードしたファイルの内容を編集して保存してください。

ダウンロード

2. CSVファイルをアップロードします

編集したCSVファイルを指定して「アップロード」ボタンをクリックしてください。
アップロード完了後、インポートの確認画面に移動します。

ファイルを選択 .csv

5 アップロード

[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。

下記内容でよろしければ「インポート実行」をクリックしてください。

7 インポート実行

6 全6件

行	[S]Android機器	[S]iOS機器	[S]Mac OS機器	[S]Windows機器	[S]資産管理対象機器	[F]機器名	[S]種別	[S]ユーザー	[S]組織	[F]MACアド
1	ON									
2	ON									
3	ON									
4		ON								
5		ON								
6		ON								

インポートする内容を変更する場合は、CSVファイルを編集後再度アップロードしてください。

(A) ファイルを選択 選択されていません

(B) アップロード

2.3.2 インポート用の CSV ファイルの構造

形式	<ul style="list-style-type: none"> ● 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● 日本語環境 Shift_JIS (CP932) ● 日本語以外の環境 UTF-8 <p> 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。</p>
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	57
Android (専用デバイス)	Android Device Policy	57
iOS Mac OS	MDM 構成プロファイル 構成プロファイル エージェント (任意)	57 57 57

 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

本製品の同期とは、管理サイトで設定した内容を端末に反映したり、管理サイトで保持している端末の情報を更新したりすることです。

2.5.1 同期の仕組み

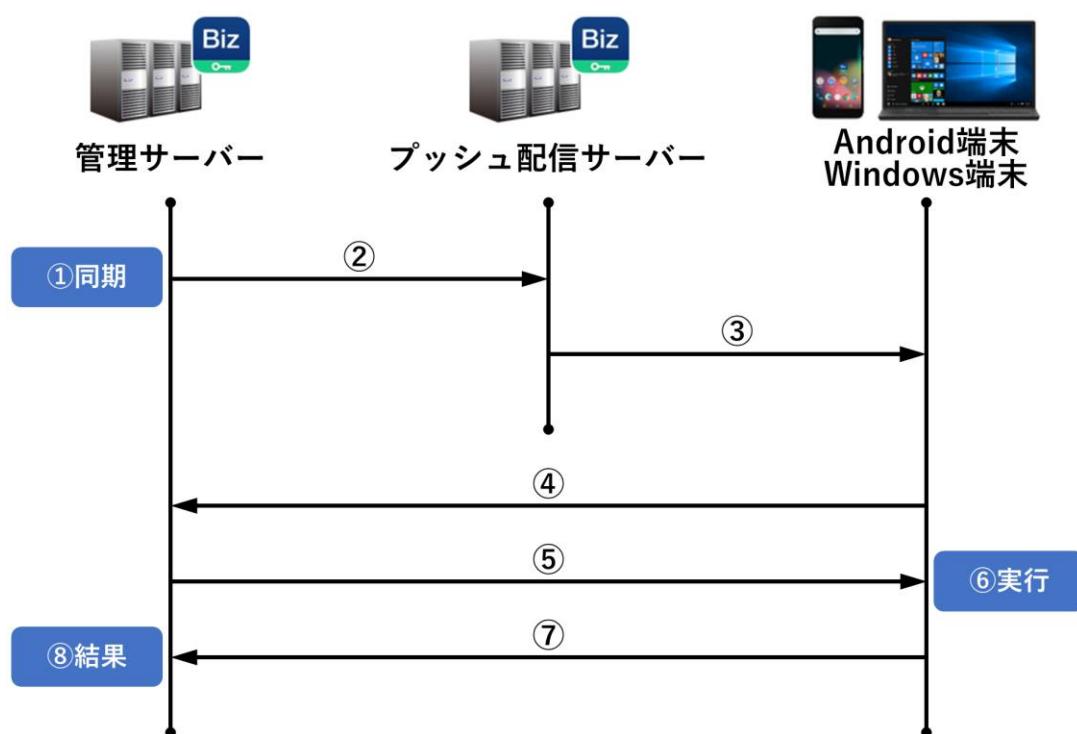
どのような仕組みで同期が行われるかを OS ごとにイメージ図で説明します。

管理サイトと端末の同期を行うには、以下の同期用サーバーまたはサービスを経由します。

OS	同期用サーバーまたはサービス	参照ページ
Android Windows	● プッシュ配信サーバー 本製品の独自 Push 方式のサーバーです。	59
Android（専用デバイス）	● Android Management API（以降、AMAPI と呼ぶ） Google が提供するサービスです。 ● Cloud Pub/Sub 情報を送受信するための Google が提供するサービスです。	60
iOS Mac OS	● Apple Push Notification Service（以降、APNs と呼ぶ） Apple が提供しているサーバーです。	61

