DIGNO® ケータイ4

A202KC

DIGNO® ケータイ4 for Biz

A204KC

Device Control アプリ ご利用マニュアル

第1.0版

目次

Device Control アプリとは

ご利用方法

従業員端末への機能制限設定までの流れ
1. 事前設定
2. ポリシーの作成
3. ポリシーの設定
4. ポリシーの転送、受信 (他端末にも同じポリシーを適用する場合)

サインインパスワードの変更
ステータスの確認方法

機能制限中の端末動作

設定可能なポリシー一覧
端末の機能制限中の動作
アプリの起動制限中の動作

注意事項・FAQ（よくあるご質問）

お問い合わせ先

※ポリシーとは、機能制限の一連の設定のことです。

Device Control アプリとは

Device Control アプリとは

Device Control アプリは、業務用モバイル端末の
設定に最適なアプリです。

特長① 端末機能の利用を制限

電話帳登録外の発着信の制限や、Wi-Fi/Bluetoothの利用を制限するなど
端末機能の利用を制限できます。

特長② 業務に不要なアプリの起動を制限

プリインストールされているアプリの起動を制限できます。

特長③ 端末のみで設定が完結

端末だけで設定でき、操作用PCなどの環境整備が不要です。

特長④ 設定を簡単に複製可能

1台を設定すれば、あとはWi-Fi通信で、他の端末に設定の複製が可能です。

ご利用に適している
お客様

- **従業員の私的利用を防ぎたいお客様**
- **必要最低限の機能制限をしたいお客様**
- **EMMの導入が困難なお客様**

ご利用方法

従業員端末への機能制限設定までの流れ

1. 事前設定(P.7～10)

① Device Control アプリを有効化し、利用できるようにする。
※この処理は**初期状態からのみ実施可能**です。
利用開始済み端末に設定する場合、**「初期状態へのリセット」が必要**となります。

② Device Control アプリをカスタマイズキーに設定する。

③ Device Control アプリへサインインする。

2. ポリシー作成(P.12～14)

④ 端末に設定する制限項目を作成する。 (この時点で、ポリシー設定/機能制限は完了していません。)

3. ポリシー設定(P.15)

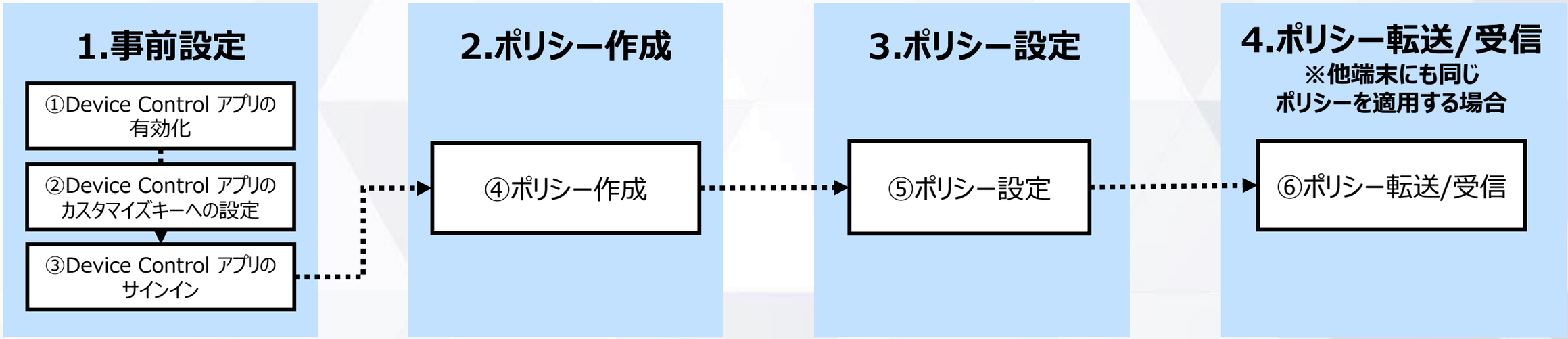
⑤ ポリシーを設定し、機能制限を完了する。

4. ポリシー転送、受信(P.16～17) ※他端末にも同じポリシーを適用する場合

⑥ 他の端末に、ポリシーの転送、受信を行う。

ポイント

ポリシーとは、機能制限の一連の設定のことです。



【注意事項】

- **端末機能の「機能別ロック」とDevice Control アプリは同時に使用しないようご注意をお願い致します。**
  「機能別ロック」を使用中に、Device Control アプリで「設定」アプリを起動制限すると、動作が不安定になる場合がございます。
- 機能制限をご利用される場合、Device Control アプリのサインインパスワードは初期値から変更されることをおすすめします。
  (P.18)サインインパスワードの変更
- 端末に設定されたポリシーは、ステータスから確認できます。
  (P.19)ステータスの確認方法

1. 事前設定　Device Control アプリの有効化（初期状態の場合）

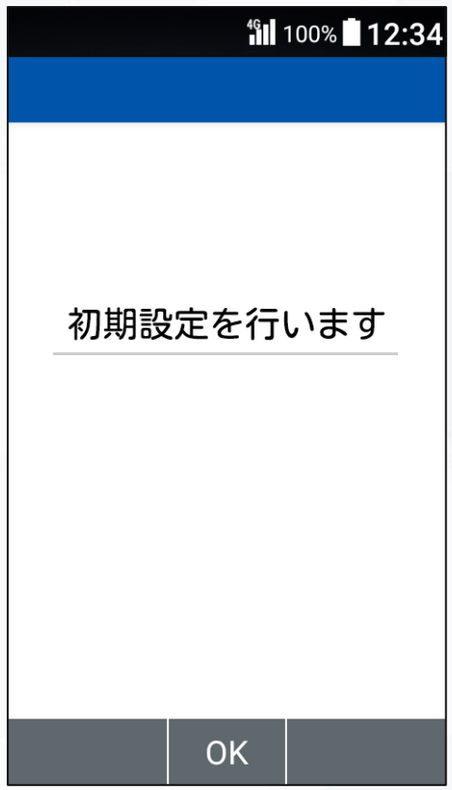
初めて、Device Control アプリをご利用いただく際には有効化の設定が必要です。

※既にDevice Control アプリをご利用の場合は、本操作は不要です。

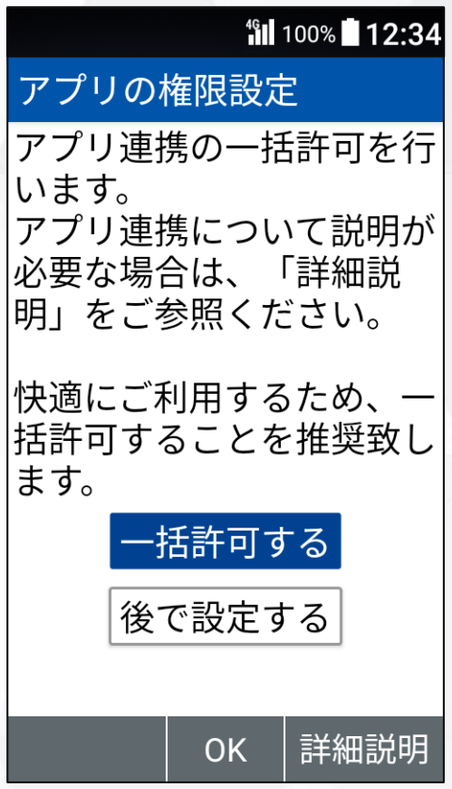
ご注意

有効化には「初期状態にリセット」が必要で、端末内のすべてのデータが消去されます。
そのため、初期設定を行う前や従業員への端末配布前に、有効化を完了することをおすすめします。

