

Device Control アプリ

取扱説明書

January 2022, 1st Edition

目次

目次	1
はじめに	2
Device Control アプリとは	2
記載内容について	2
準備	2
DC アプリ対応モデル	3
管理用端末の準備	4
QR コードを利用して DC アプリをインストールする	4
ポリシー	6
ポリシーの作成	6
ポリシーの編集	6
ポリシーの確認	7
ポリシーの名前の変更	7
ポリシーの削除	8
詳細設定	8
配布用端末の準備	10
DC アプリのインストール	10
配布用端末へのポリシーの転送	12
QR コードを使用した配布用端末へのポリシーの転送	12
配布用端末のポリシー管理	12
DC アプリの管理	14
アプリのアップデート	14
登録ユーザーの削除	14
アプリのアンインストール	14
ポリシー作成例	15
重要な注意事項	15
設定例 1	15
設定例 2	15
ポリシーの制限と機能	17

はじめに

Device Control アプリとは

Device Control アプリ（以下「DC アプリ」と表記します）は小規模オフィス向けに開発した端末管理アプリです。京セラの MDM 機能を利用することで、携帯電話の機能を制限し、業務に最適な状態にすることができるサポートツールです。誤った設定や設定の組み合わせは意図しない結果を招き、端末の動作を停止させる可能性があります。

端末の制御は主に企業の IT 管理者またはアカウント管理者の端末管理支援を目的としています。これは、すべての端末が一貫した制御された構成を持つことを保証するための費用対効果の高い方法を提供します。

記載内容について

端末を管理するための方法及び、それを配布用端末へ配布するために必要な基本情報を提供します。

- 管理用端末の準備
 - 管理者がポリシーを設定します
- ポリシー の作成
 - 特定の端末構成（機能の有効/無効）を作成します
- 配布用端末の準備
 - 作業員へ配布用に管理用端末のセットアップ内容を複製します
- 配布用端末へポリシーの転送

この取扱説明書は、DC アプリ Ver. 4.0.0 を元に記載しています。この取扱説明書に記載の操作方法は、端末のソフトウェアバージョンやアプリのバージョンによって変わることがあります。

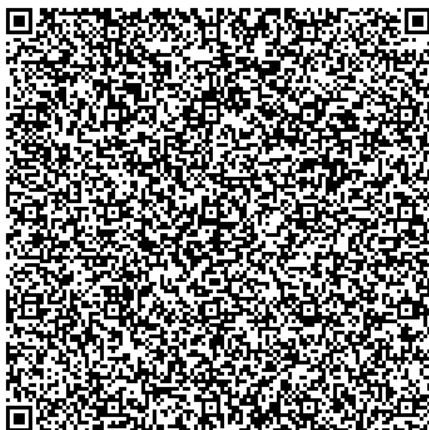
ご注意： DC アプリを立ち上げる時、ホーム画面から [Device Control] をタップできるモデルと、一度  をタップした後、[Device Control] をタップするモデルがあります。

準備

以下のものを準備してください。

- 登録済みユーザーアカウントとパスワード
 - DC アプリを使用するには、ユーザーアカウントのメールアドレスとパスワードを京セラに登録する必要があります。
<https://www.kyocera.co.jp/prdct/telecom/office/phone/rd/dcapp.html> へアクセスして登録してください。

- DC アプリ対応京セラ製端末
 - 管理用端末
 - 配布用端末
- DC アプリ
 - DC アプリをインストールするには、次の QR コードと「管理用端末の準備」の手順を参照してください。



DC アプリ対応モデル

京セラ製の DC アプリ対応モデルについての最新の情報は、
<https://www.kyocera.co.jp/prdct/telecom/office/phone/concept/solution/dcapp.html>
をご確認ください。

管理用端末の準備

管理用端末は、アカウント管理者がポリシーを作成するために使用します。最大 30 のポリシーを端末に保存できます。管理用端末から QR コードを利用して配布用端末に DC アプリや作成したポリシーをコピーすることができます。

QR コードを利用して DC アプリをインストールする

京セラから提供される QR コードを使用して、DC アプリを工場出荷時の状態の端末にインストールします。DC アプリを端末にインストールし、端末所有者モードに設定します。