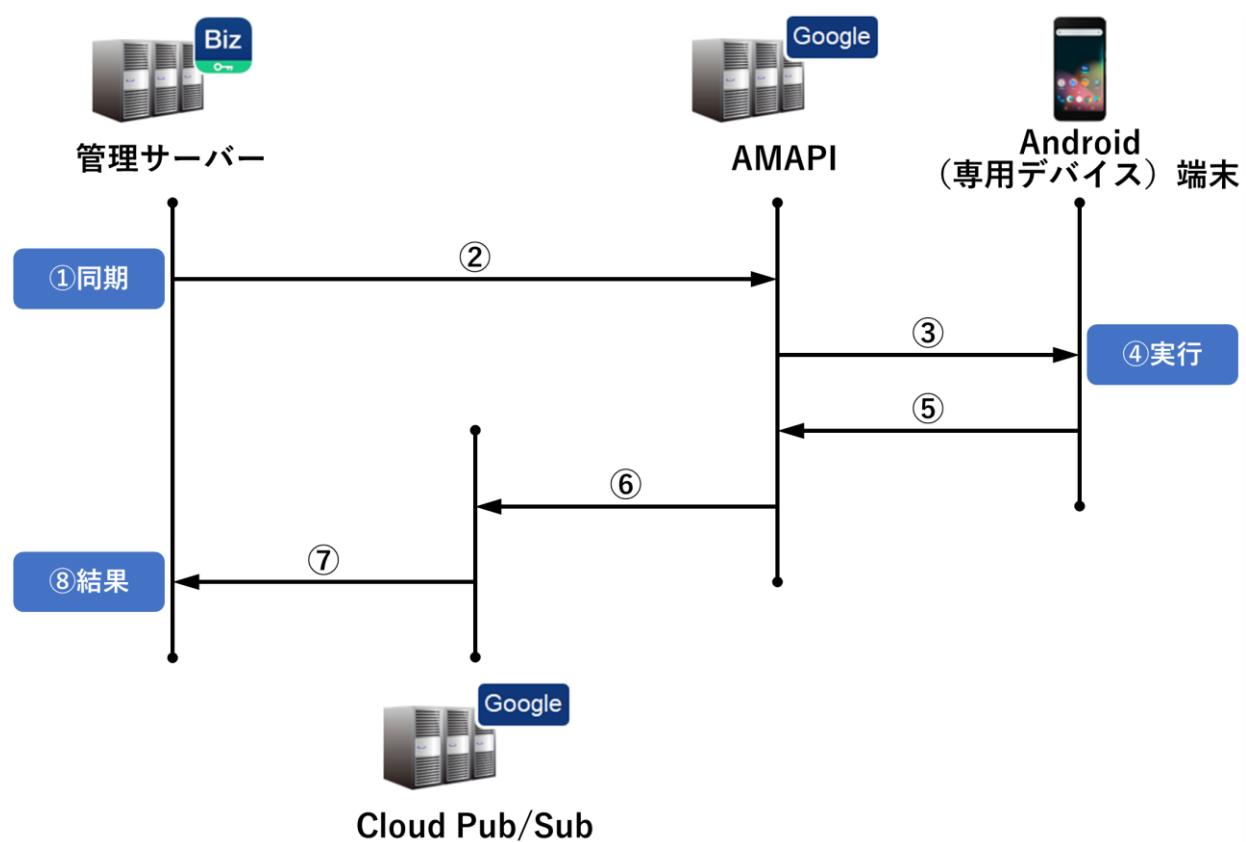
2.5.1.1 Android／Windows

- ① 管理サイトで [同期] を行う
- ② 管理サーバーからプッシュ配信サーバーに同期することを通知する
- ③ プッシュ配信サーバーから端末に同期することを通知する
- ④ 端末から管理サーバーに同期する内容を確認する
- ⑤ 管理サーバーから端末に同期する内容を通知する
- ⑥ 端末で同期する内容を実行する
- ⑦ 端末から管理サーバーに実行結果を通知する
- ⑧ 管理サイトに実行結果が表示される