初めてDIGNOケータイ4の電源を入れたとき、
または初期状態から有効化する場合



以降は画面表示に沿って、端末の初期設定を行ってください



1 「＊＃＊＃＊＃」をコマンド入力

2 「はい」を選択

3 「一括許可する」または「後で設定する」を選択

4 端末の初期設定完了後、待受画面が表示されます

1. 事前設定　Device Control アプリの有効化（既にご利用中の場合）

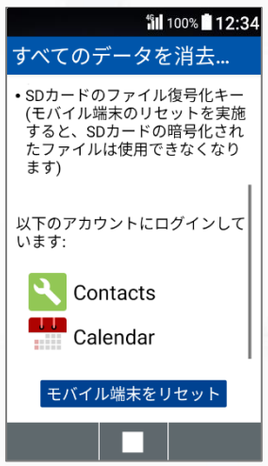
初めて、Device Control アプリをご利用いただく際には有効化の設定が必要です。

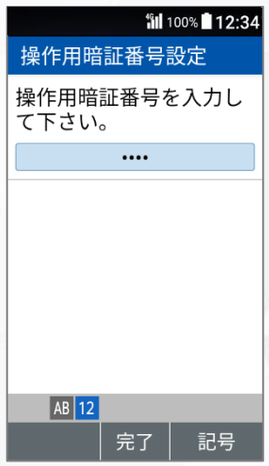
※既にDevice Control アプリをご利用の場合は、本操作は不要です。

ご注意

有効化には「初期状態にリセット」が必要で、端末内のすべてのデータが消去されます。
そのため、初期設定を行う前や従業員への端末配布前に、有効化を完了することをおすすめします。

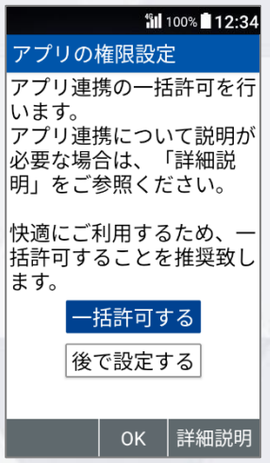
既にご利用中の端末から有効化する場合

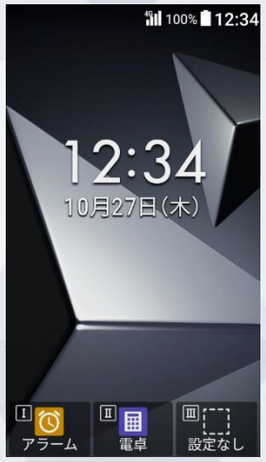




再起動

以降は画面表示に沿って、初期設定を行ってください





1 「設定」→「その他の設定」→「リセットオプション」→「すべてのデータを消去(初期状態にリセット)」→「モバイル端末をリセット」を選択

2 画面の指示に沿って、新しい操作用暗証番号を入力してください。

3 「すべて消去」を選択

4 「＊＃＊＃＊＃」をコマンド入力

5 「はい」を選択

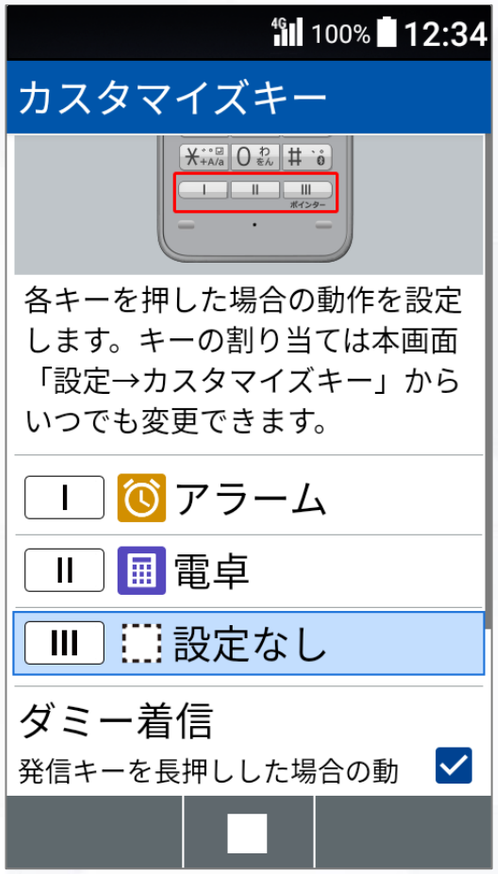
6 「一括許可する」または「後で設定する」を選択

7 端末の初期設定完了後、待受画面が表示されます

1. 事前設定　Device Control アプリをカスタマイズキーに設定

Device Control アプリを起動するには、カスタマイズキーにDevice Control アプリを設定する必要があります。

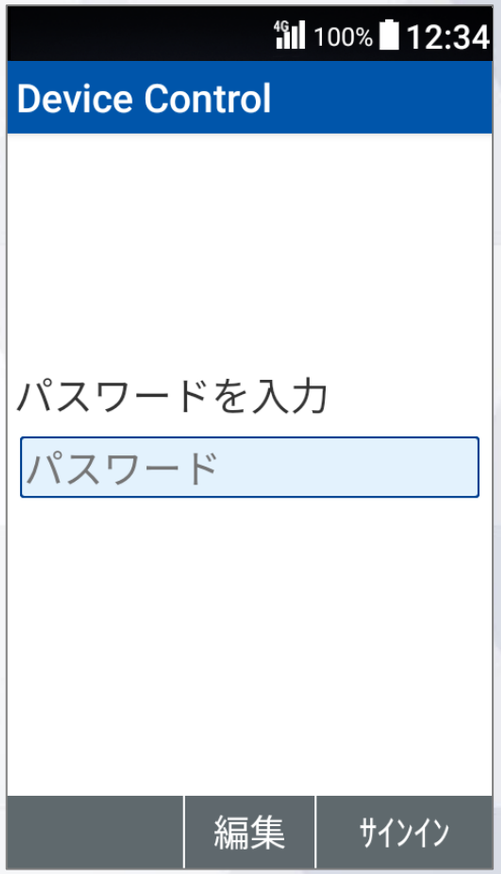
※ポリシー設定後は、カスタマイズキーからDevice Control アプリを外しても、機能制限は継続されます。
ただし、ポリシー変更やパスワード変更などで、Device Control アプリを改めて起動するには、Device Control アプリのカスタマイズキーへの再設定が必要です。



