Mobile Device Manager

STAR-MDM

Android Enterpriseマニュアル

第 2.4 版

版	日 付	内 容	備 考
1.0.0	2017/08/24	初版	
1.1.0	2018/01/24	デバイス制御：シングルアプリモード追加	
1.2.0	2018/01/24	デバイス制御：SmartLock 制限追加	
1.3.0	2018/06/21	デバイス制御：節電モード許可追加	
1.4.0	2018/07/05	管理モード：Comp 追加	
1.5.0	2019/08/01	証明書配布機能 追加 承認アプリ管理 アクセス権対応 LINE WORKS 連携設定 管理モード：WorkProfile 追加 SafetyNet 機能追加 パスワード管理ポリシー追加 デバイス制御：複数機能追加 証明書管理機能追加 EAP Wi-Fi 設定機能追加 証明書配布拡張子対応 限定公開アプリ/ウェブアプリ機能追加 Zero-touch enrollment 追加 Work Managed Device 端末での E-API による外部メモリ削除対応 Comp OS 9 に対応 ChromeURL 制限対応 AE 管理アカウントの追加削除制限	
1.6.0	2020/05/21	QR コード自動設定項目に関する機能追加 緊急指示画面の変更に伴う修正 サイレントインストール/アンインストール機能およびアプリ設定機能の一部仕様変更に伴う修正 ハッシュタグキッティングの手順追加 アプリ設定（高度な設定）機能追加 Android10 対応に伴う修正 QR コード /SetUpMaster に関する変更 デバイス制御機能の機能追加に伴う修正 パスワード管理機能の機能追加に伴う修正 アカウント無効および削除時の対応を追記 Gsuite アカウントで企業登録時のトークン生成方法変更に伴う修正 キオスク管理機能追加に伴う修正 サイレントインストールの新機能追加に伴う修正	
1.6.1	2020/12/01	システムアップデートの新機能追加に伴う修正	

1.7	2021/04/21	サイレントインストールの新機能追加に伴う修正 Android11 対応に伴う修正 アプリ設定のブックマーク設定方法およびホームページ URL 設定方法の追加	
1.8	2022/2/13	管理モード:WorkProfile[企業所有] 追加 個人情報利用の許諾追加に伴う修正 アプリ設定の設定反映状況機能追加 クロスプロファイル権限設定の機能追加に伴う修正	
1.9	2022/9/25	Android12 対応に伴う修正 Android Enterprise 企業登録のリンク変更に伴う修正 Google 管理コンソール画面変更に伴う修正 承認アプリ管理機能変更に伴う修正	
2.0	2023/3/24	Android13 対応に伴う修正	
2.1	2023/9/6	軽微な表現の見直し	
2.2	2023/11/10	URL の変更・削除	
2.3	2024/4/25	Android14 対応に伴う修正	
2.4	2024/8/6	Managed Google Play アカウント登録手順変更に伴う修正 位置情報の権限許可に関する修正 EAP Wi-Fi 設定登録に関する修正	

1 Android Enterprise とは

1. 概要

本書は、STAR-MDMにおけるAndroid Enterpriseの利用方法を記載した管理者用のマニュアルです。

Android Enterprise はビジネスデバイスをより安全・便利にご利用いただくためのデバイス管理機能です。
Google社より提供される企業向けデバイス制御機能（旧称：Android for Work）を利用し、
通常のMDMアプリでは実現できなかった項目の制御を、OSレベルで実現できます。

※本マニュアルに掲載しているGoogle社が管理するWEB画面キャプチャは2018年6月時点のものであり、
Google社により予告なく変更される場合がございます。予めご了承ください。

STAR-MDMにおけるAndroid Enterpriseでは Work Managed Device / Work Profile / Work Profile[仕事領域]/
Comp の4つの管理モードを提供しています。

Work Managed Device

利用デバイス全体を
企業の監視下におき、
より強い制御機能により
管理することができます。

Work Profile

デバイス内に仕事領域を作成し、
仕事領域のみ企業の監視下で
管理することができます。

Comp

WorkManaged Device
端末内に Work Profile
（仕事領域）を作成し、
それぞれの領域を区
別して管理することが
できます。

Work Profile[企業所有]

企業所有の端末内に仕事
領域（Work Profile）を作成
し、仕事用の領域と個人用
の領域（プライベート領域）
の一部機能を管理すること
ができます。

2. 稼働環境

【対応端末】

■対応OS

Work Managed Device	：	Android OS 6.0 以降
Work Profile	：	Android OS 8.0 以降
Work Profile[企業所有]	：	Android 11以降
Comp	：	Android OS 8.0～OS 10 ※Android 11 以降は、Compは非対応です。

■対応SPPM Agent ver

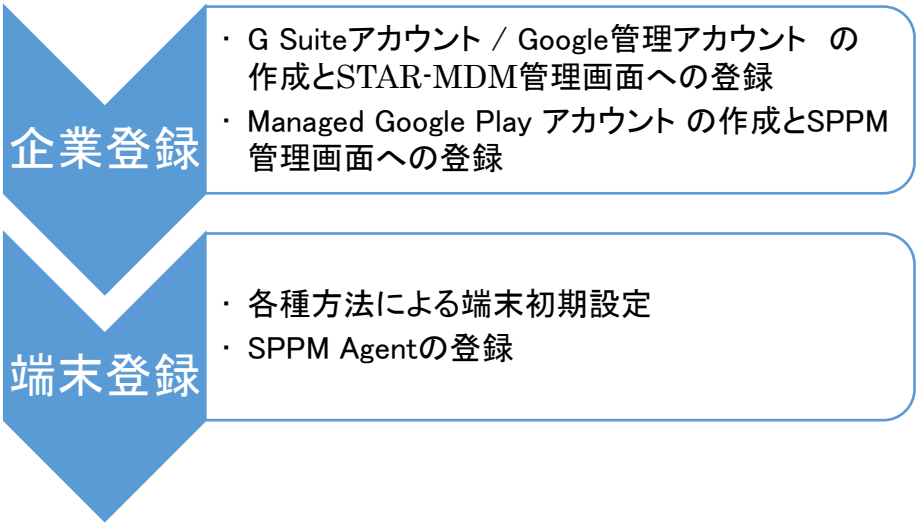
Work Managed Device	：	SPPM Agent v3.25 以降
Work Profile	：	SPPM Agent v3.40 以降
Work Profile[企業所有]	：	SPPM Agent v3.59 以降
Comp	：	SPPM Agent v3.30 以降

■対応機種

動作検証とAgent対応を行っていない端末につきましては、対応OS以降であっても、
動作保証対象外となります。非対応機種でのご利用はユーザー様の責任において行ってください。
Android Enterpriseの動作検証対応が完了している端末につきましては、弊社にお問い合わせください。
※Android Enterprise の対応状況については、「対応一覧」をご覧ください。
※新機種における対応状況については、検証機貸し出し時にご相談ください。

3. 設定手順について

Android Enterprise では組織で管理する G Suite アカウント/Google 管理者アカウント/Managed Google Play アカウントのいずれかを利用し、デバイスを Android Enterprise 端末として STAR-MDM の管理下に置きます。



4. 使用アカウントについて

組織で管理するG Suiteアカウント/Google管理者アカウント/ManagedGooglePlayアカウントをSTAR-MDM管理画面へ登録することで、Android Enterpriseをご利用いただけます。

■G Suite アカウント

G Suiteにお申し込みされた組織によって発行されます。

https://gsuite.google.com/

■Google 管理者アカウント（管理対象のGoogleアカウント）

Androidを管理する組織のドメインによって管理されます。

申込みページ：https://workspace.google.com/gcpidentity/signup?sku=identitybasic

■Managed Google Play アカウント

G Suiteアカウントや管理対象のGoogleアカウントを持っていない組織に適しています。

〇〇〇@gmail.comのような個人向けGoogleアカウントを利用して管理設定を実施する事が可能です。

※個人向けGoogleアカウントを利用する場合の注意事項はこちら。

※各アカウント種別の詳細については下記を参照してください。

https://support.google.com/work/android/answer/6371476?hl=ja&ref_topic=6151012

※設定手順や端末に追加されるアカウントを除き、STAR-MDMの機能上は登録アカウントの種別による差分はありません。

【Android Enterpriseにおけるアカウントの種別と扱いについて】

	G Suite サービス	キッティング方法	個別のGoogleアカウントの必要有無	ドメイン取得	対応管理モード
G Suite アカウント	利用可能	①QRコード ②SetUpMaster ③Googleアカウント入力 ④ハッシュタグ	STAR-MDM登録時に、1台につき1つのG Suiteアカウントが必要 ※1	必要	・Work Managed Device ・WorkProfile ・WorkProfile［企］
Google管理者アカウント	利用不可	①QRコード ②SetUpMaster ③Googleアカウント入力 ④ハッシュタグ	STAR-MDM登録時に、1台につき1つの自社ドメインアカウント（管理対象のGoogleアカウント）が必要 ※1	必要	・Work Managed Device ・WorkProfile ・WorkProfile［企］
Managed GooglePlay アカウント	利用不可	①QRコード ②SetUpMaster ③ハッシュタグ	1社で1つのManaged GooglePlayアカウントが必要 ※設定方法はこちら。	不要	・Work Managed Device ・WorkProfile ・Comp ・WorkProfile［企］