1. 管理者用端末が出荷時の状態であることを確認する
 - すでに端末の電源を入れているときは、「すべてのデータを消去(出荷時リセット)」を行い、出荷時の状態にする
2. 電源ボタンを長押しする
3. 管理用端末に「日本語（日本）」が出ていることを確認する
4. 画面上の任意の空白個所を数回タップする
 - QR コードリーダーが立ち上がる
5. 京セラが提供する QR コードを読み取る
 - Wi-Fi[®] 設定画面が表示される
6. [Wi-Fi の使用] または ON/OFF 設定をタップして「Wi-Fi の使用」を [ON] にする
7. 接続する Wi-Fi ネットワーク名をタップする
8. 必要に応じて [パスワードを入力] → [接続] → [次へ]
 - 「端末を設定してください」が表示される
9. [メッセージを読む] → [同意して続行]
 - 「仕事用端末を設定中」が表示されるので、画面の案内に従い操作する
10. [Device Control] アプリを立ち上げる
11. 「ソフトウェア使用許諾契約」と「情報収集」に同意する
 - a. [ソフトウェア使用許諾契約] → 「ソフトウェア使用許諾契約」を読む → [OK]
 - b. [情報収集] → 「情報収集」を読む → [OK]
 - c. 同意できれば、[同意する] をタップする

12. 「インフォメーション」 (Device Config Plugin のインストール) に同意する

a. 「インフォメーション」を読む → [OK]

13. DC アプリ用の[メールアドレス]と[パスワード]を入力する

注意 : [メールアドレス]と[パスワード]は

<https://www.kyocera.co.jp/prdct/telecom/office/phone/rd/dcapp.html> で登録したメールアドレスとパスワードです。

- 業種を教えてください メニューが出る

14. [(未選択)] → 「業種を選択」 → [OK]

ポリシー

ポリシーとは、特定のデバイス構成を作成するための一連の設定（制限と機能）です。最大 30 個の異なるポリシーを保存できますが、有効にできるポリシーは 1 つだけです。各ポリシーには名前を付けることができ、保存、編集、確認、名前の変更、または削除を行うことができます。たとえば、ホテルでは、「ハウスキーピング」、「メンテナンス」、や「管理」のために別々のポリシーを作成する場合があります。各ポリシーには、端末の動作を制御するさまざまな設定のグループが含まれています。ハウスキーピングスタッフ用の装置を準備するときには、「ハウスキーピング」ポリシーのみが配布装置に転送されて有効化されます。ポリシーのサンプルは「[ポリシー作成例](#)」に記載しています。

ポリシーの作成

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [新規作成]

– または –

[ポリシー管理] → 

3. [ポリシーの名前を入力] → [OK]

注意： 同じ名前のポリシーを作ることはできません。

4. 制限する項目または[詳細設定]をタップする

例： Bluetooth[®] 機能全体を無効にする

- a. [Bluetooth の無効化]または ON/OFF 設定をタップして Bluetooth の無効化を[ON]にする

5. [保存]

- 設定した内容が表示される

注意： “データの初期化の禁止” は初期設定でオンになっています。

6. [保存]

ポリシーの編集

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [一覧から選ぶ]

– または –

[ポリシー管理] をタップしてポリシーメニューを開く

3. 編集するポリシー設定をタップする
4. [編集]
5. 制限する項目もしくは、[詳細設定]をタップして編集する
6. [保存]
 - 設定した内容が表示される
7. 制限事項の一覧を確認する
8. [保存]

ポリシーの確認

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [一覧から選ぶ]
 - または –

[ポリシー管理] をタップしてポリシーメニューを開く
3. 内容を確認するポリシーをタップする
4. [項目レビュー]
 - 設定内容が表示される
5. [OK]

ポリシーの名前の変更

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [一覧から選ぶ]
 - または –

[ポリシー管理] をタップしてポリシーメニューを開く
3. 名前を変更するポリシーをタップする
4. [名前変更]
5. [新しい名前を入力] → [OK]

注意： 同じ名前のポリシーを作ることはできません。

ポリシーの削除

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [一覧から選ぶ]
- または -
[ポリシー管理] をタップしてポリシーメニューを開く
3. 削除するポリシーをタップする
4. [削除]
5. 確認して [削除] をタップする

詳細設定

詳細設定では、機能のオン/オフだけでなく詳細な設定が可能です。

注意：「詳細設定では、機能のオン/オフだけでなく詳細な設定も可能ですが、デバイスの使いやすさに大きな影響を与える可能性があります。これらの設定を誤って変更すると、重要なデータの損失、工場出荷時の状態へのリセットまたは、端末が使用できなくなる可能性があります。

