THE NEW VALUE FRONTIER

KYOCERA

GRATINA グラティーナ KYF42

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

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


au
KYF42
100%
10:07
8/30(月)
天気アプリ
ニュース
乗換・地図
アラーム
F1
電卓
F2
設定なし
F3
設定なし
GRATINA
ペア
メモ
アプリ
クリア
1 .@
2 か ABC
3 さ DEF
4 た GHI
5 な JKL
6 は MNO
7 ま PQRS
8 や TUV
9 ら WXYZ
* +小
0 わ をん。
コ」
F1
F2
F3
ポインター

従業員端末への機能制限設定までの流れ

1. 事前設定(P.7～11)

① Device Control アプリを有効化し、利用できるようにする。
※この処理は工場出荷状態からのみ実施可能です。
利用開始済み端末へ設定する場合、工場出荷状態への初期化が必要となります。

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. ポリシー転送、受信(P.15～16)

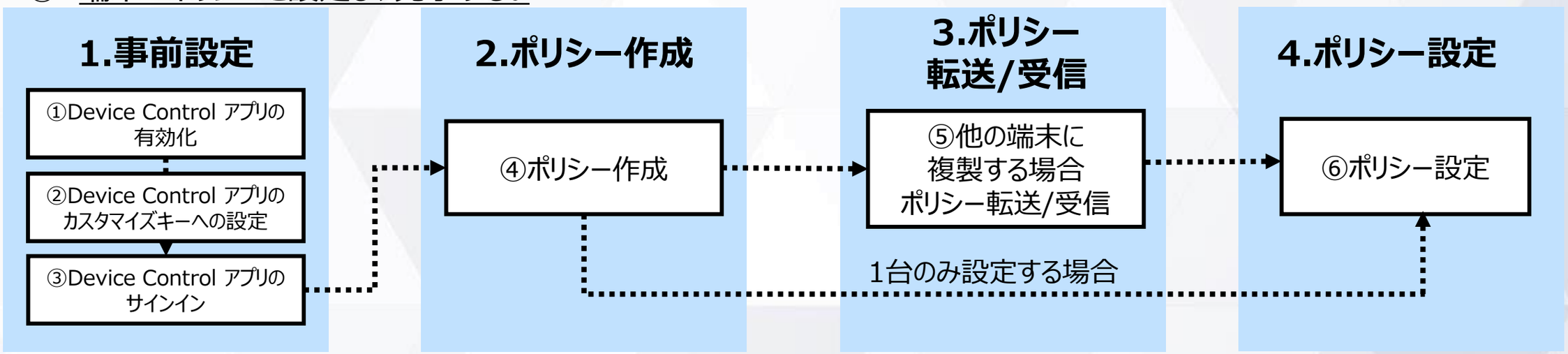
⑤ 他の端末へ機能制限を複製する場合、ポリシーの転送、受信を行う。
※Wi-Fi利用制限ポリシーを設定完了した端末からは、ポリシーの転送/受信は行えません。

4. ポリシー設定(P.17～18)

⑥ 端末へポリシーを設定し、完了する。

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。
  ※「機能別ロック」についてはauのホームページ掲載の本製品 取扱説明書（PDFファイル）をご覧ください。
- 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.19)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.20)ステータスの確認方法

1. 事前設定　Device Control アプリの有効化（工場出荷状態の場合）

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。

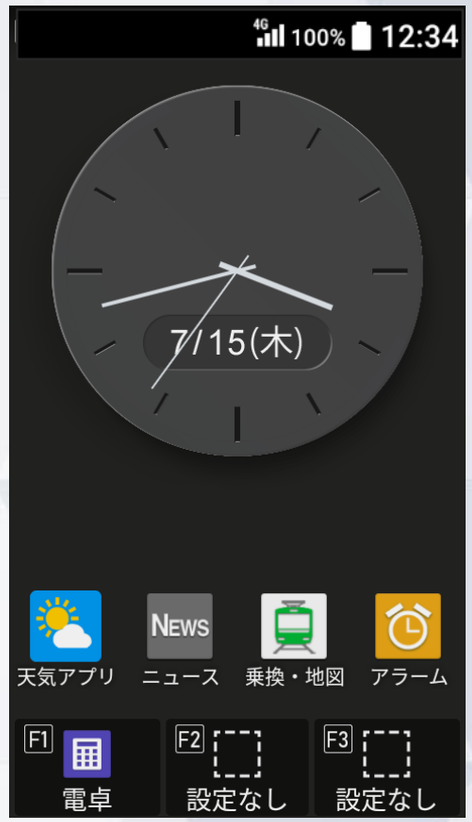
※既にDevice Control アプリをご利用の場合は、本操作は不要です。

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。

初めて本モデル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

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）

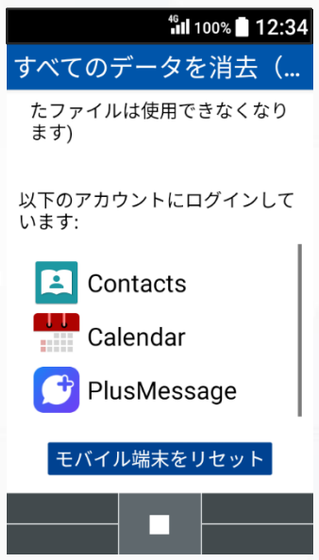
初めて、Device Control アプリをご利用いただく際には有効化の設定が必要です。