※1 各端末ユーザー毎のG Suite/自社ドメインアカウントはGoogle管理コンソール、またはSTAR-MDM管理画面のGoogleアカウント管理機能からのアカウント追加が可能です。

STAR-MDM管理画面のGoogleアカウント管理機能は企業登録時にGoogle管理コンソールとの連携設定が必要です。設定方法はこちら。

≪Managed Google Play アカウント利用時の注意事項≫

〇〇〇@gmail.com のような個人向けGmailアカウントは、長期間ログインされない場合や、Googleでポリシー違反※と判断された場合にアカウントの無効化や削除（もしくは無効化後、削除）がGoogleによって実施されることがあります。そのため、アカウントへの定期的なログインやサブアカウントの登録をお願いいたします。

※無効化される要因は状況によって異なります。

アカウントが無効になる理由については下記のURLをご参照ください。

https://support.google.com/accounts/answer/40695?hl=ja/#why

※ Googleのポリシーと規約については下記のURLをご参照ください。

・Googleポリシーと規約

https://policies.google.com/?gl=JP&hl=ja

・Managed Google Play 契約

https://www.android.com/enterprise/terms/

■Gooogleアカウントが無効または削除された場合に影響を受ける機能

Google APIを利用する以下の機能が利用できなくなります。

・SafetyNet 設定
・Googleアカウント管理
・Comp 設定
・承認アプリ管理
・サイレントインストール / アンインストール
・アプリ設定
・PlayStoreレイアウト設定
・証明書管理

■アカウント無効時に発生する影響への対策

アカウント無効時に発生する、一部機能の利用不可状態を防いだり、再キッティングを実施する事態を回避するため、あらかじめサブアカウントの登録をお願いしています。

詳細は☞「Google サブアカウントの登録方法」

■アカウント無効および削除時の対応

アカウントが無効となった場合は、以下の Google のサイトに記載された内容で復元することが可能です。

https://support.google.com/accounts/answer/40695?hl=ja

※復元が行えなかった場合、速やかに弊社までお問合せください。

復旧可否含め、調査・Google社への問い合わせを実施いたします。

アカウントが削除されて復元ができない場合は、全台ライセンスキーリセットと初期化を実施した上で、再取得したアカウントでの企業登録と端末の再キッティングを実施する必要があります。

2 企業登録

1. 登録方法

管理画面のメニューバー[その他]のAndroid企業登録をクリックしてください。

次の画面で、登録に使用するアカウントの種類を選択します。

※「G Suiteアカウント / Google管理者アカウント」ではCompモードに対応していないためご注意ください。

G Suiteアカウント / Google管理者アカウント

「G Suiteアカウント / Google管理者アカウント」を選択し、**「登録」**をクリックしてください。

必要な情報を入力し、**「登録」**をクリックします。

≪各入力項目について≫

■企業メイン（必須）

G Suiteアカウント・Google管理者アカウントで使用しているドメインを入力します。

■トークン（必須）

Google管理コンソールで発行したトークンを入力します。

➤参照：トークン生成方法

■Googleアカウント管理機能登録（任意）

「する」に設定すると、Googleアカウントの管理をSTAR-MDM管理画面上で行えるようになります。

➤参照：Googleアカウント管理機能登録　設定方法

※アカウントの申し込みは以下から行えます。

Google Workspace（旧G Suiteアカウント）の申し込みはこちら

Cloud Identity（旧Gogle管理者アカウント）の申し込みはこちら

Android 企業登録が完了し、企業登録情報が表示されます。

■トークン生成方法

Google管理コンソール ： https://admin.google.com/AdminHome

Google管理コンソールへ「G Suiteアカウント / Google管理者アカウント」でログインし、トークンを生成します。

ホーム>デバイス> Third-party Integrations >EMM プロバイダの管理>トークンを生成

1. 管理コンソールにログインし、サイドバーのメニューから「デバイス」>「モバイルとエンドポイント」>「設定」>「サードパーティとの連携」の順にクリックします。

2. 「Android EMM」をクリックします。

3.「サードパーティの Android モバイル管理を有効にする」にチェックを入れます。
その後、「EMMプロバイダを追加」をクリックします。

4.**「トークンを生成」**をクリック。生成されたトークンをAndroid企業登録「トークン」へ入力してください。
※トークンの期限は30日と表示されますが、登録までの有効期限であり、登録後は再度トークンの更新は必要ありません。
※生成したトークンは1回のみ使用可能です。企業登録を削除し再登録する場合、トークンを生成し直す必要があります。
※トークン登録後、Google管理コンソール画面に反映されるまでに時間がかかる場合があります。

■Google アカウント管理機能登録 設定方法

利用にはGoogle Developers ConsoleとGoogle管理コンソールでの設定が必要です。

詳細な設定方法は「Android_Enterprise Googleアカウント管理機能登録_設定手順書」をご確認ください。

Managed Google Playアカウント

「**Managed Google Play アカウント**」を選択し、「**登録**」をクリックしてください。

管理者アカウント作成画面に遷移するので、個人のメールアドレスを入力して「次へ」をクリックしてください。

※ メールアドレスを入力すると「次へ」ボタンが活性化します。

※ 本画面では、G-Suiteのメールアドレスを設定しないでください。正常に利用できない可能性があります。

登録方法選択画面が表示されるので、「Android のみ登録」の下部にある「登録」リンクをクリックしてください。

Google Play画面に遷移するので**「ログイン」**をクリックし、Googleのログイン画面でログインしてください。
このときアカウントは通常のGoogleアカウントを使用できます。
※Android Enterprise企業登録用のアカウントをひとつ用意し、管理することを推奨します。

通常のGoogleアカウントは、状況により**アカウントの無効化や削除状態となる場合があり、**
企業登録の再実施や再キッティングが必要になる場合があります。詳細はこちら。

企業登録で使用するアカウントでログインされていることを確認し、Google Play画面で**「スタートガイド」**をクリックしてください。

「企業/組織名」を入力し、**「次へ」**をクリックしてください。
※「組織名」はSTAR-MDM管理画面上では使用されません。

データ保護責任者とEU担当者の入力欄に情報を入力し「**managed Google Play　契約を確認しました。この内容に同意します。**」にチェックをいれて、「**確認**」をクリックしてください。

設定完了画面が表示されるので、「**登録を完了**」をクリックしてください。

Android 企業登録が完了し、企業登録情報が表示されます。

※Managed Google Play アカウントによる登録が行われた場合、「企業ドメイン」「トークン」「クライアントID」は空欄となります。また、Googleアカウント管理機能登録「する」の設定になりますが、STAR-MDM管理画面の「Googleアカウント管理」機能は非対応です。

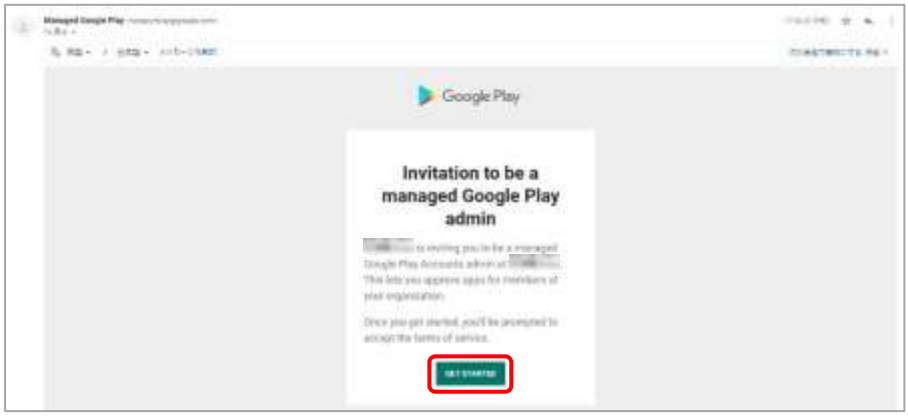
〇〇〇@gmail.com のような個人向け Gmail アカウントは、長期間ログインされない場合や、Google でポリシー違反と判断された場合にアカウントの無効化や削除（もしくは無効化後、削除）が Google によって実施されることがあります。
アカウント無効時に発生する、AndroidEnterpise 機能の利用不可状態を防いだり、再キッティングを実施する事態を回避するため、次ページの手順にてあらかじめサブアカウントの登録をお願いいたします。（推奨設定）
関連情報☞「Managed Google Play アカウント利用時の注意事項」