詳細設定の項目については、「[ポリシーの制限と機能](#)」を参照ください。

次の手順で詳細設定を有効にできます。

1. [Device Control] アプリを立ち上げる
2. [管理用端末] → [ポリシー作成/編集] → [新規作成]
- または -
[ポリシー管理] → 
3. [ポリシーの名前を入力] → [OK]
4. [詳細設定]
5. 設定する項目をタップし、タイトルまたは ON/OFF 設定をタップしてオンにする

例：Bluetooth テザリングを無効にする

- a. [Bluetooth]

- b. **「テザリングの無効化」** または ON/OFF 設定をタップして、「テザリングの無効化」をオンにする

6. 必要な設定が終わるまで、ステップ5を繰り返す

7. **「保存」**

- 設定した内容が表示される

注意：“データの初期化の禁止” は初期設定でオンになっています。

8. **「保存」**

配布用端末の準備

配布用端末へは特定の設定ポリシーを入れて使用者に配布することができます。 端末の機能を設定し制限を適用するには、正しくプロビジョニングする必要があります。 プロビジョニングプロセスを開始するには、管理用端末の「プロビジョニング」で QR コードを使用する方法を選択します。

DC アプリのインストール

＜ 配布用端末の操作 ＞

1. 出荷時の状態であることを確認する
 - すでに端末の電源を入れているときは、「すべてのデータを消去(出荷時リセット)」を行い、出荷時の状態にする
2. 電源ボタンを長押しする
3. 「日本語（日本）」が出ていることを確認する

＜ 管理用端末の操作 ＞

4. [Device Control] アプリを立ち上げる
 - a. 必要に応じて、メールアドレスとパスワードを入力し、[サインイン]をタップする
5. [管理用端末] → [プロビジョニング] → [QR コードプロビジョニング]
6. 必要に応じて、「Wi-Fi ネットワーク名」、「Wi-Fi セキュリティタイプ」及び「Wi-Fi パスワード」を入力する
7. [システムアプリの無効化をスキップします] をタップして「システムアプリの無効化をスキップします」をオンにする
8. [QR コード生成]
 - QR コードが表示される

＜ 配布用端末の操作 ＞

9. 画面上の任意の空白個所を数回タップする
 - QR コードリーダーが立ち上がる
10. 管理者用端末に表示されている QR コードを読み取る

11. Wi-Fi 設定メニューが出たら Wi-Fi を設定し、[次へ]をタップする
12. “端末を設定してください” を読み、了承したら[同意して続行]をタップする
13. 画面の指示に従い端末の設定をする

注意 : DC アプリを初めて立ち上げたとき、「インフォメーション」ダイアログ (Device Config Plugin のインストールの同意) が表示されるので[OK]をタップする。

配布用端末へのポリシーの転送

QRコードを使用した配布用端末へのポリシーの転送

＜ 管理用端末の操作 ＞

1. [管理用端末] → [ポリシー送信] → [QRコード]
2. 転送するポリシーをタップする
3. [OK]
 - QRコードが表示される

＜ 配布用端末の操作 ＞

4. [配布用端末] → [ポリシー受信] → [QRコード]
 - QRコードリーダーが立ち上がる
5. 管理者用端末に表示されているQRコードを読み取る
 - 成功したら「成功 “〇〇”を作成しました。」が表示される
6. [OK]

配布用端末のポリシー管理

ポリシーを有効にする

1. [Device Control] アプリを立ち上げる
2. [配布用端末] → [ポリシー実行]
 - or –
 - [ポリシー管理]
3. 有効にするポリシーをタップする
4. [実行]

注意：有効にできるポリシーは1つだけです。新しいポリシーを有効にした場合、現在有効になっているポリシーは無効になります。

5. 終了したら[サインアウト]をタップする

注意：サインアウトをタップするまでユーザーは管理者権限を持ちポリシーを無効にすることができます。

ポリシーを無効にする

1. [Device Control] アプリを立ち上げる
2. サインインメニューが表示されたら、メールアドレスとパスワードを入力し、[サインイン]をタップする
 - 実行中のポリシーが表示される
3. [停止]