※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



1

待受画面で「■」→「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

「すべて消去」を選択

再起動

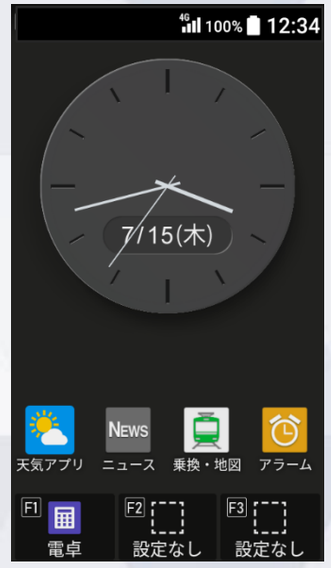
3

「＊＃＊＃＊＃」をコマンド入力

4

「はい」を選択

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



5

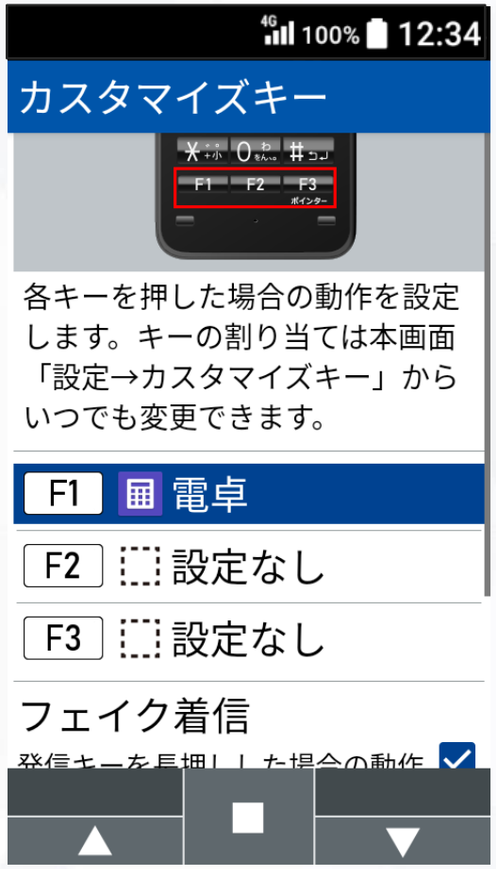
6

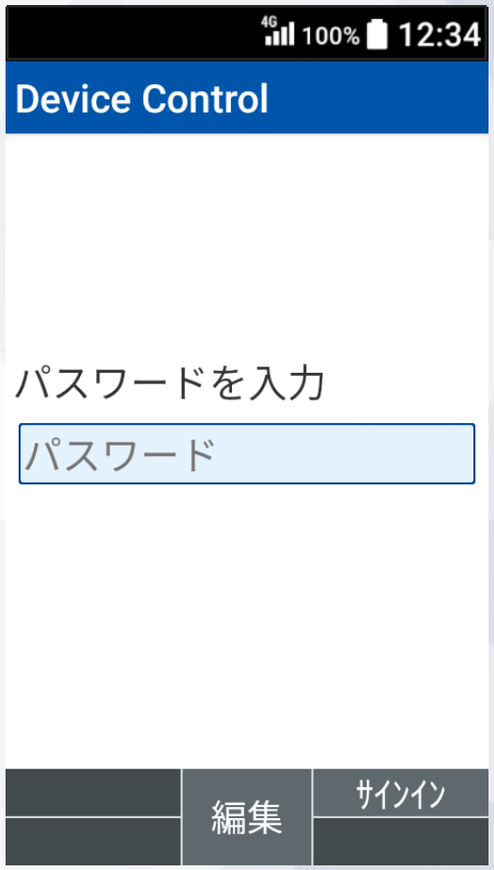
端末の初期設定完了後、待受画面が表示されます

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。





P.10へ
DCアプリへのサインイン

1 待受画面で「■」→「設定」→「カスタマイズキー」→「登録するキーF1～F3」を選択

2 「Device Control」を選択

3 カスタマイズキーへの登録完了

4 登録したカスタマイズキー「F1～F3」を押下し、Device Control アプリが起動

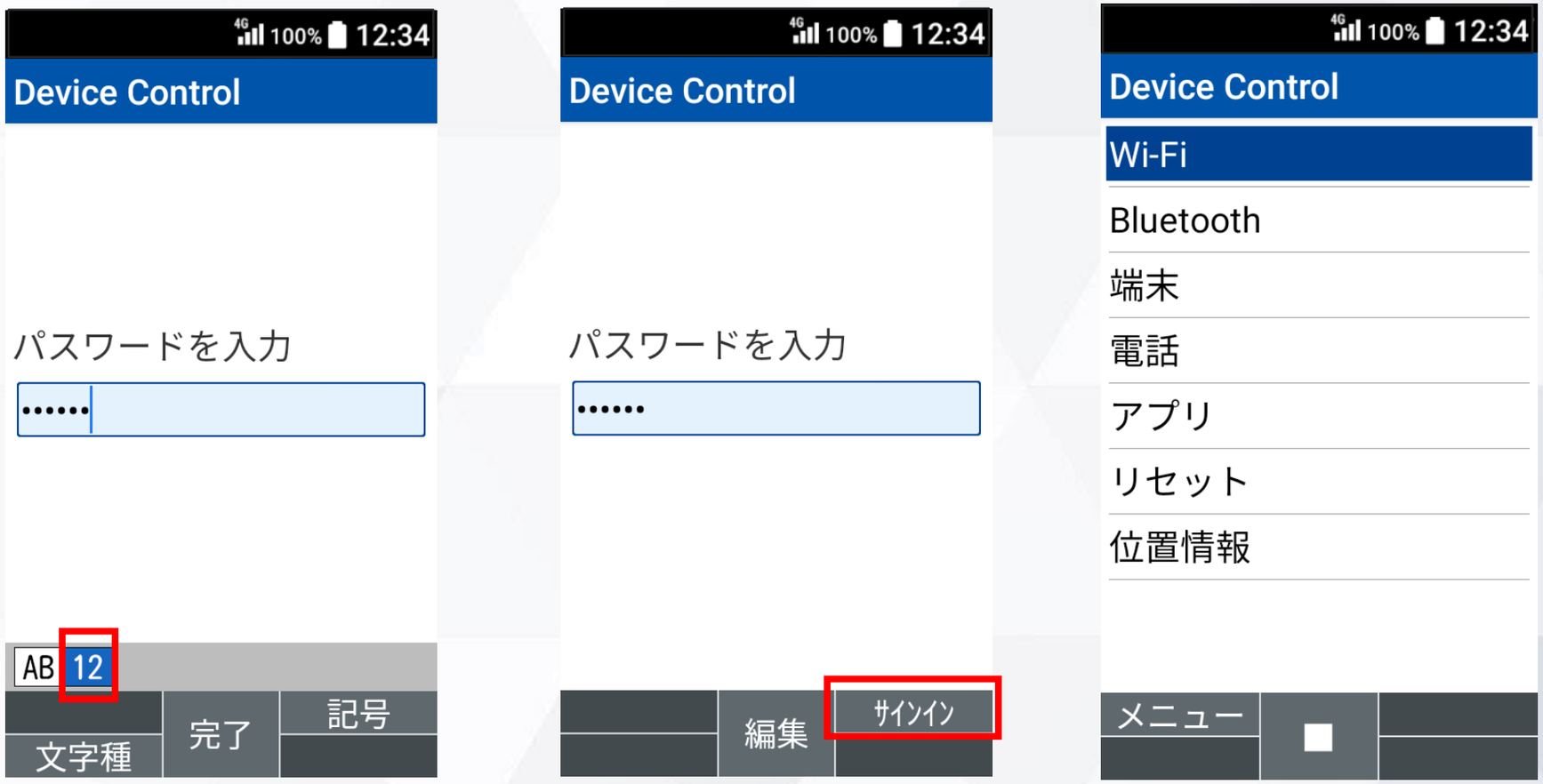
1. 事前設定　Device Control アプリへのサインイン

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。
また、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ので、ご注意ください。
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）を行い、パスワードを初期設定の「000000」にする必要があります。その際、すべてのデータが消去され、Device Controlアプリの設定も消去されます。