■Googleサブアカウントの登録方法

Google Play for Work（https://play.google.com/work）に企業登録した際のアカウントでログインをし、
管理者設定画面を開く。

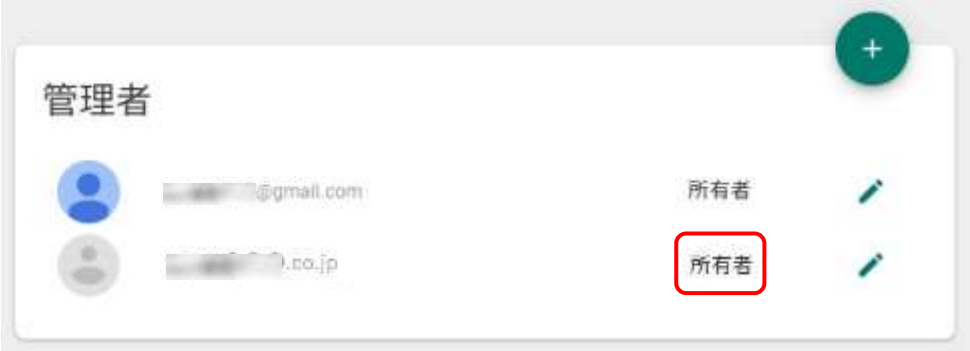
管理者横にある＋アイコンをクリックし、日常的に使用しているアカウントを入力して招待する。

入力したメールアドレス宛に招待メールが届いたら、GET STARTED をクリックする。



ログイン画面が表示されるので、先ほどメールが送られてきたアカウントでログインする。
ログインしたあと、再度管理者画面を開きアカウントが追加されていることを確認します。

再度、企業登録した際のアカウントでログイン後、サブアカウントの編集ボタンをクリックし、
追加したサブアカウントの権限を「所有者」に変更してください。



G-Suite で設定されているアカウントや、すでに別の環境で登録されているアカウントは使用できません。

2. 企業登録情報確認

企業登録後、Android 企業登録画面から企業登録情報を確認できます。

■Android Enterprise(Work Managed Device)設定ツール

・QRコード/SetUpMaster ダウンロードページ

端末をAndroid Enterprise(Work Managed Device)で登録するための「QRコード」「SetUpMasterアプリ」のダウンロードページを表示します。

■「削除」ボタン

企業登録を削除(解除)するためのボタンです。ボタンをクリックすると削除確認画面が表示されます。

※端末一覧画面にAndroid Enterprise端末が残っている場合は、企業登録を削除できません。該当端末のライセンスキーリセットを行って下さい。

≪登録したアカウント種別の確認について≫

GSuiteアカウント / Google管理者アカウント で登録した場合、「企業ドメイン」と「トークン」が表示されます。

Managed Google Play アカウント で登録した場合、「企業ドメイン」と「トークン」は表示されません。

QRコード/SetUpMaster ダウンロードページ

端末をAndroid Enterprise(Work Managed Device)で登録するための「QRコード」「SetUpMasterアプリ」をダウンロードできます。また、Wi-Fi設定やポリシー設定を自動で設定可能な専用のQRコードを作成できます。

■Android Enterprise(Work Managed Device)設定ツール

・QR コード ダウンロード

端末を Android Enterprise(Work Managed Device)で登録するための「QR コード」がダウンロードされます。

・【モバイルデータ通信専用（OS9 以降）】QR コード ダウンロード

Android9 以降で、キッティング時にモバイルデータ通信を利用する場合の専用 QR コードがダウンロードされます。※Wi-Fi でのキッティングは行えませんのでご注意ください。

・SetUpMaster ダウンロード

端末を Android Enterprise(Work Managed Device)で登録するための「SetUpMaster アプリ」の apk ファイルがダウンロードされます。

■QR コード自動設定項目

各項目に入力し、「保存」ボタンをクリックすると【自動設定】QR コード ダウンロード / 【自動設定/モバイルデータ通信専用（OS9 以降）】QR コード ダウンロードのリンクが作成されます。
作成された自動設定用の QR コードでキッティングを行うと、各項目の内容が自動設定されます。

・グループキー

「自動設定する」にチェックを入れると、Agent のライセンスキー有効化画面で自動的にグループキーが入力されます。

・SSID(サービスセット識別子) / セキュリティの種類 / パスワード

QR コード読込後の設定時に自動的に接続する WiFi を設定できます。

・自由項目

この項目に入力したキーワードが「自由枠1」に自動登録されます。

・ポリシー設定項目

専用 QR コード読み込み時に適用するポリシーを設定することができます。

(サーバ端末間通信 / 緊急時 / 異常検知・通報 / パスワード管理 / デバイス制御 / Wi-Fi 設定)

3 端末登録

1. Work Managed Device端末登録方法

Work Managed Device 登録は端末工場出荷状態から下記の手順で行います。

※機種や Android OS バージョンによって画面表示が異なります。

① 端末を工場出荷状態から、会社管理デバイスとして設定します。方法は複数の種類から選択できます。
このとき管理アプリとして SPPM Agent がインストールされます。
※設定方法により登録後の端末に機能差分は生じません。

②SPPM Agent の登録を行います。
”Android 企業登録”に使用したアカウントの種類での登録手順を確認してください。

①

▼端末初期設定▼

- **QR コード** ※Android OS 7.0 以降の端末のみ対応
- **QR コード** ※Android11 以降
- **SetUpMaster アプリ** ※NFC 対応端末のみ対応
- **G Suite アカウント/Google 管理者アカウント入力**
- **ハッシュタグ <afw#sppm> 入力**