DC アプリの管理

アプリのアップデート

1. [Device Control] アプリを立ち上げる
2.  → [設定]
3. [アップデートをチェック]
 - Google Play ストアの DC アプリのダウンロード画面が表示される
 - Google Play にサインインしていない場合、サインインメニューが表示される
4. 画面に従い操作する

登録ユーザーの削除

1. [Device Control] アプリを立ち上げる
2.  → [設定]
3. [登録ユーザーの削除]
 - 削除確認画面が表示される
4. [OK]

注意：登録ユーザーの削除を実行すると適用中のポリシーは解除されます。

アプリのアンインストール

DC アプリをアンインストールするには、端末を初期化（工場出荷状態）にしてください。

注意：データの初期化を実行すると本体内のすべてのデータが消去されます。データの初期化を実行する前に本体内のデータをバックアップすることをおすすめします。

ポリシー作成例

例題は、特定の顧客の要件を満たすようにポリシーを構築するために複数の制限と機能を選択できることを示しています。これらの例題は意図的に単純化しており、1つのポリシーのみを表しています。DC アプリは、指定された一連の要件を満たすために使用できるさまざまな設定、制限、機能を公開します。

一部の設定または設定の組み合わせ（特に「詳細設定」で公開されている設定）は、デバイスの操作性に重大な影響を与える可能性があることに注意してください。

重要な注意事項

DC アプリのポリシーによって提供される設定と制限は、ユーザーが割り当てられた構成を変更または回避できない場合にのみ有効です。次の各サンプルでは、ユーザーが「設定」メニューのオプションを使用して電話をリセットできないようにするために、「データの初期化の禁止」が選択されています。電話機を工場出荷時の状態に初期化することは、ユーザーがポリシーを回避する方法の一例です。技術的なスキルとユーザーの決定に応じて、目的のポリシーが有効であることを保証するために、追加の設定と高度な方法が必要になる場合があります。

設定例 1

シナリオ：宅配便業者は、街中に荷物を配達するトラックを所有しています。宅配業者はオフィスに連絡できるようにドライバーに端末を提供したいと考えています。しかし、ドライバーにGPS 設定を変更させたくありません。

端末制御の制限

カテゴリー	タイトル	設定内容
位置情報	位置情報設定の有効化	位置情報設定を強制的に有効にします
リセット	データの初期化の禁止	データの初期化を禁止します

設定例 2

シナリオ：建設会社は、すべての労働者に端末を提供することを計画していますが、インストールされているアプリを使用して時間を無駄にさせたくありません。

注意

DC アプリには、ユーザーが使用できるアプリケーションを制限するための複数の方法が用意されています。各方法の意味と、それがユーザーに与える影響を理解することが重要です。たとえば、単一のアプリケーションを無効にすると、他の依存アプリケーションが正常に動作しなくなる場合があります。

端末制御の制限

カテゴリー	タイトル	設定内容
アプリ	アプリの起動制限	起動制限アプリリストのアプリの起動を制限します
アプリ	起動制限アプリリスト	起動制限アプリリストの管理（リストから起動制限するアプリケーションを選択します）
リセット	データの初期化の禁止	データの初期化を禁止します

ポリシーの制限と機能

制限機能一覧

タイトル		内容
Wi-Fi の無効化 *1		すべてのWi-Fi 機能を無効にするかどうかを設定します
Bluetooth の無効化		すべてのBluetooth 機能を無効にするかどうかを設定します
NFC の無効化 *1		NFC 機能を無効にするかどうかを設定します
カメラの無効化		カメラを無効にするかどうかを設定します
不明なアプリのインストールを禁止		提供元不明アプリのインストールを制限するかどうかを設定します
USB ファイル転送の無効化		パソコンと USB ケーブルで接続した時にファイル転送（ファイル・写真の転送）を無効にするかどうかを設定します
SD カードのマウント操作を禁止		SD カードを装着した時にマウント操作を無効にするかどうか設定します。 既に SD カードが端末にマウントされている場合は無効になりません。
モバイルデータの無効化 *1		モバイルデータ通信を無効にするかどうかを設定します
カテゴリー	タイトル	内容
着信制限	着信の制限 *1	着信を制限するかどうかを設定します
	電話帳を除く *1	着信制限の対象から電話帳登録済みの番号を除外するかどうかを設定します
	許可リスト番号 *1	着信制限の対象から許可リストに登録した番号を除外するかどうかを設定します
発信制限	発信の制限 *1	発信を制限するかどうかを設定します
	電話帳を除く *1	発信制限の対象から電話帳登録済みの番号を除外するかどうかを設定します
	許可リスト番号 *1	発信制限の対象から許可リストに登録した番号を除外するかどうかを設定します