P.9から続き



1 サインインするパスワードを入力後、「■」を押下
初期設定は000000

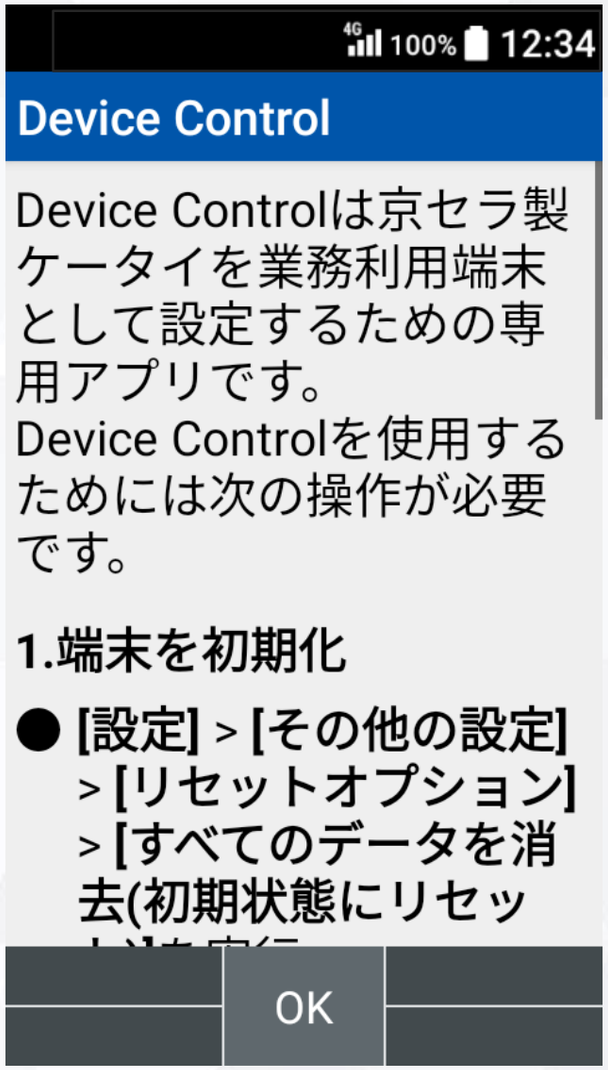
2 「**サインイン**」を選択

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は、 Device Control アプリの起動時、Device Control アプリ有効化の手順が表示されますので、P8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場合は
有効化の手順が画面に表示されます



2. ポリシーの作成

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

ご注意

Wi-Fiの無効化を実行した場合、本アプリのポリシーの転送はWi-Fi通信で行うため、転送することができなくなります。そこで、Wi-Fiの無効化のポリシーを転送する際は、以下手順に沿って、ポリシー設定を実行する前に、必ずポリシー転送（P15,16）を行ってください。

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

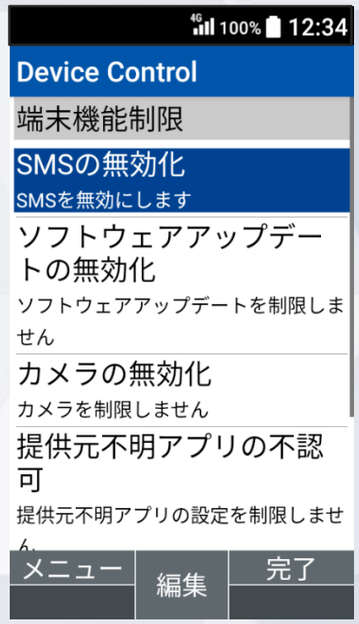
「すべてのBluetooth機能を無効にします」と表示されます

「クリアキー」を押下

続けて、他の項目も設定する場合、再度メインメ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）

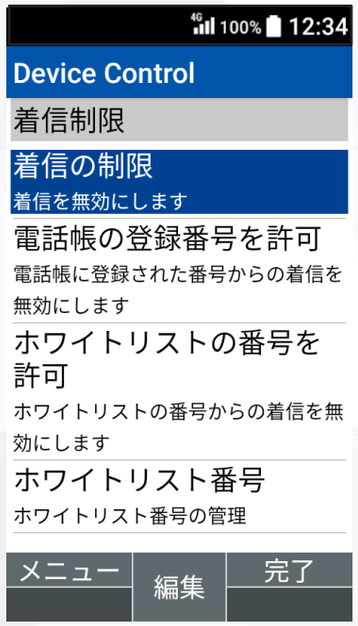
着信制限、発信制限のポリシー作成の手順をご説明します。
着信制限、発信制限ともに手順は同様ですので、着信制限を例にご説明します。