1 「設定」→「カスタマイズキー」→「登録するキーⅠ～Ⅲ」を選択

2 「Device Control」を選択

3 カスタマイズキーへの登録完了



P.10へ
DCアプリへのサインイン

4 登録したカスタマイズキー「Ⅰ～Ⅲ」を押下し、Device Control アプリが起動

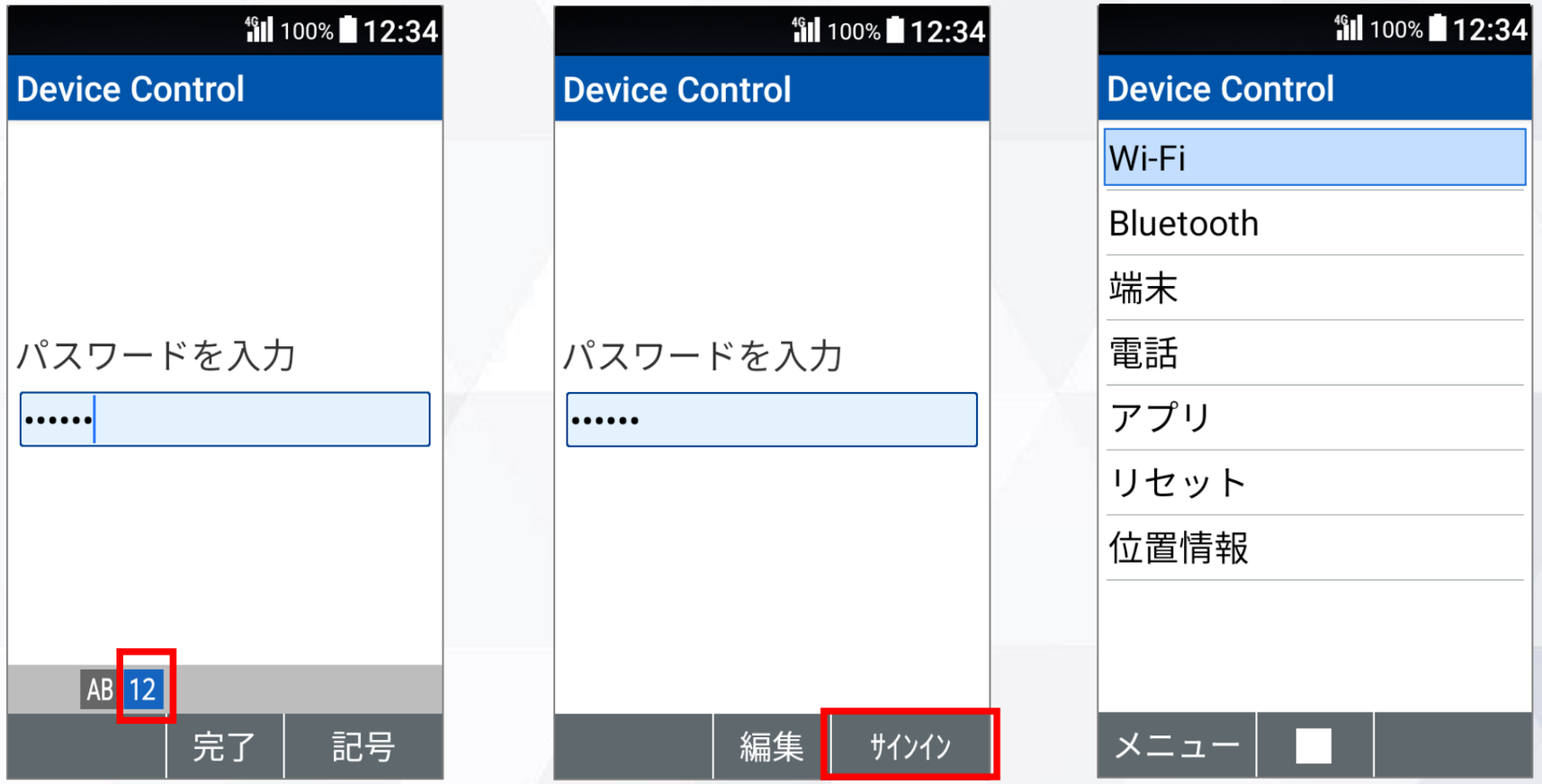
1. 事前設定　Device Control アプリへのサインイン

Device Control アプリへサインインするには、パスワードを入力する必要があります。

ご注意

従業員が設定変更しないよう、端末管理者にてパスワードを変更、管理することをおすすめします。
万一、パスワードを忘れた場合、Device Control アプリにサインインできなくなります。パスワードをお忘れで、改めてDevice Controlアプリにサインインするには、端末の初期化（リセット）をする必要があります。

P.9から続き



1 サインインするパスワードを入力
初期設定は000000

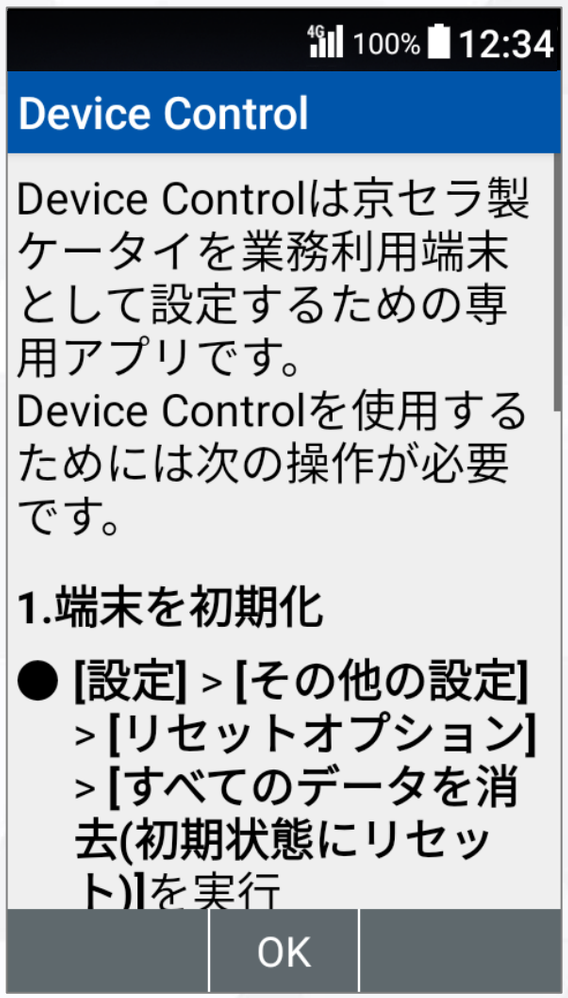
2 「**サインイン**」を選択

3 サインインが完了し、Device Control アプリをご利用になれます

（補足） Device Control アプリが有効化されていない場合

Device Control アプリが有効化されていない場合、Device Control アプリを起動すると、Device Control アプリ有効化の手順が表示されますので、P.8の手順に沿ってDevice Control アプリを有効化してください。

有効化されていない状態で
Device Controlアプリを起動すると、
有効化の手順が画面に表示されます



2. ポリシーの作成

BluetoothとSMSの無効化の機能制限を行う場合を例に、ポリシー作成の手順をご説明します。

1

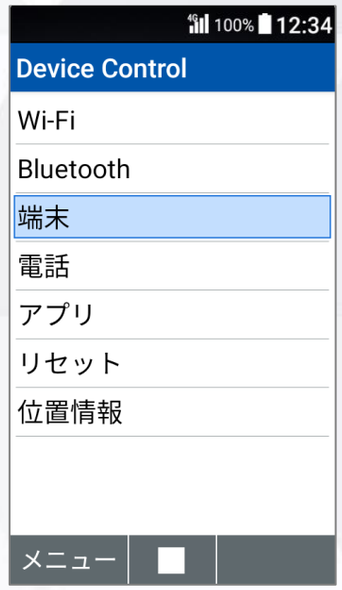
Device Control アプリへサインインすると、メインメニューが表示されます