・SPPM Agent インストール（自動）

②

▼SPPM Agent 登録▼

- **G Suite アカウント/Google 管理者アカウント**
- **Managed Google Play アカウント**

端末初期設定方法

■【QRコード】によるキッティング方法

セットアップ用のQRコードの読込みによりキッティングを行います。

※Android OS　7.0　未満の端末ではQRコードの読込みは非対応です。

※Android OS　9.0　以降の端末ではQRコードのセットアップ手順が省略される場合があります。

※Android11以降の場合は☞こちら

※セットアップ用のQRコードはSTAR-MDM管理画面”Android 企業登録”ページからダウンロードできます。

① 初期設定画面
（工場出荷状態）

② 画面を複数回タップしてください。

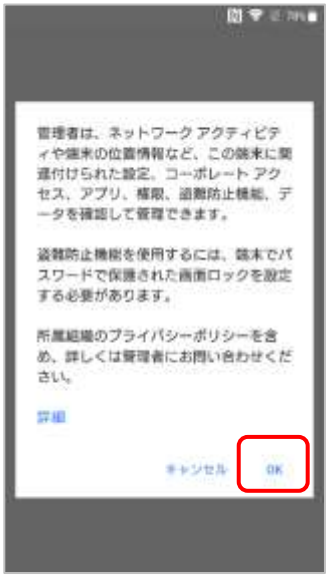
③「次へ」をタップしてください。

④ ネットワークの接続がない場合、WiFi の設定画面が表示されるので接続してください。

⑤ QR リーダーのインストールが行われます。

⑥ QR リーダーが起動するのでセットアップ用の QR コードをカメラで読み込んでください。

➤参照：企業登録情報確認



⑦「OK」をタップしてください。

⑧ 仕事用端末の設定が行われます。

⑨ セットアップが完了します。

※機種により表示内容が異なります。

⑩ SPPM Agent が起動します。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。

下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

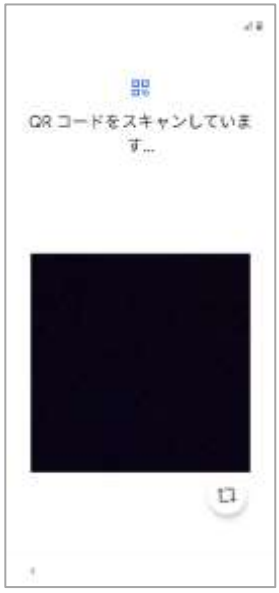
■【QRコード】によるキッティング方法（Android11以降）

セットアップ用のQRコードの読込みによりキッティングを行います。

※セットアップ用のQRコードはSPPM管理画面”Android 企業登録”ページからダウンロードできます。

① 初期設定画（工場出荷状態）

② 画面を複数回タップしてください。

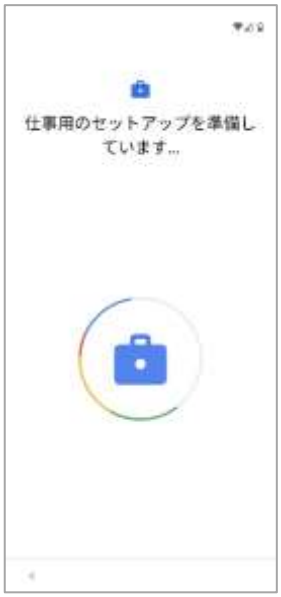


③ QR リーダーが起動するのでセットアップ用の QR コードをカメラで読み込んでください。

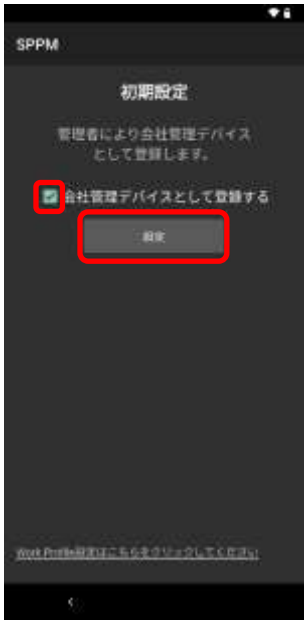
➤参照：企業登録情報確認

④ ネットワークの接続がない場合、WiFi の設定画面が表示されるので接続してください。

⑤「次へ」をタップしてください。



⑥ 仕事用端末のセットアップ準備が行われます。



⑦ **「会社管理デバイスとして登録する」**にチェックを付け、**「設定」**をタップします。

⑧ セットアップが行われます。
「同意して続行」をタップし、案内に従って設定してください。

⑨ 設定が完了します。
※機種により表示内容が異なります。

⑩ SPPM Agent が起動します。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。
下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

■SPPM Agent v3.51以降をご利用の場合

SPPM Agent　v3.51以降をご利用の場合、キッティング後に
「SPPM　管理者により更新されています」の通知が表示される
場合があります。
正常な動作となりますが、通知は自動では消えないため、
必要に応じて手動で削除してください。

■Android 11 以降の場合

Android 11 以降をご利用の場合、キッティング時に
「位置情報のアクセスが許可されています
IT 管理者があなたの位置情報アクセスを SPPM に許可しています」
の通知が表示されます。
正常な動作となりますが、通知は自動では消えないため、
必要に応じて手動で削除してください。

■【SetUpMasterアプリ】によるキッティング方法

セットアップ専用アプリをインストールした端末とのNFC通信によりキッティングを行います。

※NFC非対応端末ではSetUpMasterアプリによる設定は非対応です。

※AndroidOS10以降では非推奨です。端末によっては利用できない場合もあります。

≪事前準備≫

・キッティング対象端末とは別のNFC対応端末を用意し、SetUpMasterアプリをインストールしてください。
SetUpMasterアプリのapkファイルはSTAR-MDM管理画面”Android企業登録”ページからダウンロードできます。

・SetUpMasterアプリをインストールした端末のNFC機能をONにしてください。

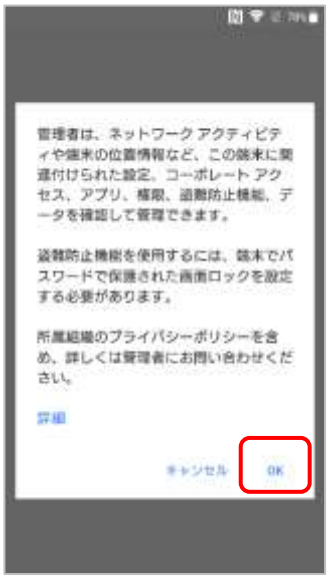
① 「SetUpMaster」を起動した端末を用意。

② キッティング対象端末の初期設定画面を表示。

③ ①と②の端末の NFC 接続部分を重ねると端末の画面が変化します。その状態で端末の画面をタップしてください。

※NFC マーク/Felica マークの位置は端末によって異なります。

④ ネットワークの接続がない場合、
WiFi の設定画面が表示されるので
接続して「次へ」をタップしてください。



⑤「OK」をタップしてください。

⑥ 仕事用端末の設定が行われます。

⑦ セットアップが完了します。
※機種により表示内容が異なります。

⑧ SPPM Agent が起動します。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。
下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

■Android 11 以降の場合

Android 11 以降をご利用の場合、
キッティング時に「位置情報のアクセスが
許可されています IT 管理者があなたの
位置情報アクセスを SPPM に許可しています」
の通知が表示されます。
正常な動作となりますが、通知は自動では
消えないため、必要に応じて手動で削除して
ください。

■【G Suiteアカウント/Google管理者アカウント入力】によるキッティング方法

端末の初期設定時のGoogleアカウント入力画面で「G Suiteアカウント/Google管理者アカウント」を入力し、キッティングを行います。

※Managed Google Play アカウントをご利用の場合、この方法での初期設定は非対応です。

① 初期設定画面で「開始する」をタップしてください。

② セットアップを進め、ネットワーク接続がない場合は WiFi に接続してください。

③ G Suite アカウントまたは Google 管理者アカウントの管理対象となっているユーザーアカウントを入力してください。

④ アカウントのパスワードを入力し**「次へ」**をタップしてください。

⑤ **「同意する」**をタップしてください。

⑥ 情報の確認が行われます。

⑦ 「**インストール**」を
タップしてください。

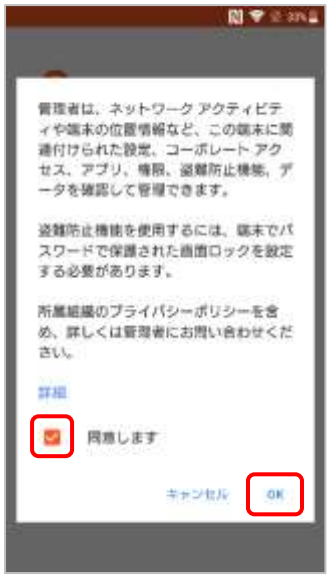
⑧ SPPM Agent のダウンロードが
実施されます。

⑨ 「**インストール**」をタップして
ください。

⑩ SPPM Agent の初期設定画面が
表示されます。

⑪ チェックを ON にして、
「**設定**」をタップしてください。

⑫ 「**次へ**」をタップしてください。



⑬ チェックを ON にして、
「OK」をタップしてください。

⑭ 仕事用端末の設定が行われます。

⑮ セットアップが完了します。
※機種により表示内容が異なります。

⑯ SPPM Agent が起動します。

■SPPM Agent 登録方法について

本設定方法は「G Suiteアカウント/Google管理者アカウント」での登録のみ有効のため下記からSPPM Agentの登録方法をご確認ください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

■Android 11 以降の場合

Android 11 以降をご利用の場合、
キッティング時に「位置情報のアクセスが許可されています IT 管理者があなたの位置情報アクセスを SPPM に許可しています」の通知が表示されます。
正常な動作となりますが、通知は自動では消えないため、必要に応じて手動で削除してください。

■【ハッシュタグ入力】によるキッティング方法

EMM識別子（afw#sppm）の入力によりデバイスのキッティングを行います。

※SPPM Agent v3.51未満で対応している機種では、動作未検証のため非推奨です。

① 初期設定画面
（工場出荷状態）

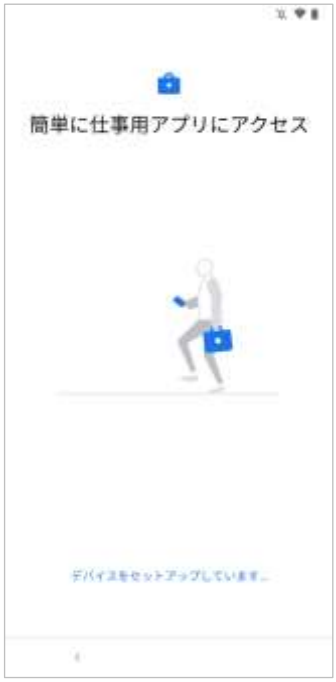
② Google アカウントのログイン画面まで設定を進み、メールアドレスの入力欄に「afw#sppm」と入力し「次へ」を押してください