ご注意

Wi-Fiの無効化を実行した場合、本アプリのポリシーの転送はWi-Fi通信で行うため、転送することができなくなります。そこで、Wi-Fiの無効化のポリシーを転送する際は、以下手順に沿って、ポリシー設定を実行する前に、必ずポリシー転送（P15,16）を行ってください。

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

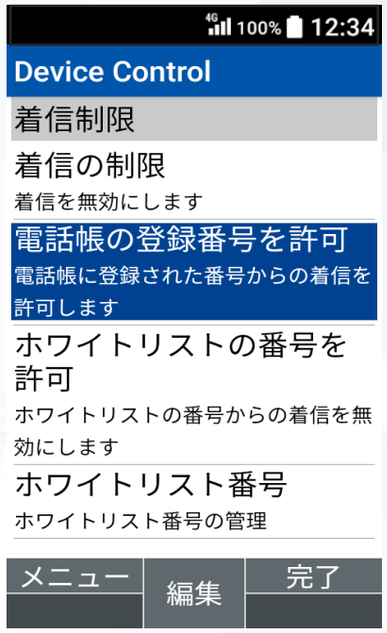


2

「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制限の対象外とする場合

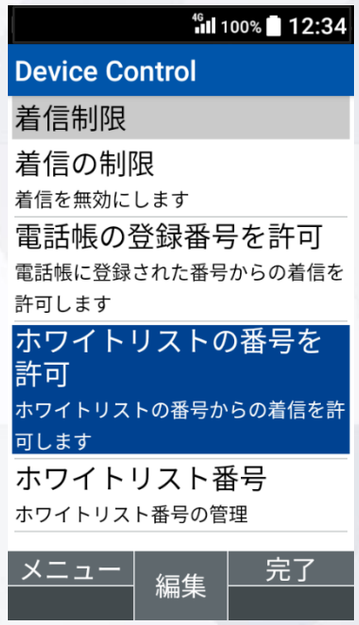


3

「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制限の対象外とする場合
※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

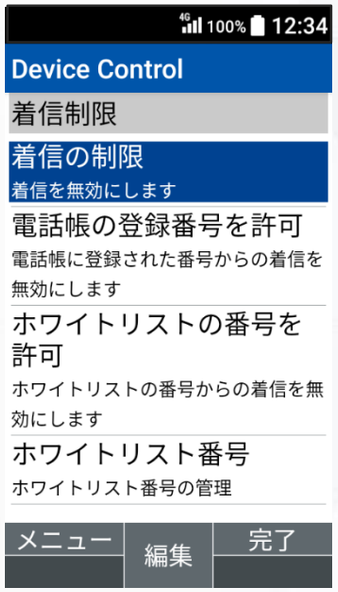
2. ポリシーの作成 (着信制限、発信制限)ホワイトリスト番号の編集

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制限、発信制限を対象外とすることができます。

ご注意

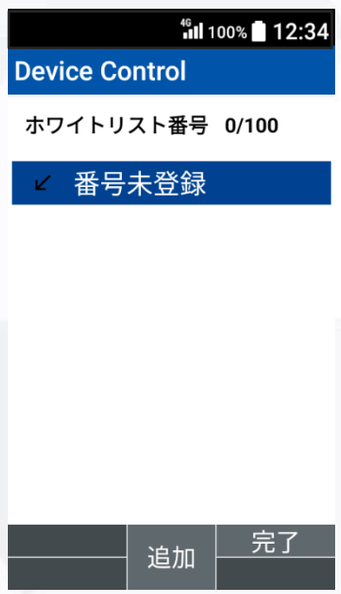
Wi-Fiの無効化を実行した場合、本アプリのポリシーの転送はWi-Fi通信で行うため、転送することができなくなります。そこで、Wi-Fiの無効化のポリシーを転送する際は、以下手順に沿って、ポリシー設定を実行する前に、必ずポリシー転送（P15,16）を行ってください。