2

「Bluetooth」→「Bluetoothの無効化」→「On」を選択

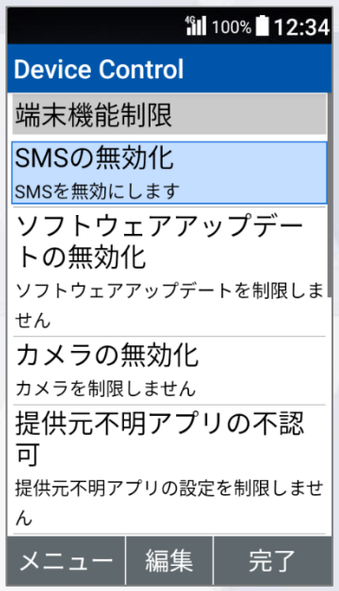
「すべてのBluetooth機能を無効にします」と表示されます

続けて、他の項目も設定する場合、「クリアキー」を押下し、再度メインニューから設定する項目を選択します



3

Device Control アプリのメインメニューから設定する項目を選択します



4

「端末」→「端末機能の制御」→「SMSの無効化」→「On」を選択

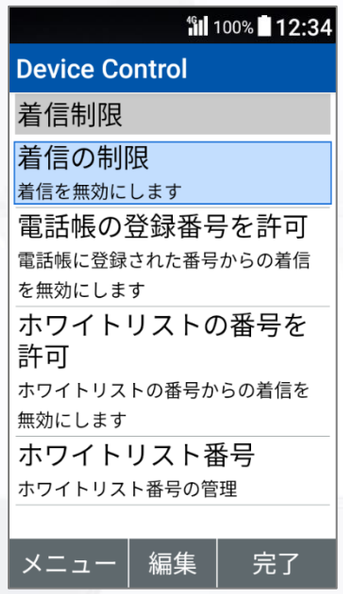
「SMSを無効にします」と表示されます

2. ポリシーの作成 （着信制限、発信制限）

着信制限、発信制限のポリシー作成の手順をご説明します。
着信制限、発信制限ともに手順は同様ですので、着信制限を例にご説明します。

1

Device Control アプリへサインインすると、メインメニューが表示されます

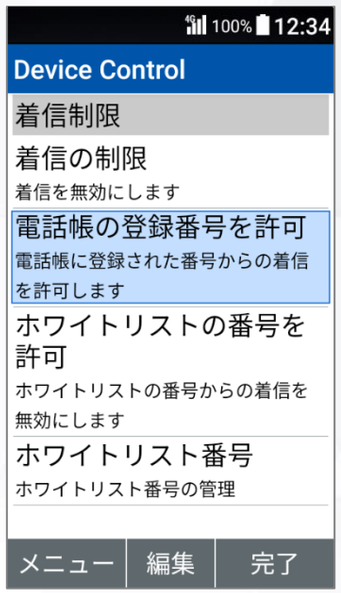


2

「電話」→「着信制限」→「着信の制限」→「On」を選択

「着信を無効にします」と表示されます

電話帳登録された番号からの着信を許可する場合

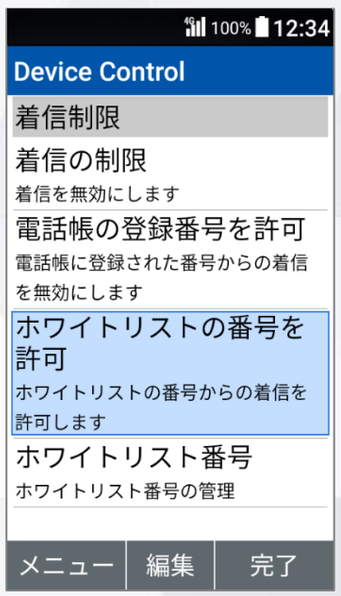


3

「電話帳の登録番号を許可」→「On」を選択

「電話帳に登録された番号からの着信を許可します」と表示されます

ホワイトリスト番号からの着信を許可する場合
(ホワイトリスト番号の編集はP14を参照)



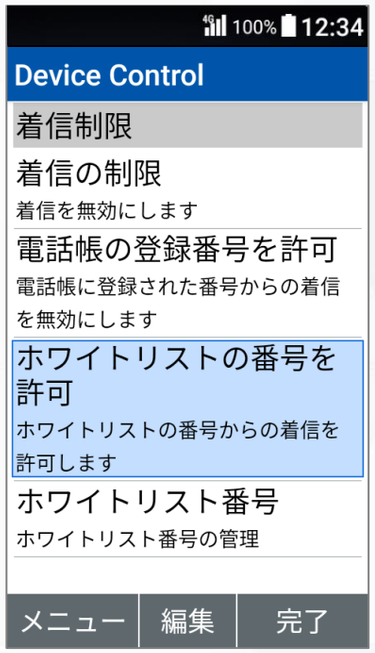
4

「ホワイトリストの番号を許可」→「On」を選択

「ホワイトリストの番号からの着信を許可します」と表示されます

2. ポリシーの作成 (着信制限、発信制限)ホワイトリスト番号の編集

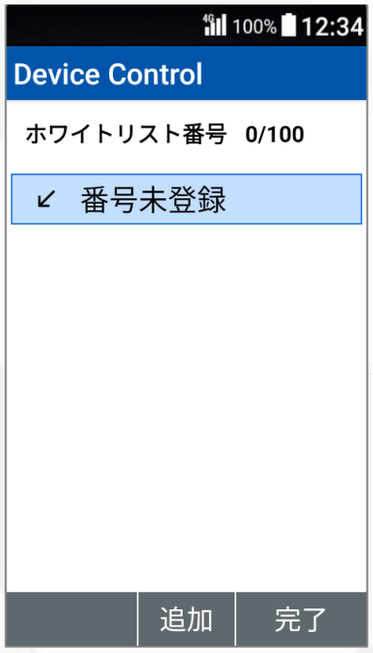
着信制限、発信制限のホワイトリスト番号の編集方法をご説明します。ホワイトリストに番号を登録すると、登録されたホワイトリスト番号からの着信、発信を許可することができます。