③インストールを押してください

④インストールを押してください

⑤「会社管理デバイスとして登録する」にチェックをいれて設定を押してください

⑥「同意して続行」を押します



⑦ 設定が完了するまで待ちます

⑧「次へ」を押します

⑨「同意して続行」を押します

⑩ SPPM Agent が起動します。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。
下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

■Android 11 以降の場合

Android 11 以降をご利用の場合、
キッティング時に「位置情報のアクセスが許可されています IT 管理者があなたの位置情報アクセスを SPPM に許可しています」の通知が表示されます。
正常な動作となりますが、通知は自動では消えないため、必要に応じて手動で削除してください。

SPPM Agent 登録方法

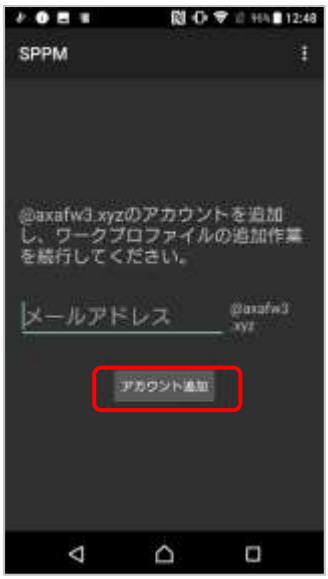
■【G Suiteアカウント / Google管理者アカウント】

① 「**許可する**」をタップしてください。

② 必要な権限を ON にしてください。
バックキーをタップすると①の画面に戻るので全ての権限が ON になるまで権限の許可を続けて下さい。

③ 12 桁の「**グループキー**」を入力し、「**G Suite / Google**」にチェックを付けてください。

④ 「**設定**」ボタンをタップしてください。



⑤ ユーザーが使用するアカウントを入力し、「**アカウント追加**」ボタンをタップしてください。
※端末初期画面からアカウント入力でセットアップした方は同じアカウントを入力してください。

⑥ アカウントのパスワードを入力し、「**次へ**」ボタンをタップしてください。

⑦ 「次へ」をタップしてください。

⑧ SafetyNet による端末検査と管理サーバへの登録が行われます。

⑨ 登録完了。

≪正常な登録完了の確認について≫

■Google アカウント登録

端末の Google アカウントに、SPPM Agent 登録時に追加したアカウントが登録されています。

■Google Play ストア

端末の Google Play ストアが、Android Enterprise 専用の表示になっています。

※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。

■【Managed Google Play アカウント】

① 「**許可する**」をタップしてください。

② 必要な権限を ON にしてください。バックキーをタップすると①の画面に戻るので全ての権限が ON になるまで権限の許可を続けて下さい。

③ 12 桁の「**グループキー**」を入力し、「**Managed Google Play**」にチェックを付けてください。

④ 「**設定**」ボタンをタップしてください。

⑤ 登録に必要な環境を構築します。

⑥ SafetyNet による端末検査と管理サーバへの登録が行われます。

⑦ 登録完了。

≪正常な登録完了の確認について≫

■管理アカウント登録

端末に管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、
管理者による準備は必要ありません。

■Google Play ストア

端末の Google Play ストア Android Enterprise 専用の表示になっています。

※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。

2. Work Profile端末登録方法

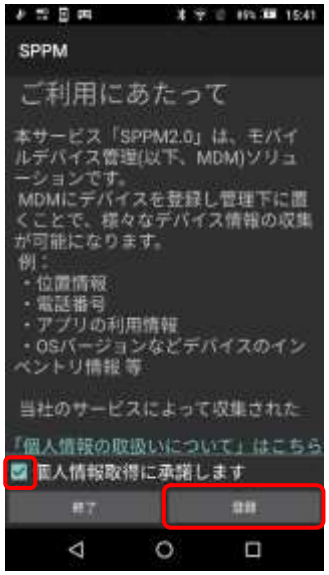
Android Enterprise (Work Profile) 登録は現在使用中の端末に SPPM Agent をインストールして利用できます。
”Android 企業登録”に使用したアカウントの種類での登録手順を確認してください。
※Work Managed Device とは異なり端末工場出荷状態からの設定は必要ありません。
※各手順画像は Nexus5X の画面です。機種や Android OS バージョンによって画面表示が異なります。

▼SPPM Agent 登録▼

- G Suite アカウント/Google 管理者アカウント
- Managed Google Play アカウント

SPPM Agent 登録方法

■【G Suiteアカウント / Google管理者アカウント】



① Play ストアから SPPM をインストールし、Agent を起動します。
SPPM v3.59.1.1 以降の場合は、利用許諾画面にて**「個人情報取得に承諾します」**にチェックを付け、**「登録」**をタップしてください。

② 権限催促画面で**「許可する」**をタップしてください。

③ 必要な権限を ON にしてください。
バックキーをタップすると②の画面に戻るので、全ての権限が ON になるまで権限の許可を続けて下さい。

④ 12 桁の**「グループキー」**を入力し、**「WorkProfile を使用する」**
にチェックをいれ、
「G Suite / Google」にチェックを
付けてください。

⑤ **「設定」**ボタンをタップしてください。

⑥ **「同意して続行」**ボタンをタップしてください。

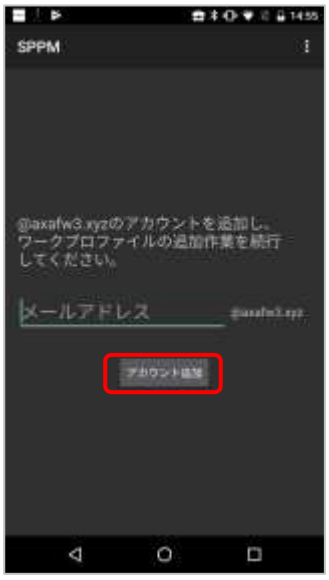
⑦ 仕事用プロファイルの
セットアップが行われます。

⑧ 一度ホーム画面に戻ります。
この時、SPPM を起動しないでください。

⑨ SafetyNet 機能による端末
検査が実施されます。

⑩ 管理サーバ通信とポリシー
更新確認が行われます。

⑪ Agent 画面に遷移します。



⑫ ユーザーが使用するアカウントを入力し、
「アカウント追加」をタップしてください。
※Agent 画面を一度閉じて、再度 Agent
画面を開き直す必要があります。

⑬ 情報の確認が行われます。

⑭ アカウントを確認し、「**次へ**」ボタンをタップしてください。

⑮ アカウントのパスワードを入力し、「**次へ**」ボタンをタップしてください。

⑯ 「**同意する**」をタップしてください。

⑰ 情報の確認が行われます。

⑱ 登録完了。

■SPPM Agent3.51 以降の場合

⑱の画面の後に「他のアプリの上表示」の権限が要求されます。
表示された場合は許可してください。
※Android10 の場合は通知から設定を完了する必要があります。

＜Android10 で表示される通知の例＞

■Android 12 以降の場合

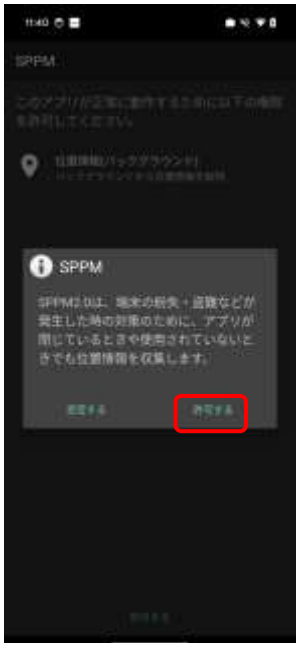
⑱の画面の後に「他のアプリの上に重ねて表示」以外の権限も要求されます。表示された場合は許可してください。

また、「位置情報」の権限を許可する際、「正確」を選択して許可してください。

＜位置情報の権限許可画面＞

① 「許可する」を選択します

②「アプリの使用時のみ」または「今回のみ」を選択します



③「許可する」を選択します

④ 「常に許可」を選択します

※「常に許可」を選択しなかった場合、
許可を促す通知が表示されます

≪正常な登録完了の確認について≫

■管理アカウント

仕事用アカウントに管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、管理者による準備は必要ありません。