制限機能一覧（詳細設定）

カテゴリー	タイトル	内容
Wi-Fi	Wi-Fi 制限	
	Wi-Fi の無効化 *1	すべての Wi-Fi 機能を無効にするかどうかを設定します
	オープンネットワークの無効化 *1	セキュリティで保護されていない Wi-Fi アクセスポイントへの接続を無効にするかどうかを設定します
	セットアップの無効化 *1	Wi-Fi アクセスポイントの追加や編集を禁止するかどうかを設定します
	テザリングの無効化 *1	Wi-Fi テザリング機能を無効にするかどうかを設定します
Bluetooth	Bluetooth 制限	
	Bluetooth の無効化	すべての Bluetooth 機能を無効にするかどうかを設定します
	テザリングの無効化 *1	Bluetooth テザリング機能を無効にするかどうかを設定します
	Bluetooth 設定の変更を禁止	設定アプリから Bluetooth 設定の変更操作を無効にするかどうかを設定します
	HFP プロファイルのみ許可 *1	Bluetooth プロファイルの利用を制限するかどうかを設定します。制限中に利用可能なプロファイルは個別に設定できます。 このポリシーは HFP、HSP、MAP、PBAP プロファイルの利用を許可します。許可していない他のプロファイルは利用できなくなります。
	オーディオプロファイルのみ許可 *1	Bluetooth プロファイルの利用を制限するかどうかを設定します。制限中に利用可能なプロファイルは個別に設定できます。 このポリシーは A2DP、AVRCP、HFP、HSP プロファイルの利用を許可します。許可していない他のプロファイルは利用できなくなります。
	データプロファイルのみ許可 *1	Bluetooth プロファイルの利用を制限するかどうかを設定します。制限中に利用可能なプロファイルは個別に設定できます。 このポリシーは GATT、HID、MAP、OPP、PAN、PBAP プロファイルの利用を許可します。許可していない他のプロファイルは利用できなくなります。
	Bluetooth Class of Device/Service	
	Class of Device/Service Field の指定 *1	端末の Class of Device/Service Field を指定した値に変更します

緊急通知	有効設定	
	緊急速報の有効化 *1	緊急速報を強制的に有効にします
	重大通知の有効化 *1	重大通知を強制的に有効にします
	異常通知の有効化 *1	異常通知を強制的に有効にします
	無効設定	
	緊急速報の無効化 *1	緊急速報を強制的に無効にします
	重大通知の無効化 *1	重大通知を強制的に無効にします
	異常通知の無効化 *1	異常通知を強制的に無効にします
ネットワーキング	ネットワークの制限	
	VPN 設定の編集を禁止	VPN 設定の変更を無効にするかどうかを設定します
	グローバルプロキシ指定	グローバルプロキシを指定した値に変更します
端末	端末機能の制限	
	端末機能制限	
	SMS の無効化	SMS の送受信を無効にするかどうかを設定します
	NFC の無効化 *1	NFC 機能を無効にするかどうかを設定します
	ソフトウェアアップデートの無効化 *1*2	ソフトウェアアップデートを無効にするかどうかを設定します
	カメラの無効化	カメラを無効にするかどうかを設定します
	日付と時刻変更の禁止	日付と時刻の変更を禁止するかどうかを設定します
	通知パネルの無効化	クイック設定を含む通知シェードの表示を制限するかどうかを設定します。 ロック画面に表示される通知は制限されません。
	バイブレーションの無効化 *1	バイブレーションを無効にするかどうかを設定します
	不明なアプリのインストールを禁止	提供元不明アプリのインストールを禁止するかどうかを設定します
	壁紙設定変更の禁止	壁紙設定の変更を禁止するかどうかを設定します
	電源オフの無効化 *1	端末の電源オフ操作を無効にするかどうかを設定します
	セーフモードの無効化	セーフモード機能の利用を無効にするかどうかを設定します
	リカバリーモードの無効化 *1	リカバリーモード機能の利用を無効にするかどうかを設定します
	カーキット電源連動制限 *1	カーキット接続と端末の電源 ON・OFF 動作を連動させるかどうかを設定します。 設定した値を強制的に適用します。
	自動入力サービスの無効化	アカウントやパスワードが必要な入力フォームでの自動入力サービスを無効にするかどうかを設定します
	音量調整の無効化	すべてのボリュームをミュートするかどうかを設定します