1

「電話」→「着信制限」→「着信の制限」→「On」を選択

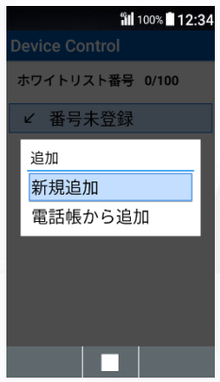
「着信を無効にします」と表示されます



2

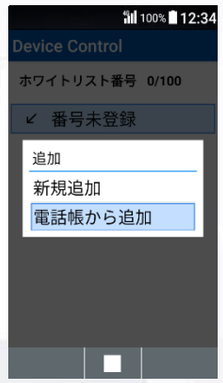
「ホワイトリスト番号」→「番号未登録」を選択

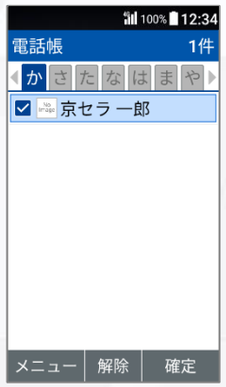
ホワイトリスト番号を新規に登録する場合



「新規追加」を選択

ホワイトリスト番号を電話帳から追加する場合



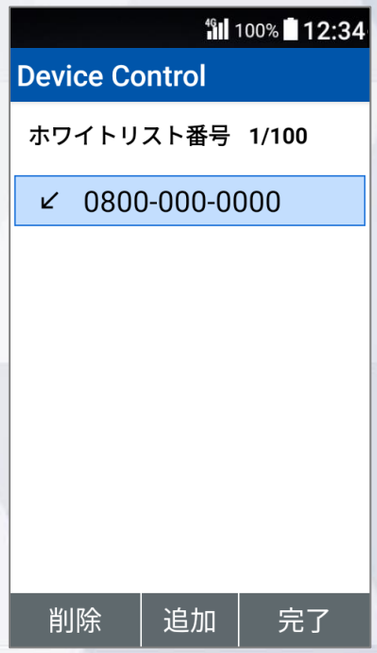


「電話帳から追加」を選択

3

4

ホワイトリストに登録したい電話番号を入力



5

さらに電話番号を追加する場合、「追加」を選択し、

4.と同様に電話番号を入力

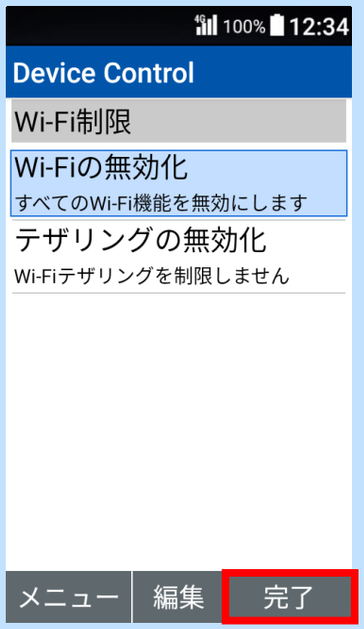
3. ポリシーの設定

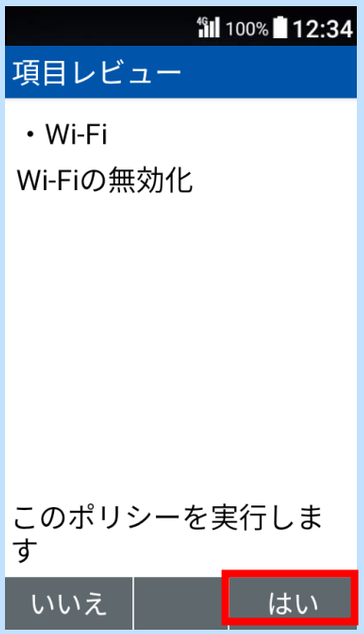
機能制限を完了するには、以下の手順でポリシーの設定が必要です。

2.ポリシー作成

P.12～14
に沿って操作

3.ポリシー設定





1
「完了」を選択

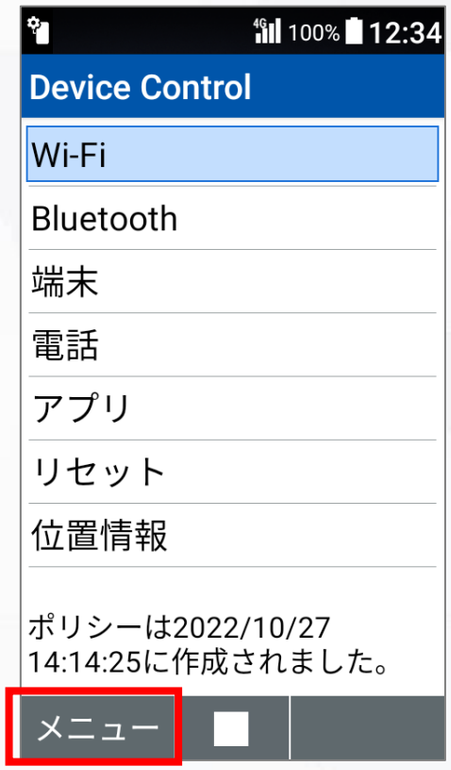
2
「はい」を選択

3
ポリシーの設定が完了

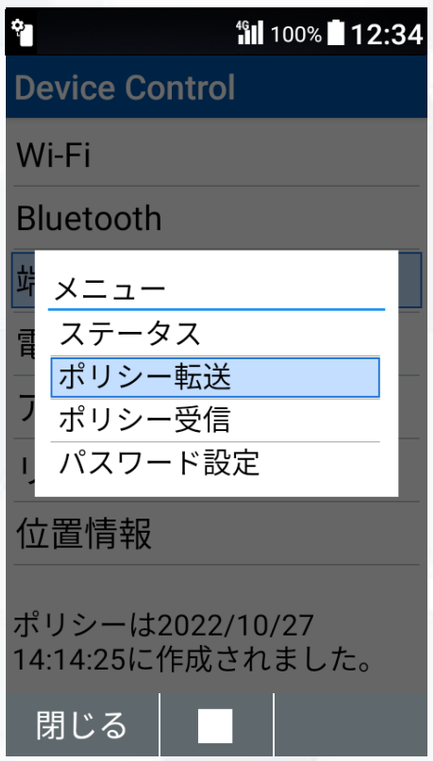
4. ポリシーの転送、受信（送信側端末）

ポリシーを他の端末に転送するには、送信側の端末にQRコード/ID番号の表示が必要です。

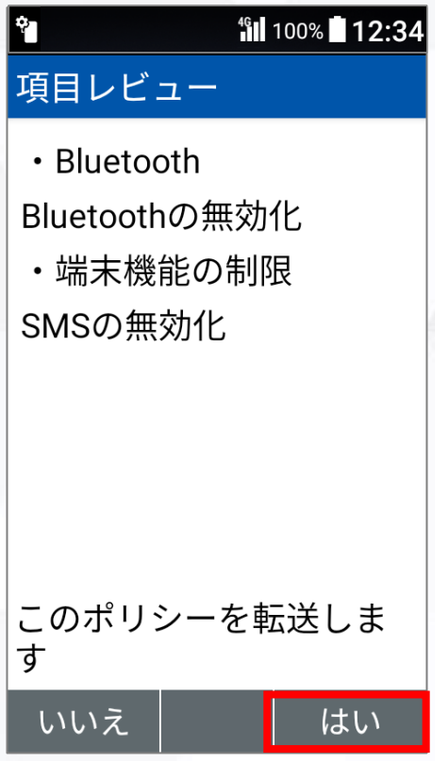
送信側端末の手順



1 Device Control アプリのメインメニューから「メニュー」を選択

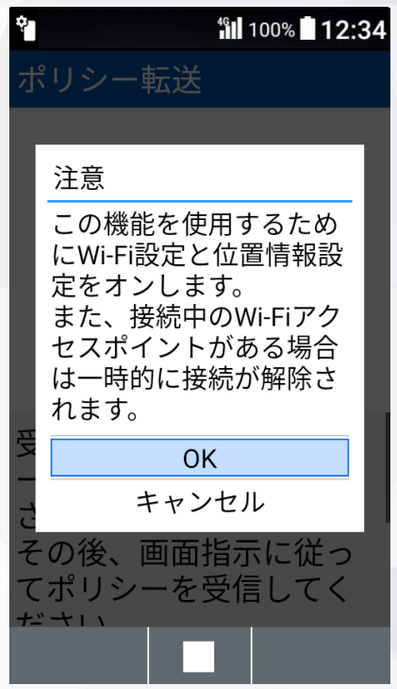


2 「ポリシー転送」を選択



3 「はい」を選択

Wi-Fiや位置情報がOFFの場合もポリシー転送のため、自動的にONになります



4 「OK」を選択

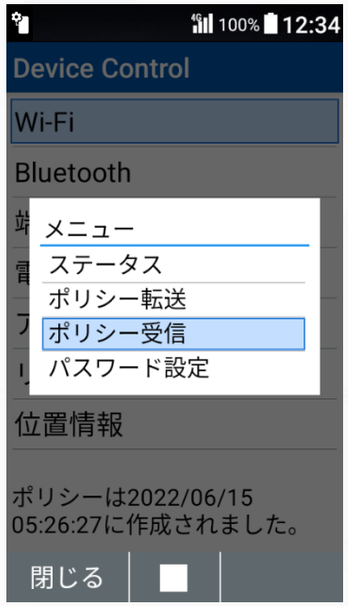
5 転送には、本画面に表示される**QRコード**または**ID番号**を利用します