■Work Profile アプリ

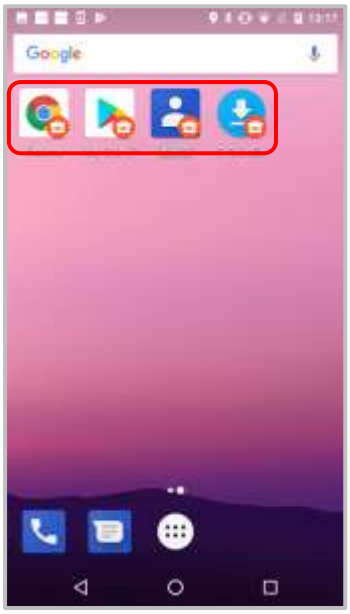
端末内の一部アプリが仕事用アプリとしてアイコンにバッジがついた状態で複製されます。※仕事用アプリとして複製されるアプリは OS により判定されており、端末毎で異なる場合があります。

(例)Nexus5X では Chrome/Play ストア/連絡先/ダウンロード

■Google Play ストア

端末の Google Play ストアが Android Enterprise 専用の表示になっています。

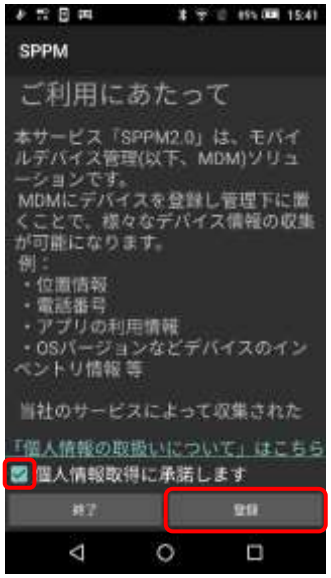
※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。



【管理アカウントの追加】

「管理用アカウントを追加しました」
というメッセージが表示されます。

■【Managed Google Play アカウント】



① Play ストアから SPPM をインストールし、Agent を起動します。
SPPM v3.59.1.1 以降の場合は、利用許諾画面にて**「個人情報取得に承諾します」**にチェックを付け、**「登録」**をタップしてください。

② 権限催促画面で**「許可する」**をタップしてください。

③ 必要な権限を ON にしてください。
バックキーをタップすると②の画面に戻るので、全ての権限が ON になるまで権限の許可を続けて下さい。

④ 12 桁の**「グループキー」**を入力し、**「WorkProfile を使用する」**にチェックをいれ、**「Managed Google Play」**にチェックを付けてください。

⑤ **「設定」**ボタンをタップしてください。

⑥ **「同意して続行」**ボタンをタップしてください。

⑦ 仕事用プロファイルの
セットアップが行われます。

⑧ 一度ホーム画面に戻ります。
この時、SPPM を起動しないでください。

⑨ SafetyNet 機能による端末
検査が実施されます。

⑩ 管理サーバ通信とポリシー
更新確認が行われます。

⑪ 登録完了。

■SPPM Agent3.51 以降の場合

⑩の画面の後に「他のアプリの上表示」の権限が要求されます。
表示された場合は許可してください。
※Android10 の場合は通知から設定を完了する必要があります。

＜Android10 で表示される通知の例＞

■Android 12 以降の場合

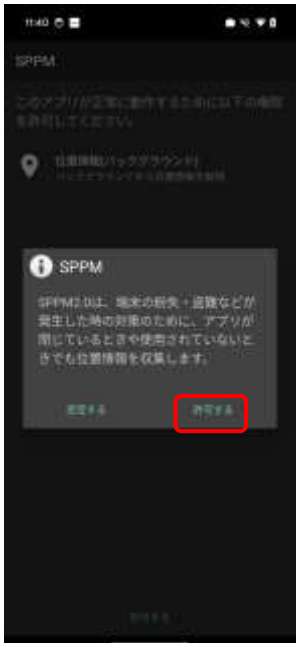
⑱の画面の後に「他のアプリの上に重ねて表示」以外の権限も要求されます。表示された場合は許可してください。

また、「位置情報」の権限を許可する際、「正確」を選択して許可してください。

＜位置情報の権限許可画面＞

① 「許可する」を選択します

②「アプリの使用時のみ」または「今回のみ」を選択します



③「許可する」を選択します

④ 「常に許可」を選択します

※「常に許可」を選択しなかった場合、
許可を促す通知が表示されます

≪正常な登録完了の確認について≫

■管理アカウント

仕事用アカウントに管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、管理者による準備は必要ありません。

■Work Profile アプリ

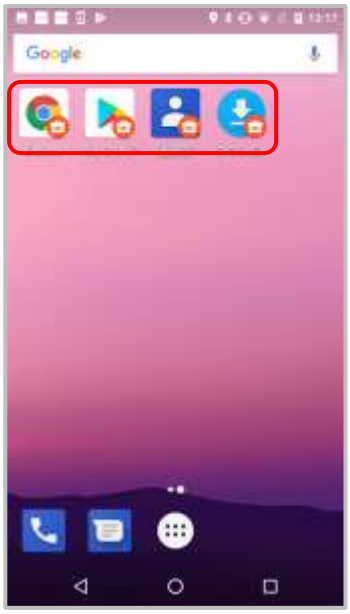
端末内の一部アプリが仕事用アプリとしてアイコンにバッジがついた状態で複製されます。※仕事用アプリとして複製されるアプリは OS により判定されており、端末毎で異なる場合があります。

(例)Nexus5X では Chrome/Play ストア/連絡先/ダウンロード

■Google Play ストア

端末の Google Play ストアが Android Enterprise 専用の表示になっています。

※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。



【管理アカウントの追加】

「管理用アカウントを追加しました」
というメッセージが表示されます。

3. Work Profile[企業所有]端末登録方法

Android Enterprise (Work Profile[企業所有]) 登録は端末工場出荷状態から下記の手順で行います。
”Android 企業登録”に使用したアカウントの種類での登録手順を確認してください。
※Work Profile[企業所有]のキッティングは Android11 以降から利用できます。
※各手順画像は機種や Android OS バージョンによって画面表示が異なります。

①端末を工場出荷状態から、会社管理デバイスとして設定します。
このとき管理アプリとして SPPM がインストールされます。
②SPPM Agent の登録を行います。
”Android 企業登録”に使用したアカウントの種類での登録手順を確認してください。

①

▼端末初期設定▼

・QR コード

・SPPM Agent インストール（自動）

②

▼SPPM Agent 登録▼

・G Suite アカウント/Google 管理者アカウント

・Managed Google Play アカウント

端末初期設定方法

■【QRコード】によるキッティング方法

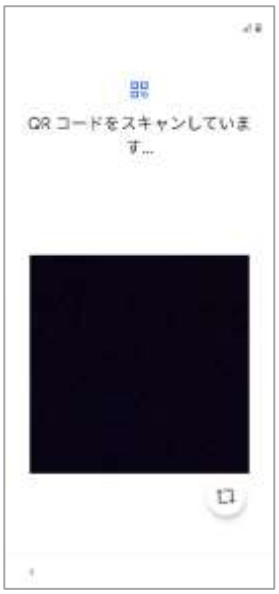
セットアップ用のQRコードの読込みによりキッティングを行います。

※Android OS　9.0　以降の端末ではQRコードのセットアップ手順が省略される場合があります。

※セットアップ用のQRコードはSTAR-MDM管理画面”Android 企業登録”ページからダウンロードできます。

① 初期設定画(工場出荷状態)

② 画面を複数回タップしてください。

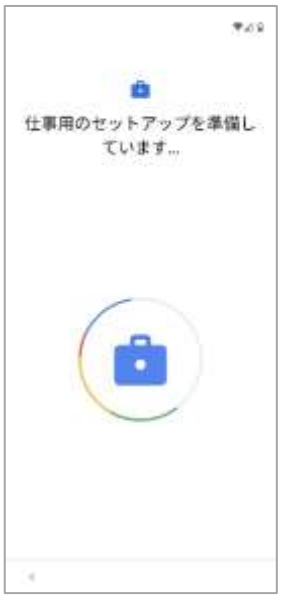


③ QR リーダーが起動するのでセットアップ用の QR コードをカメラで読み込んでください。

➤参照:企業登録情報確認

④ ネットワークの接続がない場合、WiFi の設定画面が表示されるので接続してください。

⑤「次へ」をタップしてください。



⑥ 仕事用端末のセットアップ準備が行われます。

⑦「**Work Profile 設定はこちらをクリックしてください**」をタップします。

⑧ 仕事用端末の設定が行われます。
「同意して続行」をタップし、案内に従って設定してください。

⑨ セットアップが完了します。
案内に従って画面をスワイプしてください。
※機種により表示内容が異なります。

⑩ ホーム画面に追加された SPPM のアイコンをタップし、SPPM Agent を起動してください。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。
下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