マイクの無効化	マイク入力を無効にするかどうかを設定します。 ボイスレコーダーや通話時のマイク入力も無効になります。
スクリーンショットの制限	画面キャプチャが許可されていない画面のスクリーンショットの取得や画面の録画機能を制限するかどうかを設定します
クリップボードの無効化	コピー＆ペースト操作を無効にするかどうかを設定します
Doze モードの無効化 *1	電池の最適化を無効にするかどうかを設定します
デバッグ機能の無効化	開発者オプションや USB デバッグを含むすべてのデバッグ機能を無効にするかどうかを設定します
通知制限	
クイック設定編集の禁止 *1	クイック設定の編集を無効にするかどうかを設定します
電池へのショートカットの無効化 *1	通知シェードから電池のショートカット起動を無効にするかどうかを設定します
USB 制限	
USB テザリングの無効化 *1	USB テザリング機能を無効にするかどうかを設定します
USB デバッグの無効化 *1	USB デバッグ機能を無効にするかどうかを設定します。開発者オプションは無効化しません。
USB ファイル転送の無効化	パソコンと USB ケーブルで接続した時にファイル転送（ファイル・写真の転送）を無効にするかどうかを設定します
USB ホストの無効化 *1	USB 子機の接続を無効にするかどうかを設定します
SD カード制限	
SD カードのマウント操作を禁止	SD カードを装着した時にマウント操作を無効にするかどうかを設定します。 既に SD カードが端末にマウントされている場合は無効になりません。
暗号化の有効化 *1	SD カードの暗号化を有効にするかどうかを設定します
キーコントロール	
キーイベント置換	
キーイベント置換の有効化 *1	キー操作時に発行する_intentを指定します
キー制限	
履歴キーの無効化 *1	履歴キー押下を無効にするかどうかを設定します
電源ボタンの無効化 *1	電源ボタン押下を無効にするかどうかを設定します
ボリュームアップボタンの無効化 *1	ボリュームアップボタン押下を無効にするかどうかを設定します

ボリュームダウンボタンの無効化 *1	ボリュームダウンボタン押下を無効にするかどうかを設定します
ホームキー長押しの無効化 *1	ホームキー長押下を無効にするかどうかを設定します
カメラボタンの無効化 *1	カメラボタン押下を無効にするかどうかを設定します
ダイレクトボタンの無効化 *1	ダイレクトボタン押下を無効にするかどうかを設定します
外部スピーカーボタンの無効化 *1	外部スピーカーボタン押下を無効にするかどうかを設定します
SOS ボタンの無効化 *1	SOS ボタン押下を無効にするかどうかを設定します
アシスタントボタンの無効化	アシスタントボタン押下を無効にするかどうかを設定します
Kiosk 設定	
Kiosk 設定	
Kiosk モードの有効化	Kiosk モードを設定します。 Kiosk モードでは、Kiosk アプリの選択で選択したアプリのみを表示し、他のアプリは制限します。 Kiosk モードを解除する場合は端末起動時に表示される特別な画面を素早く 5 回をタップします。
Kiosk アプリの選択	Kiosk モードで表示されるアプリを選択します

電話	モバイルネットワークの制限	
	モバイルネットワークの制限	
	音声ローミングの無効化 *1	音声ローミングを無効にするかどうかを設定します
	データローミングの無効化	データローミングを無効にするかどうかを設定します
	モバイルデータの無効化 *1	モバイルデータ通信を無効にするかどうかを設定します
	電話帳制限	
	電話帳制限	
	電話帳編集の無効化 *1	電話帳の登録や編集を無効にするかどうかを設定します
	着信制限	
	着信制限	
	着信の制限 *1	着信を制限するかどうかを設定します
	電話帳の登録番号を許可 *1	着信制限の対象から電話帳登録済みの番号を除外するかどうかを設定します
	許可リストの番号を許可 *1	着信制限の対象から許可リストに登録した番号を除外するかどうかを設定します
	発信制限	
	発信制限	
	発信の制限 *1	発信を制限するかどうかを設定します
	電話帳の登録番号を許可 *1	発信制限の対象から電話帳登録済みの番号を除外するかどうかを設定します
	許可リストの番号を許可 *1	発信制限の対象から許可リストに登録した番号を除外するかどうかを設定します