4. ポリシーの転送、受信（受信側端末）

ポリシーを他の端末から受信するには、QRコードの読み取りまたは、ID番号の入力が必要です。
※ポリシーの受信側端末でもDevice Control アプリの有効化、サインインが必要です。

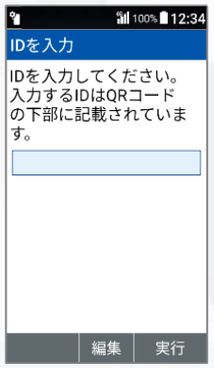
受信側端末の手順

受信側端末がカメラ搭載の場合



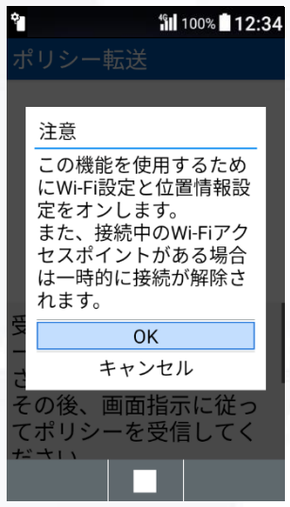
送信側端末に表示の
QRコードを読み取り

受信側端末がカメラ非搭載の場合

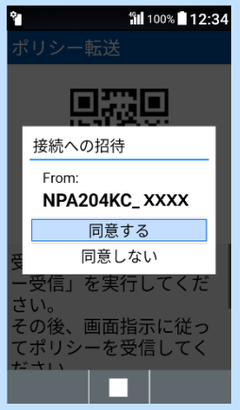


送信側端末に表示のID番号
を入力し、「実行」を選択

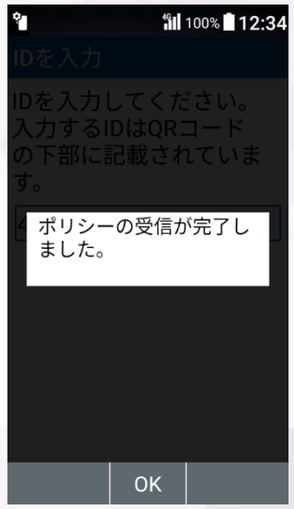
Wi-Fiや位置情報がOFFの場合も
ポリシー転送のため、自動的にONになります



送信側端末



受信側端末



機能制限を完了するには、
ポリシー受信後、受信側端末
でポリシー設定が必要です。

3.ポリシー設定

**P.15
に沿って操作**

1 Device Control アプリのメインメニューから「メニュー」→「ポリシー受信」を選択

2 QRコードの読み取り、またはID番号を入力

3 「OK」を選択

4 送信側端末に接続への招待画面が表示されるので、「同意する」を選択

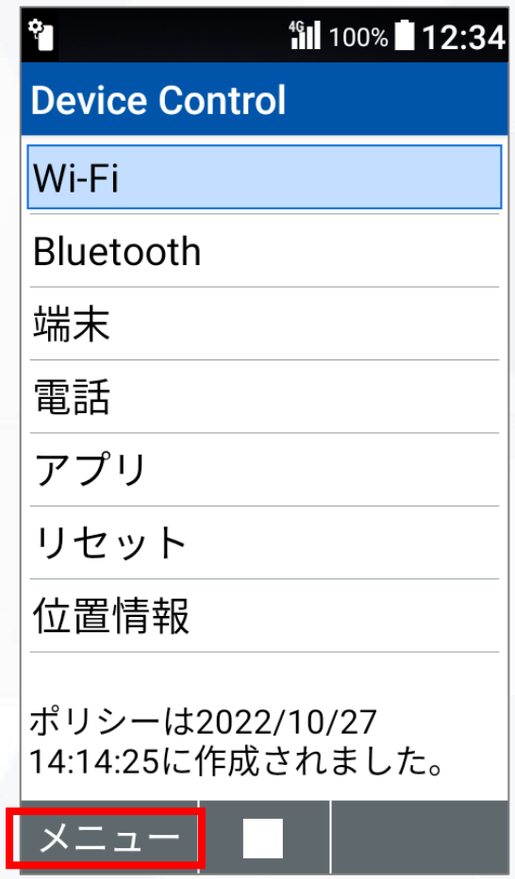
5 受信側端末で「ポリシーの受信が完了しました。」と表示されたら、「OK」を選択

サインインパスワードの変更

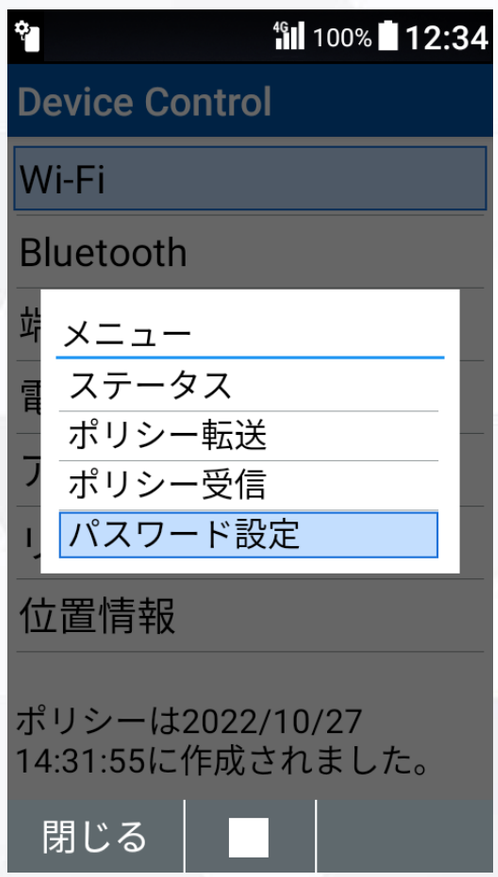
サインインパスワードを変更する手順は以下となります。初期値のパスワードは「000000」です。