ホワイトリスト番号を新規に登録する場合



「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



「ホワイトリスト番号」→「番号未登録」を選択

「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

ホワイトリストに追加したい電話番号を登録

さらに電話番号を追加する場合、「追加」を選択し、3.4.と同様の手順で電話番号を登録

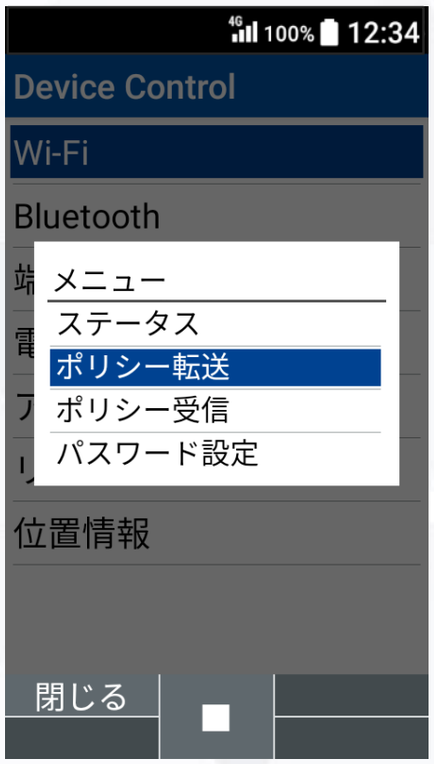
3．ポリシーの転送、受信（送信側端末）

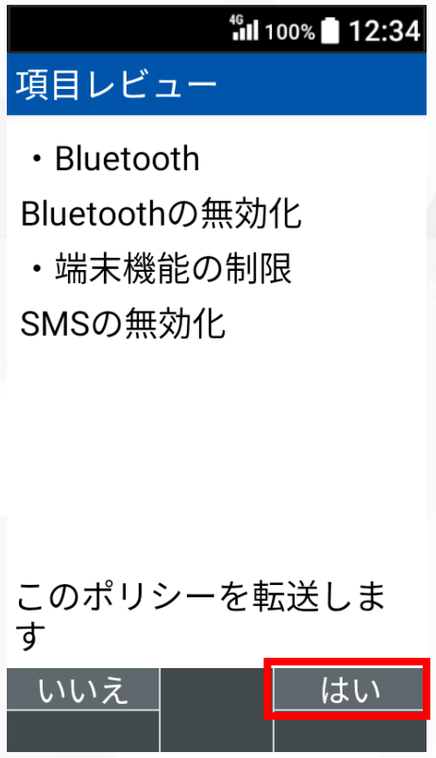
作成したポリシーを他の端末に転送するには、送信側の端末にQRコード/ID番号の表示が必要です。

ご注意

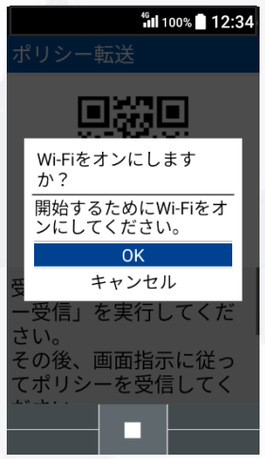
ポリシーの転送、受信の際、Wi-Fi通信を利用するため周囲に多くのWi-Fi機器がある場合は干渉により接続品質が低下する場合があります。受信失敗が続く場合はWi-Fi機器から離れた場所にて再度お試しください。

送信側端末の手順



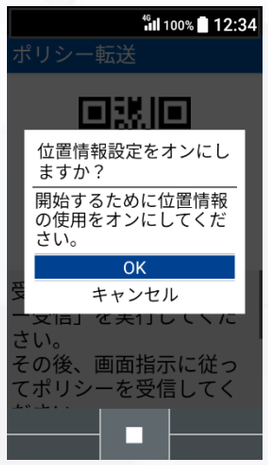


（Wi-FiがOFF時に表示）



Wi-FiをONに設定後、「クリアキー」を押下

（位置情報がOFF時に表示）



位置情報をONに設定後、「クリアキー」を押下

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

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**

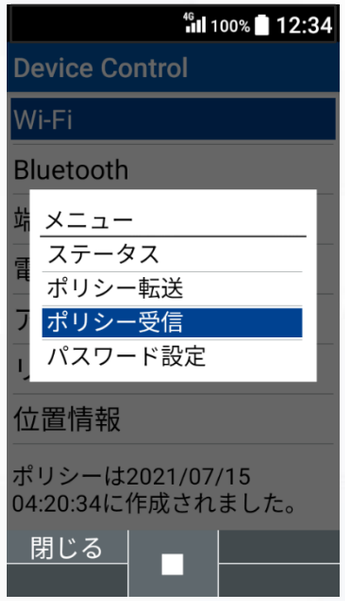
3．ポリシーの転送、受信（受信側端末）

ポリシーの受信側端末にもあらかじめ、Device Control アプリの有効化、サインインが必要です。

ご注意

ポリシーの転送、受信の際、Wi-Fi通信を利用するため周囲に多くのWi-Fi機器がある場合は干渉により接続品質が低下する場合があります。受信失敗が続く場合はWi-Fi機器から離れた場所にて再度お試しください。

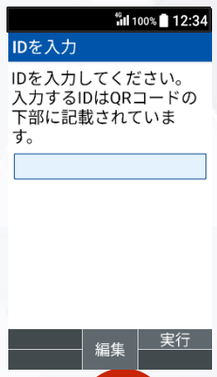
受信側端末の手順



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

送信側端末に表示のQRコードを読み取ってください

カメラ無しモデルの場合

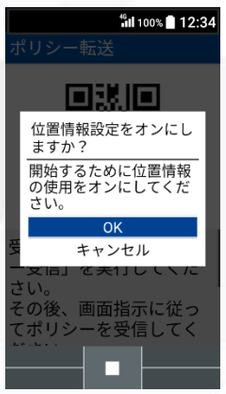


2 送信側端末に表示の「QRコード」読み取り、またはID番号を入力してください。

（Wi-FiがOFF時に表示）

Wi-FiをONに設定後、「クリアキー」を押下

（位置情報がOFF時に表示）



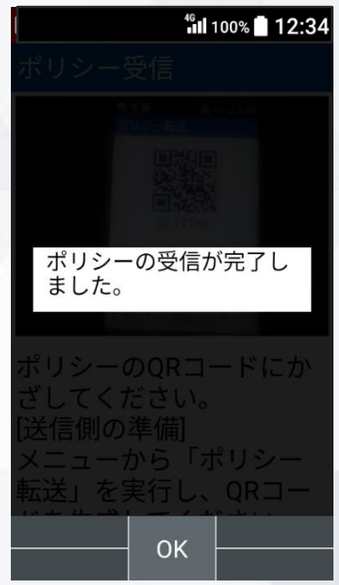
位置情報をONに設定後、「クリアキー」を押下

3 「OK」を選択

受信側

送信側

4 送信側端末でWi-Fi接続確認画面が表示されますので、「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