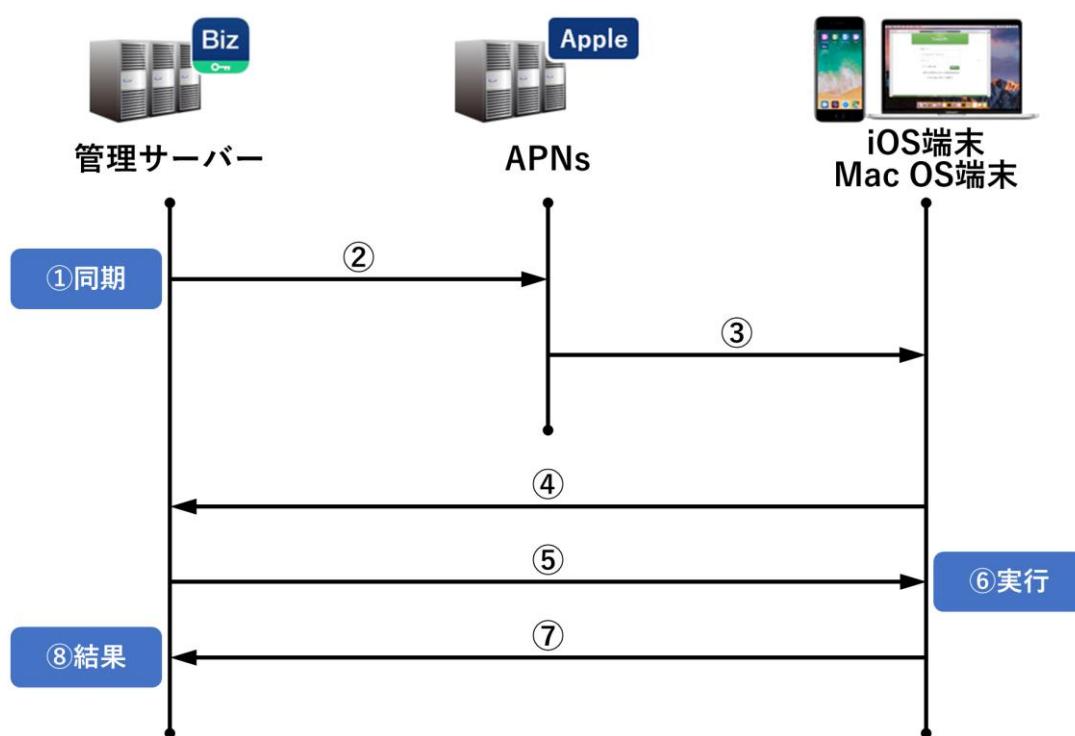
2.5.1.2 Android（専用デバイス）

- ① 管理サイトで [同期] を行う
- ② 管理サーバーから AMAPI に同期する内容を通知する
- ③ AMAPI から端末に同期する内容を通知する
- ④ 端末で同期する内容を実行する
- ⑤ 端末から AMAPI に実行結果を通知する
- ⑥ AMAPI から Cloud Pub/Sub に実行結果を通知する
- ⑦ Cloud Pub/Sub から管理サーバーに実行結果を転送する
- ⑧ 管理サイトに実行結果が表示される



2.5.1.3 iOS/Mac OS

- ① 管理サイトで [同期] を行う
- ② 管理サーバーから APNs に同期することを通知する
- ③ APNs から端末に同期することを通知する
- ④ 端末から管理サーバーに同期する内容を確認する
- ⑤ 管理サーバーから端末に同期する内容を通知する
- ⑥ 端末で同期する内容を実行する
- ⑦ 端末から管理サーバーに実行結果を通知する
- ⑧ 管理サイトに実行結果が表示される



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」 62 ページ

「手動同期」 62 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	10 分から月 1 まで選択可能（デフォルト 30 分）
Windows	
Android（専用デバイス）	24 時間ごと
iOS	前回の同期から最短 8 時間後
Mac OS	

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。