ご注意

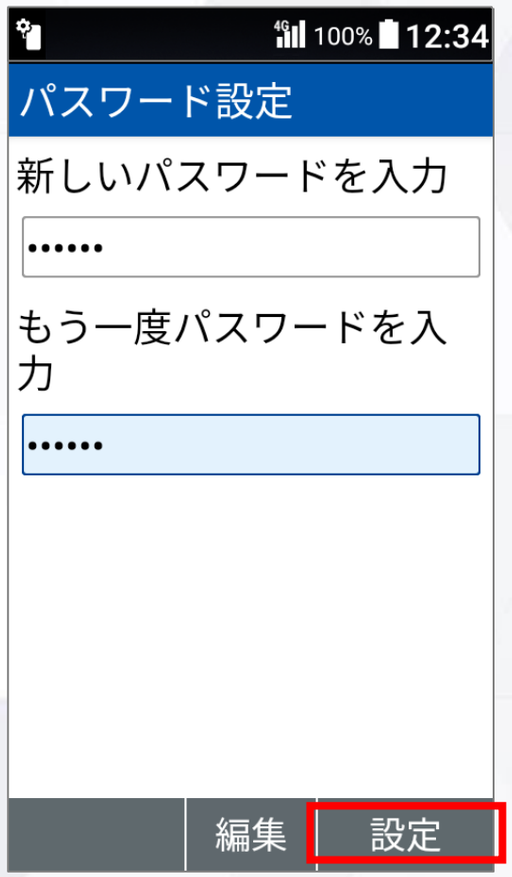
従業員が設定変更しないよう、端末管理者にてパスワードを変更、管理することをおすすめします。
万一、パスワードを忘れた場合、Device Control アプリにサインインできなくなります。パスワードをお忘れで、改めてDevice Controlアプリにサインインするには、端末の初期化（リセット）をする必要があります。