機能制限の設定を完了するには、送信側、受信側双方にポリシーの設定が必要です

4.ポリシー設定

P.17～18に沿って操作

4. ポリシーの設定

機能制限の設定を完了するには、ポリシー転送の送信側、受信側の双方にポリシーの設定が必要です。ポリシーの設定を完了する手順は以下となります。

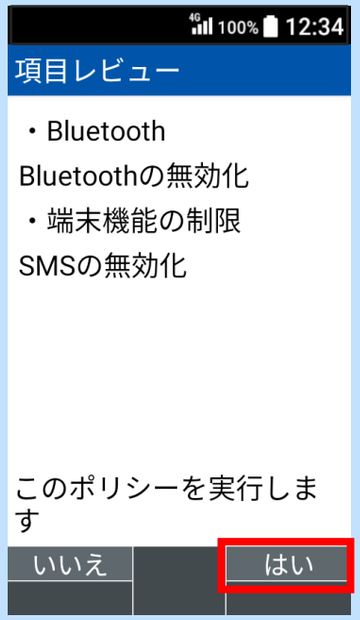
2.ポリシー作成

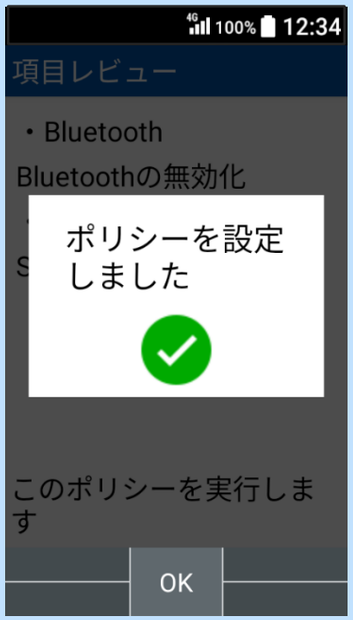
P.12～14 に沿って操作

3.ポリシー転送/受信

P.15～16 に沿って操作

4.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．ポリシーの設定（ポリシーにWi-Fi無効化を含む場合）

ポリシーにWi-Fiの無効化を含む場合の、ポリシーの設定の手順は以下となります。

ご注意

Wi-Fiの無効化を実行した場合、本アプリのポリシーの転送はWi-Fi通信で行うため、転送することができなくなります。そこで、Wi-Fiの無効化のポリシーを転送する際は、以下手順に沿って、ポリシー設定を実行する前に、必ずポリシー転送（P15,16）を行ってください。