■SPPM Agent v3.51以降をご利用の場合

SPPM Agent　v3.51以降をご利用の場合、キッティング後に
「STAR-MDM　管理者により更新されています」の通知が表示される場合があります。
正常な動作となりますが、通知は自動では消えないため、
必要に応じて手動で削除してください。

■Android 11 以降の場合

Android 11 以降をご利用の場合、キッティング時に
「位置情報のアクセスが許可されています
IT 管理者があなたの位置情報アクセスを SPPM に許可しています」
の通知が表示されます。
正常な動作となりますが、通知は自動では消えないため、
必要に応じて手動で削除してください。

SPPM Agent 登録方法

■【G Suiteアカウント / Google管理者アカウント】

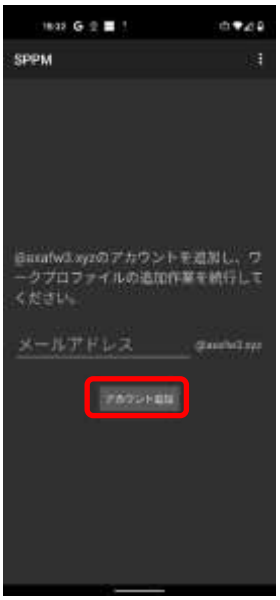
① 「**許可する**」をタップしてください。

② 必要な権限を ON にしてください。バックキーをタップして①の画面に戻った場合、全ての権限が ON になるまで権限の許可を続けて下さい。

③ 12 桁の「**グループキー**」を入力し、「**G Suite / Google**」にチェックを付けてください。

④ 「**設定**」ボタンをタップしてください。

⑤ SafetyNet による端末検査と管理サーバーへの登録が行われます。



⑥ ユーザーが使用するアカウントを入力し、「**アカウント追加**」をタップしてください。
※Agent 画面を一度閉じて、再度 Agent 画面を開き直す必要があります。

⑦「次へ」をタップしてください。

⑧ 追加したアカウントのパスワードを入力して「次へ」をタップしてください。

⑨「同意する」をタップしてください。

⑩ 登録完了

■Android 12 以降の場合

⑱の画面の後に「他のアプリの上に重ねて表示」以外の権限も要求されます。表示された場合は許可してください。

また、「位置情報」の権限を許可する際、「正確」を選択して許可してください。

＜位置情報の権限許可画面＞

① 「許可する」を選択します

②「アプリの使用時のみ」または「今回のみ」を選択します

③「許可する」を選択します

④ 「常に許可」を選択します

※「常に許可」を選択しなかった場合、
許可を促す通知が表示されます

≪正常な登録完了の確認について≫

■管理アカウント

仕事用アカウントに管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、管理者による準備は必要ありません。

■Work Profile アプリ

端末内の一部アプリが仕事用アプリとしてアイコンにバッジがついた状態で複製されます。※仕事用アプリとして複製されるアプリは OS により判定されており、端末毎で異なる場合があります。

■Google Play ストア

端末の Google Play ストアが Android Enterprise 専用の表示になっています。

※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。

【管理アカウントの追加】

「管理用アカウントを追加しました」というメッセージが表示されます。

■【Managed Google Play アカウント】

① 「**許可する**」をタップしてくださ

② 必要な権限を ON にしてください。バックキーをタップすると①の画面に戻るので全ての権限が ON になるまで権限の許可を続けて下さい。

③ 12 桁の「**グループキー**」を入力し、「**Managed Google Play**」にチェックを付けてください。

④ 「**設定**」ボタンをタップしてください。

⑤ 登録に必要な環境の構築や、サーバ通信などが行われます。

⑥ 登録完了。

■Android 12 以降の場合

⑱の画面の後に「他のアプリの上に重ねて表示」以外の権限も要求されます。表示された場合は許可してください。

また、「位置情報」の権限を許可する際、「正確」を選択して許可してください。

＜位置情報の権限許可画面＞

① 「許可する」を選択します

②「アプリの使用時のみ」または「今回のみ」を選択します

③「許可する」を選択します

④ 「常に許可」を選択します

※「常に許可」を選択しなかった場合、
許可を促す通知が表示されます

≪正常な登録完了の確認について≫

■管理アカウント

仕事用アカウントに管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、管理者による準備は必要ありません。

■Work Profile アプリ

端末内の一部アプリが仕事用アプリとしてアイコンにバッジがついた状態で複製されます。※仕事用アプリとして複製されるアプリは OS により判定されており、端末毎で異なる場合があります。

■Google Play ストア

端末の Google Play ストアが Android Enterprise 専用の表示になっています。

※ストア内のアプリ表示は管理画面の「Play Store レイアウト設定」から設定が必要です。

【管理アカウントの追加】

「管理用アカウントを追加しました」というメッセージが表示されます。

4. Comp端末登録方法

Android Enterprise（Comp）登録は Work Managed Device にキッティング完了後、下記の手順で行います。

1、「管理画面 TOP 画面>その他> Comp 設定」の画面で「Work Managed Device 端末で Work Profile 作成機能を有効化する」の項目にチェックを入れてください。
※「G Suite アカウント/Google 管理者アカウント」で企業登録されている場合は非対応となります。
※その他の詳細な設定方法については[Comp / Work Profile[企業所有] 設定]をご確認ください。

2、端末を Work Managed Device でキッティング
キッティング方法に関しては「Work Managed Device 端末登録方法」をご確認ください。

3、Agent 画面右上のメニューボタンから以下の手順で Work Profile を作成してください。

① SPPM Agent 画面右上の**メニューボタン**をタップする

②メニュー内の**「Work Profile 作成」**をタップする

③仕事用プロファイルのセットアップ画面が表示されます。

仕事用プロファイルのセットアップ画面で待機すると、その後、
【仕事領域 SPPM の権限許可】と【Work Pofile（仕事領域）の構築】が並行して表示されます。
権限の許可は仕事環境設定等のメッセージが表示されている間に同時に操作しても問題ありません。

【仕事領域 SPPM の権限許可】

④「使用履歴へのアクセス」の
権限催促画面が表示されますので
「許可する」をタップしてください。

⑤「使用履歴へのアクセス」の
バッジ付き STAR-MDM の項目を
タップしてください。

⑥使用履歴へのアクセスを
ON にしてください。

【Work Profile（仕事領域）の構築】

④「仕事環境を設定しました」
というメッセージが表示されます。

⑤「管理用アカウントを追加しました」
というメッセージが表示されます。

≪正常な登録完了の確認について≫

■管理アカウント

仕事用アカウントに管理アカウントが登録されます。

※管理アカウントは自動で発行されるため、管理者による準備は必要ありません。

■Work Profile アプリ

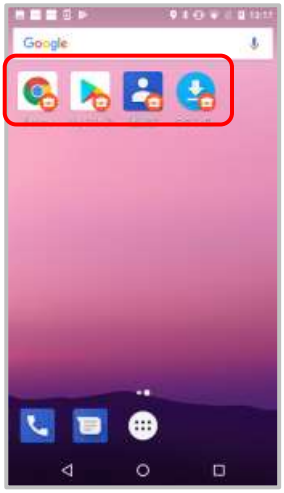
端末内の一部アプリが仕事用アプリとしてアイコンにバッジがついた状態で複製されます。※仕事用アプリとして複製されるアプリは OS により判定されており、端末毎で異なる場合があります。

(例)Nexus5X では Chrome/Play ストア/連絡先/ダウンロード

■常駐通知

従来の Agent 常駐通知に加えてバッジ付き Agent の常駐通知が表示されます。

※バッジ付きの常駐通知をタップしても SPPM Agent 画面は起動しません。



端末によっては Comp 作成時に「Google Play ストアが停止しました」というダイアログが表示される場合がありますが、その後の動作に問題はありません。

5. Zero-touch enrollmentによるキッティング方法

■Zero-touch enrollmentとは

Zero-touch enrollment（以下、Zero-touch）は、Google社の提供する端末導入・設定の支援サービスです。SPPMと Zero-touch を併せて用いることで、従来必要とされていたキッティング（初期設定）の手間を大幅に削減し、STAR-MDMによる制御をより強固なものにすることができます。

Zero-touchを利用してキッティングをするためにはGoogle社の提供する“Zero-touch”専用 ポータルページ（以下、Zero-touchポータル）に予めSTAR-MDMへの登録情報を設定する必要があります。