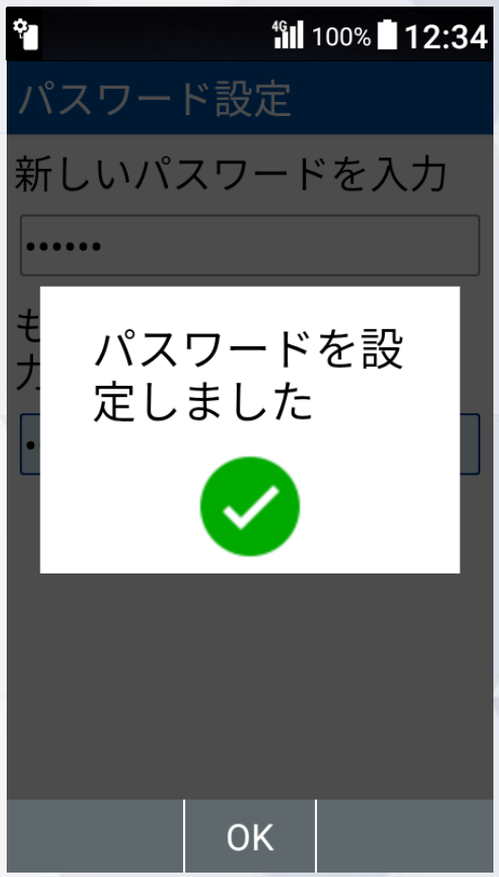
1 Device Control アプリのメインメニューから「メニュー」を選択



2 「パスワード設定」を選択



3 新しいパスワードを2回入力し、「設定」を選択

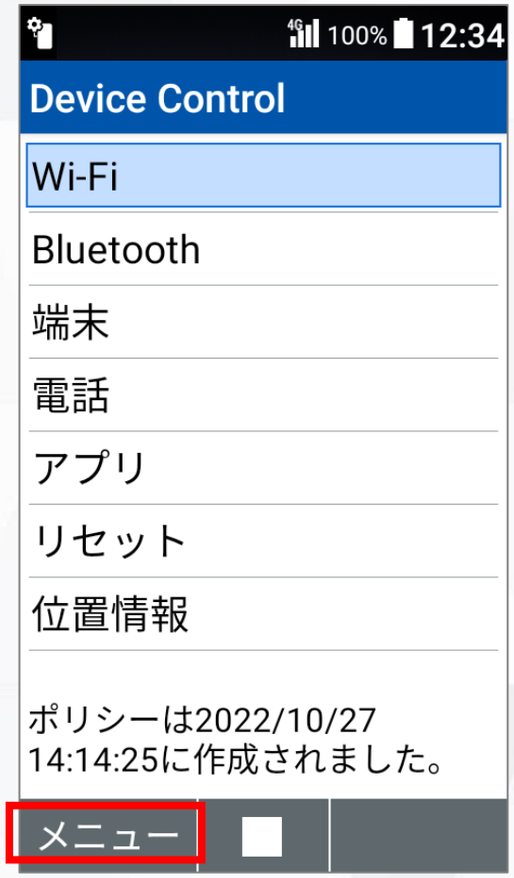


4 「OK」を選択

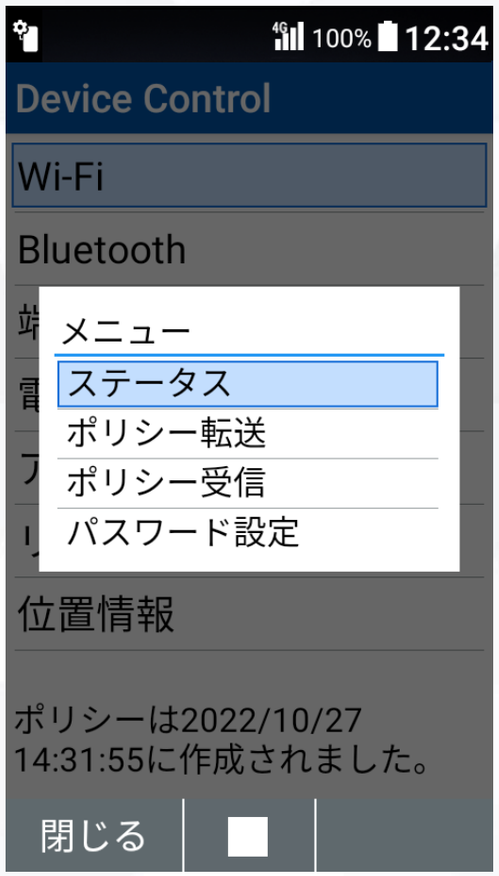
パスワードが変更されました

ステータスの確認方法

現在端末に設定されているポリシーをご確認頂けます。



1 Device Control アプリのメインメニューから「メニュー」を選択



2 「ステータス」を選択

3 「OK」を選択

機能制限中の端末動作

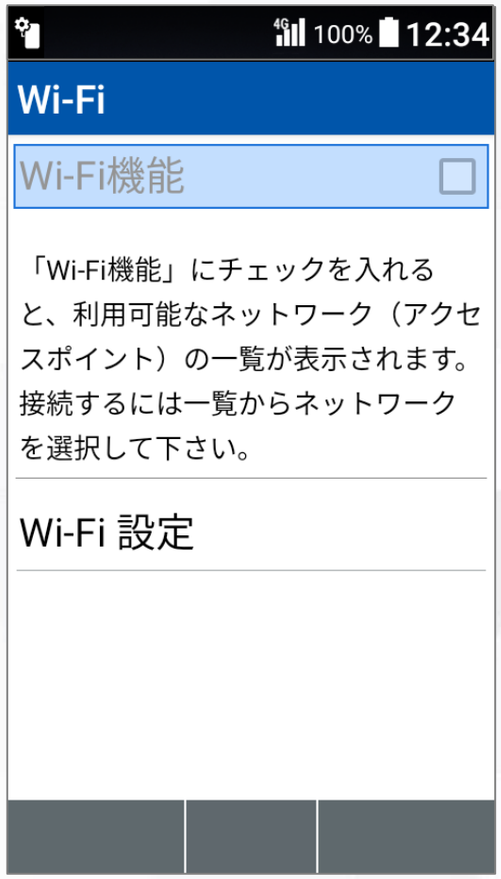
設定可能なポリシー一覧

Wi-Fi	Wi-Fiを無効化します。
	Wi-Fiテザリングを無効化します。
Bluetooth	Bluetoothを無効化します。
	Bluetoothテザリングを無効化します。
端末	SMSを無効化します。
	ソフトウェアアップデートを無効化します。 ＊ソフトウェアアップデートを無効化すると、セキュリティパッチ等が利用できなくなります。 また、ソフトウェアアップデートを無効化にしていても、故障した端末を修理し返却された際には、ソフトウェアアップデートが実施されている場合がございます。
	カメラを無効化します。
	提供元不明アプリを不認可にします。
	リカバリーモードを無効化します。 ＊リカバリーモードを無効化することで、リカバリーモードからデータの初期化を行うことも防ぐことができます。
	USBテザリングを無効化します。
	USB MTPを無効化します。
	SDカードの使用を制限します。
電話	モバイルネットワーク（音声ローミング/データローミング/モバイルデータ)を無効化します。
	電話帳の編集を無効にします。
	着信を制限することができます。電話帳の登録番号もしくはホワイトリストの登録番号からの着信を許可することも可能です。
	発信を制限することができます。電話帳の登録番号もしくはホワイトリストの登録番号への発信を許可することも可能です。
アプリ	アプリの起動を制限します。制限対象のアプリはリストで管理できます。
リセット	データの初期化を無効にします。
位置情報	位置情報の設定を**有効化**し、高精細モードに固定します。 ＊高精細モードとはGPS、Wi-Fi、Bluetooth、モバイルネットワークで現在値を特定する位置情報モードです。

端末の機能制限中の動作

Wi-Fi機能が制限されている場合を例に、機能制限中の端末動作をご説明します。

機能制限中は、Wi-FiをONに変更することができません。



「設定」→「無線・ネットワーク」→「Wi-Fi」を選択

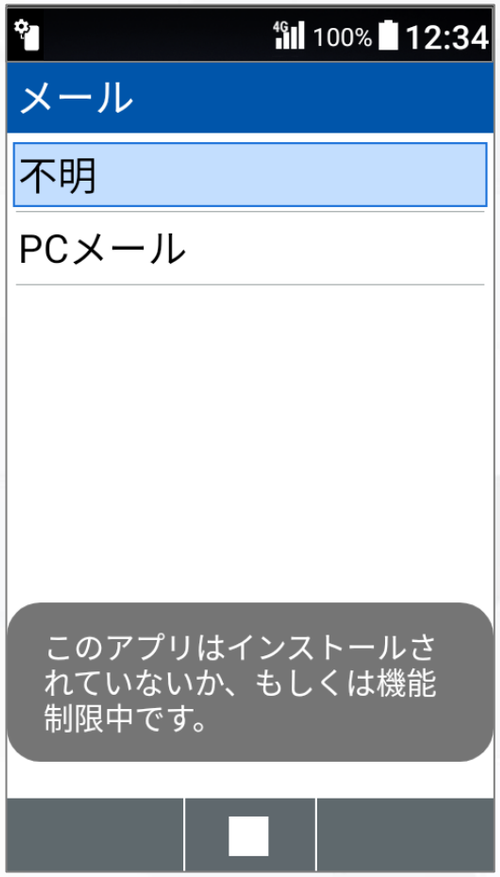
機能制限中は通知バーに  アイコンが表示されます。

待受け画面から「△キー」押下し通知バーを選択→「□」を選択

アプリの起動制限中の動作

「メール」の起動が制限されている場合を例に、アプリの起動制限中の端末動作をご説明します。

起動制限中は、メールを
起動することができません。



メインメニューから「メール」を
選択

機能制限中は通知バーに アイコンが
表示されます。

待受け画面から
「△キー」押下し
通知バーを選択
→「□」を選択

注意事項・
FAQ(よくあるご質問)

注意事項

1. Device Control アプリの有効化には、「初期状態にリセット」が必要で、端末内のすべてのデータが消去されます。そのため、従業員への端末配布前に、有効化を完了することをおすすめします。

2. 従業員が設定変更しないよう、端末管理者にてパスワードを変更、管理することをおすすめします。万一、パスワードを忘れた場合、Device Control アプリにサインインできなくなります。パスワードをお忘れで、改めてDevice Controlアプリにサインインするには、端末の初期化（リセット）をする必要があります。

3. 端末機能の「機能別ロック」とDevice Control アプリは同時に使用しないようご注意をお願い致します。「機能別ロック」を使用中に、Device Control アプリで「設定」アプリを起動制限すると、動作が不安定になる場合がございます。

4. 発信制限を行った場合、110などの緊急発信は制限されませんが、留守番電話などのネットワークサービスへの発信については制限されます。

FAQ（よくあるご質問）

Q：Device Control アプリにサインインするパスワードを忘れても、Device Control アプリで設定された機能制限は継続できますか？また、どのようにすればDevice Control アプリにサインインすることができますか？
⇒A：Device Control アプリで設定された機能制限は継続されます。
ただし、Device Control アプリに再度サインインするためには、端末の初期化を行い、パスワードの初期値を「000000」にする必要があります。端末の初期化を行うと、端末内の全てのデータが初期化され、Device Control アプリの機能制限もすべて解除されますので、ご注意ください。

Q：ポリシーは１台の端末から複数の端末に同時に転送、受信が可能ですか？
⇒A：複数の端末へ同時に転送、受信はできません。ポリシーは１台の端末から、１台の端末への転送、受信のみ可能です。

Q：初期化したら、機能制限は解除されますか？
⇒A： はい。Device Control アプリのすべての機能制限が解除されます。

Q：Device Control アプリにサインインするパスワードを、他端末に転送することはできますでしょうか？
⇒A：できません。

Q：端末に一度設定したポリシーを変更したい場合は、どうすればよいでしょうか。
⇒A：Device Control アプリにサインインし、改めてポリシーの変更、設定の完了を行ってください。

Q：SIMカードを入れなくても、Device Control アプリによる機能制限の設定はできますか？
⇒A：はい。できます。

ご利用に関する
お問い合わせ

お問い合わせについて

Device Control アプリのご利用に関して、
不明点がございましたら、以下の京セラホームページの「お問い合わせフォーム」からお問い合わせください。

https://www2.kyocera.co.jp/ce_sim_dcapp_inquiry.html

商標について

商標について

・「DIGNO」は、京セラ株式会社の登録商標です。
・「Bluetooth」は、Bluetooth SIG, Inc.の登録商標であり、京セラ株式会社はライセンスに基づいて使用しています。
・「Wi-Fi」はWi-Fi Allianceの登録商標です。
・「microSD」はSD-3C,LLCの商標です。
・文字変換は、オムロンソフトウェア株式会社のiWnn IMEを使用しています。

・その他、本書に記載している会社名、製品名は、各社の商標または登録商標です。
なお、本文中では、TM、®マークは表記していません。

◎製品仕様およびサービス内容は、予告なく変更することがあります。
◎掲載中の製品画像はすべてイメージです。さらに画面はハメコミ合成です。

改訂履歴

2022年9月13日　第1.0版発行