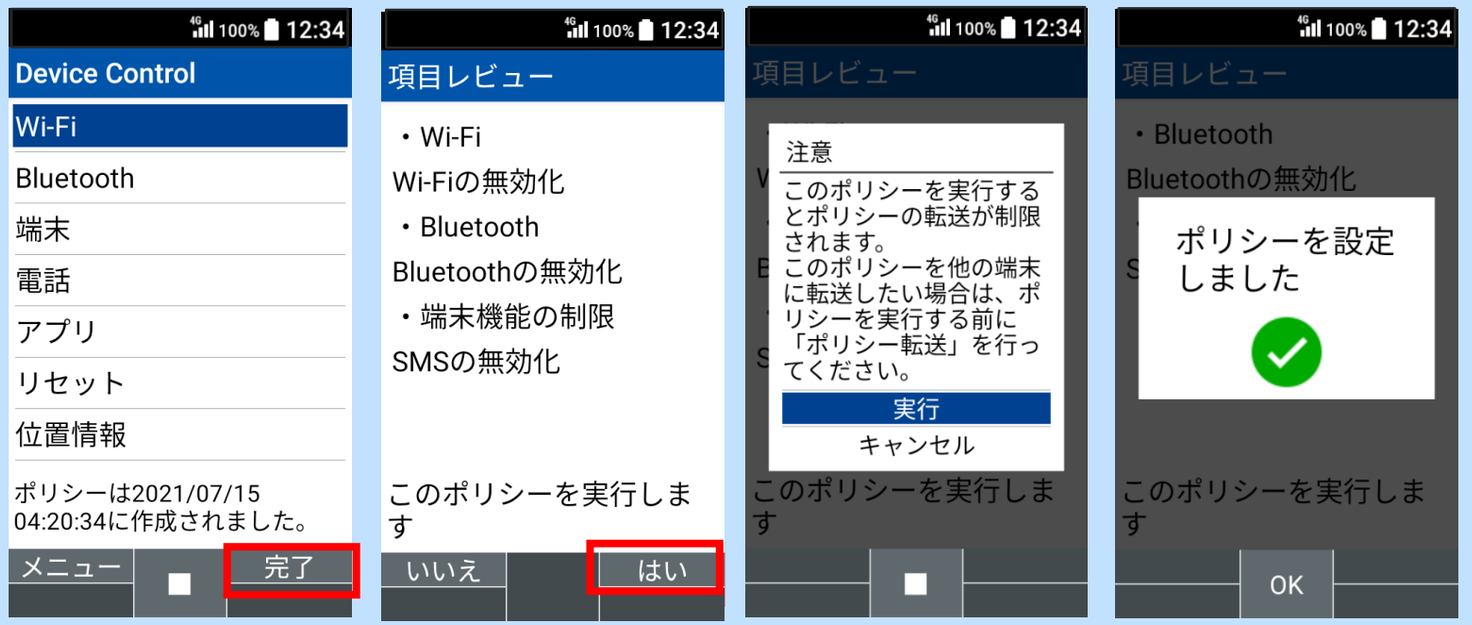
2.ポリシー作成

P.12～14 に沿って操作

3.ポリシー転送/受信

P.15～16 に沿って操作

4.ポリシー設定



1 「完了」を選択

2 「はい」を選択

3 「実行」を選択

4 ポリシーの設定が完了

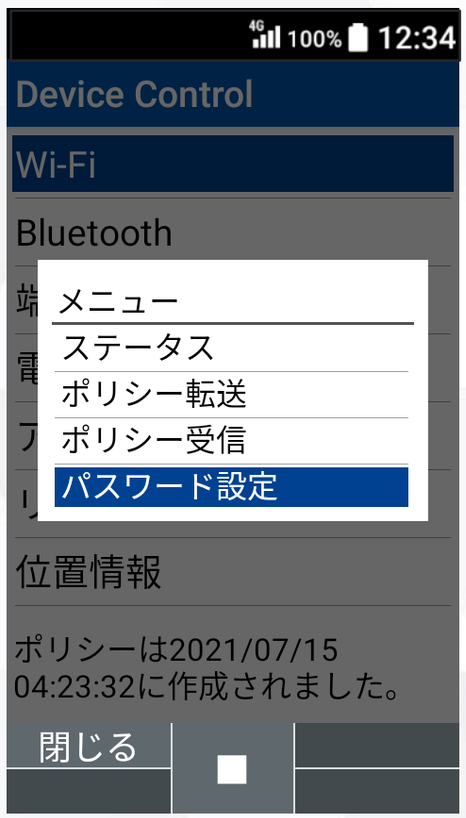
サインインパスワードの変更

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。

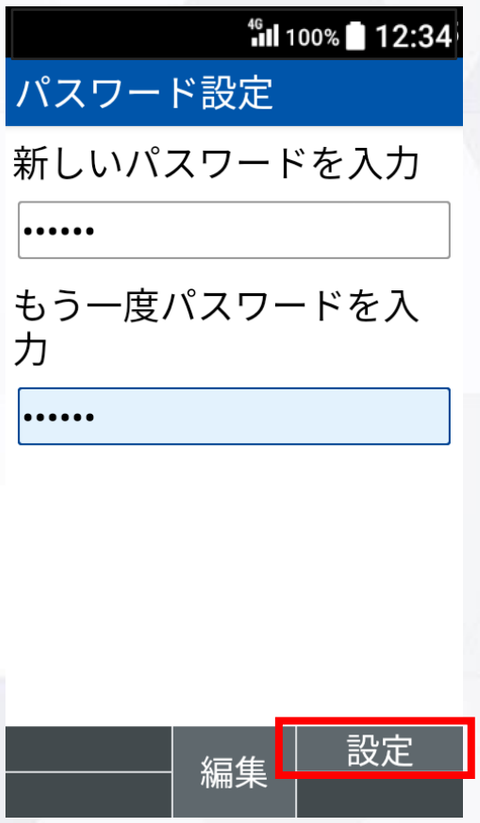
ご注意

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。
また、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ので、ご注意ください。
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）を行い、パスワードを初期設定の「000000」にする必要があります。その際、すべてのデータが消去され、Device Controlアプリの設定も消去されます。

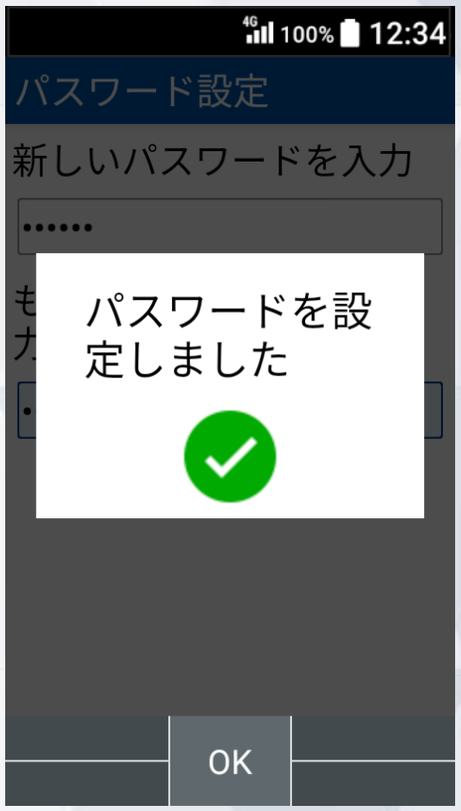
1 Device Control アプリのメインメニューから「メニュー」を選択



2 「パスワード設定」を選択



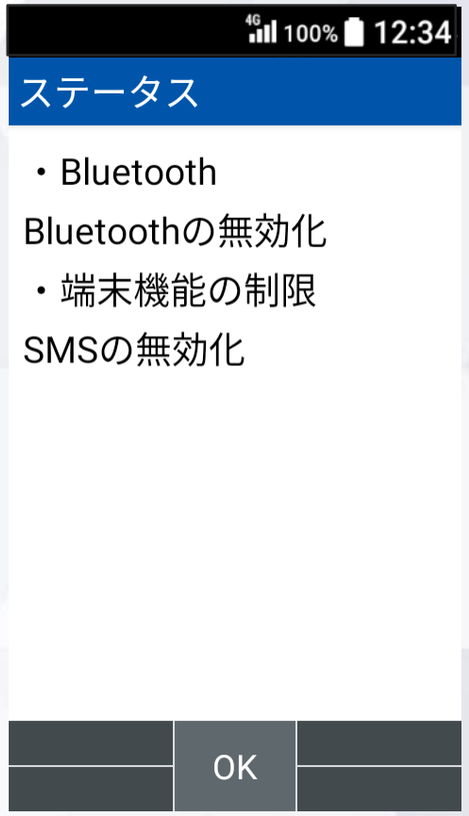
3 新しいパスワードを2回入力し、「設定」を選択



4 「OK」を選択

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


au
KYF42
100%
10:07
8/30(月)
天気アプリ
ニュース
乗換・地図
アラーム
F1
電卓
F2
設定なし
F3
設定なし
GRATINA
メモ
クリア
F1
F2
F3
ポインター

設定可能なポリシー一覧

Wi-Fi	W-Fiの利用を無効にします。
Bluetooth	Bluetoothの利用を無効にします。
端末	SMSの利用を無効にします。
	ソフトウェアアップデートを無効にします。 ＊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。
	カメラの利用を無効にします。
	提供元不明アプリを不認可にします。
	SDカードの利用を無効にします。
電話	音声ローミングの利用を無効にします。
	データローミングの利用を無効にします。
	モバイルデータの利用を無効にします。
	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。電話帳登録されている番号、もしくはホワイトリストに登録した番号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。電話帳登録されている番号、もしくはホワイトリストに登録した番号を許可と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	端末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。