アプリ	システムアプリケーション制限	
	システムアプリケーション制限	
	Google バックアップの無効化	Google バックアップを無効にするかどうかを設定します
	緊急通知の無効化	緊急通知を無効にするかどうかを設定します
	設定アプリの起動制限	設定アプリの起動を無効にするかどうかを設定します
	アンインストール禁止リスト作成	
	アンインストール禁止リスト作成	
	アンインストール禁止リスト作成	アンインストール禁止リストに登録したアプリをアンインストール禁止にします
	アンインストール禁止リスト	アンインストールを禁止にするアプリを管理します
	アプリの起動制限	
	アプリの起動制限	
	アプリの起動制限	非表示アプリケーションリストに登録したアプリを非表示または起動制限します
	起動制限アプリリスト	非表示または起動制限するアプリを管理します
	インストール許可リスト作成	
	インストール許可リスト作成	
	インストール許可リスト作成	アプリケーションの許可リストに登録したアプリ以外のアプリケーションインストールを制限します
	インストール許可リスト	インストール許可するアプリケーションを管理します
	Chrome の設定	
	Enable alternate error pages、Enable search suggestions などを設定できますが、Chrome の法人機能に関する高度な知識が必要です。 この機能の詳細は Chrome の提供元に問い合わせください。	
リセット	データの初期化制限	
	データの初期化の禁止	データの初期化を禁止するかどうかを設定します
位置情報	有効設定	
	位置情報設定の有効化	位置情報設定を強制的に有効にします
	無効設定	
	位置情報設定の無効化	位置情報設定を強制的に無効にします
	疑似ロケーション制限	
	疑似ロケーションの無効化 *1	疑似ロケーションの使用を無効にするかどうかを設定します

セキュリティ	セキュリティ設定制限	
	SIM カードロックの無効化 *1	SIM カードロックを無効にするかどうかを設定します
	スタート画面設定制限	
	スタート画面上のカメラの無効化	パターン、PIN、パスワードで画面ロックを設定時、画面ロックを維持したままカメラを起動することを無効にするかどうかを設定します
	スタート画面上のショートカットの無効化 *1	ロック画面からアプリをショートカット起動することを無効にするかどうかを設定します
	スタート画面の通知の無効化	パターン、PIN、パスワードで画面ロックを設定時、画面ロック中に通知を非表示化するかどうかを設定します
	信頼エージェントの無効化	信頼エージェントによる画面ロック制御を無効にするかどうかを設定します
	スタート画面のプライベート通知の無効化	パターン、PIN、パスワード で画面ロックを設定時、画面ロック中に秘匿化された通知のみを表示するかどうかを設定します
	スタート画面の指紋認証の無効化	指紋認証による画面ロック解除を制限するかどうかを設定します
	パスワード設定制限	
	パスワード入力の最大失敗回数	パスワード入力の最大失敗回数を設定します。パスワードの入力に指定回数失敗した場合は、端末ワイプを実行します
	ロックまでの最大時間	画面ロックまでのユーザーの無操作時間を設定します
	パスワードの有効期限	パスワードの有効期限を設定します。期限が切れた場合はロック解除パスワードの更新を要求する通知を定期的に表示します
その他	その他設定制限	
	その他の設定内容は、Device Config Plugin の設定画面を表示します。Device Config Plugin の内容はソフトのバージョンやインストールしているアプリに依存しますので、Device Config Plugin に関する詳細情報は下記ページをご参照ください。 https://www.kyocera.co.jp/prdct/telecom/office/phone/rd/dcplugin.html	

*1 Device Config Plugin の機能を利用するため、機能がサポートされていない端末では動作しない場合があります。Device Config Plugin の機能サポート状況に関する詳細情報は下記ページをご参照ください。

<https://www.kyocera.co.jp/prdct/telecom/office/phone/rd/dcplugin.html>

*2 ソフトウェアアップデートの無効化を「オン」に設定しているときにシステムトレイにソフトウェアアップデートが可能である旨の通知が行われる場合がありますが、アップデートの操作はできません。