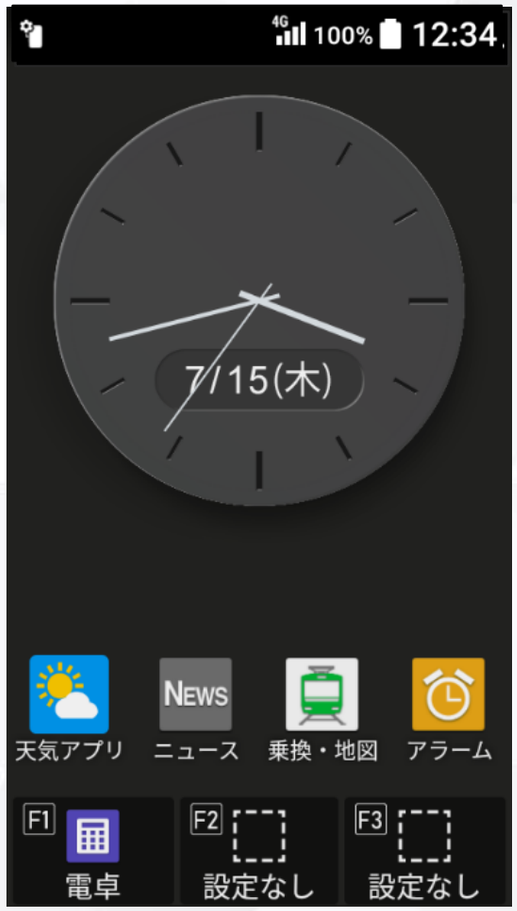
端末の機能制限中の動作

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の設定をONに変更することができません。

待受画面で「■」→「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。



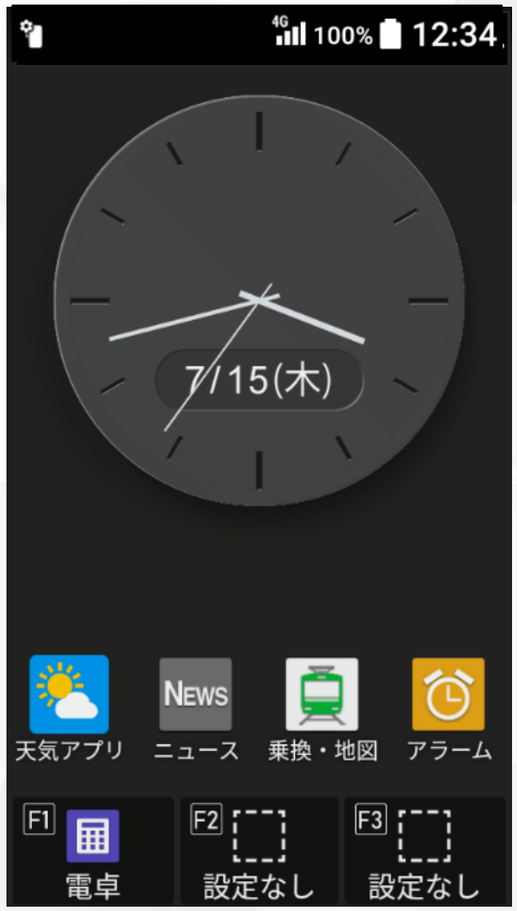
待受画面で「↑」キーを2回押下→「■」を押下

アプリの起動制限中の動作

カレンダー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、「不明」と表示され、起動することができません。

待受画面で「■」→「ツール」を選択



起動制限中は通知バーにアイコンが表示されます。

待受画面で「↑」キーを2回押下→「■」を押下

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。
また、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ので、ご注意ください。
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）を行い、パスワードを初期設定の「000000」にする必要があります。その際、すべてのデータが消去され、Device Controlアプリの設定も消去されます。

3. Wi-Fiの無効化を実行した場合、本アプリのポリシーの転送はWi-Fi通信で行うため、転送することができなくなります。そこで、Wi-Fiの無効化のポリシーを転送する際は、ポリシー設定を実行する前に、必ずポリシー転送を行ってください。

4. ポリシーの転送、受信の際、Wi-Fi通信を利用するため周囲に多くのWi-Fi機器がある場合は干渉により接続品質が低下する場合があります。受信失敗が続く場合はWi-Fi機器から離れた場所にて再度お試しください。

5. 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。※「機能別ロック」についてはauのホームページ掲載の本製品 取扱説明書（PDFファイル）をご覧ください。

6. 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 アプリに再度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。
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）を行い、パスワードを初期設定の「000000」にする必要があります。その際、すべてのデータが消去され、Device Controlアプリの設定も消去されますので、ご注意ください。

Q：Device Control アプリで「データの初期化の無効化」の機能制限をした後に、サインインするパスワードの紛失などで、端末の初期化をしたい場合はどうすればよいでしょうか。

⇒A：「データの初期化の無効化」の機能制限をしている場合は、端末の初期化（リセット）ができませんので、
auショップに端末をお持ち込みいただき、端末の初期化を行ってください。

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。

FAQ（よくあるご質問）

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：テザリング機能を制限するには、どのようにすれば良いですか？

⇒A: テザリング機能のみをDevice Controlアプリで制限することはできません。
「設定」アプリの起動を制限することにより、テザリング機能の設定変更を制限することが可能ですが、「設定」アプリのすべての設定の変更ができなくなります。

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。

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、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://www.kyocera.co.jp/prdct/telecom/office/phone/inquiry/dcapp-kyf42.html

商標について

商標について

・「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2月　第1.0版発行　※Device Control Ver.1.4.4