■Zero-touch enrollmentの利点

Zero-touch を利用することにより、STAR-MDM のキッティング（初期設定）作業を一括して行うことができます。従来はユーザの端末 1 台 1 台に対してグループキー登録などの作業が必要であり、多数の端末をご利用の場合にはキッティング作業に時間がかかっていました。

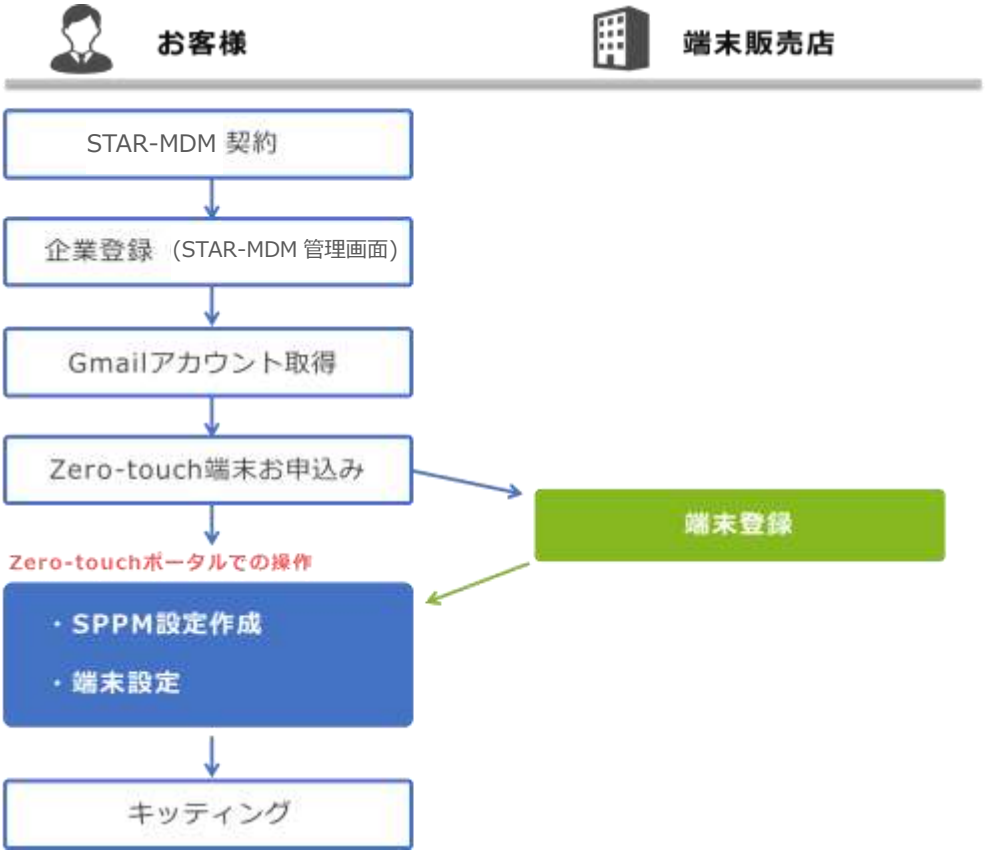
Zero-touch を用いることで、管理者が一括して、リモートでキッティング作業を行うことが可能になります。端末側では初回起動時にわずかな認証操作を行うだけで、SPPM Agent のインストールが完了します。また、Zero touch の設定により、初回起動時の認証を完了させるまで、端末の機能を制限することができるため、端末を確実に MDM の管理下に置くことができます。

■初期設定（事前準備）

・STAR-MDM ご契約後、STAR-MDM 管理画面より企業登録を行います。

・Zero-touch ポータルを利用するための、Gmail アカウントを取得します。

・端末販売店で、Zero-touch 対応端末を購入し、Zero-touch 利用申請を行います。



■Zero-touch enrollment でのキッティング方法

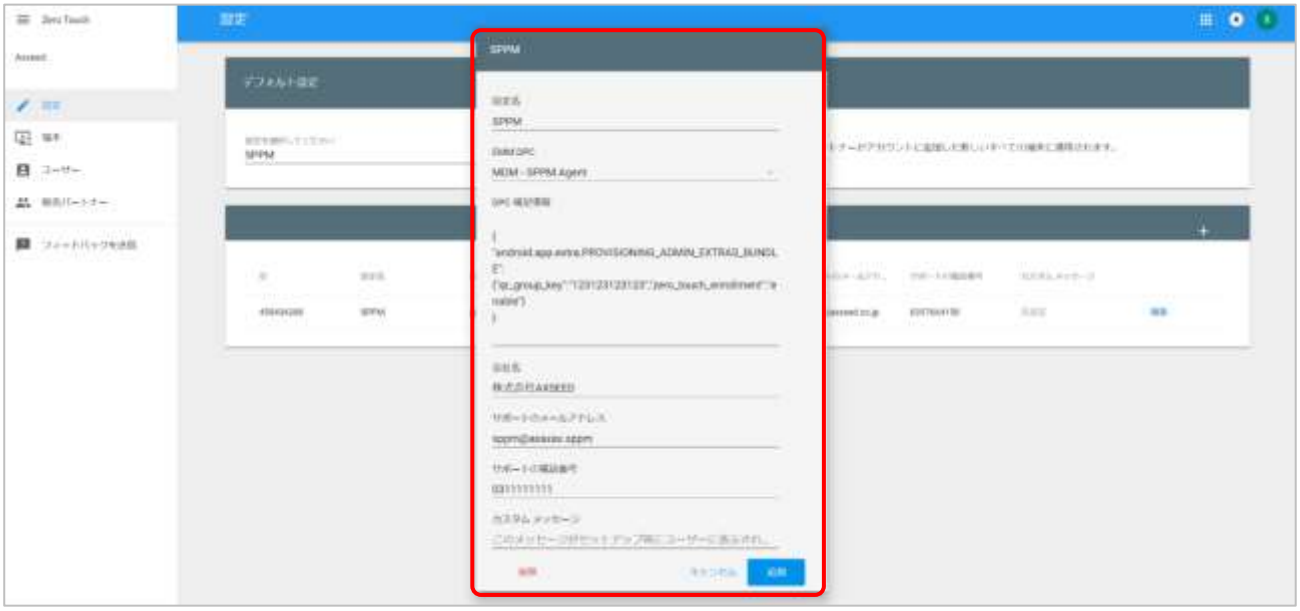
Zero-touch ポータルでの操作

<<新規設定の作成>>

端末に登録する STAR-MDM の設定を作成します。

Zero-touch ポータル（https://partner.android.com/zerotouch）にアクセスし、事前に利用者登録を行った Gmail アカウント/パスワードでサインインしてください。

1.[設定]>[+]をクリックしてください。



2.[設定名]に「STAR-MDM」等わかりやすい名称を入力してください。

3.[EMM DPC]で[MDM - SPPM Agent]を選択してください。

4.[DPC 補足情報]に SPPM に登録するためのデータを記載します。

```
{
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"qr_group_key":"(グループキー)","zero_touch_enrollment":"enable"}
}
```

※ (グループキー)"には、キッティングに使用する 12 桁のグループキーを入力してください。

※"zero_touch_enrollment":"enable"を設定すると、SPPM のライセンス有効化画面を閉じることができなくなります。また、端末の権限要求が STAR-MDM への登録後に表示されます。

設定しない場合は、"zero_touch_enrollment":"enable"を入力しないでください。

■端末の権限要求

STAR-MDM への登録が完了すると、権限要求画面が表示されます。

[許可する]をタップし、必要な権限を全て ON にしてください。

端末のバックキーを押すと、再度権限要求画面が表示されます。

※ "qr_company_type":"managed" を追加することにより、SPPM のライセンス有効化画面で Managed Google Play に自動的にチェックが入ります。

```
{
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"qr_group_key":"(グループキー)","zero_touch_enrollment":"enable",
"qr_company_type":"managed"}
}
```

5. [会社名]、[サポートのメールアドレス]、[サポートの電話番号]を入力してください。
   また、必要に応じて[カスタムメッセージ]を入力してください。
   ここで入力されたデータは、キッティング時に端末に表示されます。

今後、新規で Zero-touch ポータルに登録される端末全てに同じ設定を適用する場合は、
デフォルト設定に指定し[適用]してください。
※既に登録済みの端末にはデフォルト設定は適用されません。

<<端末設定>>

作成した設定を端末に 1 台ずつ適用します。

1.[端末]をクリックします。

2.IMEI またはシリアル番号を使って、設定を適用する端末を検索します。

3.[設定]から適用する設定を指定します。

<<端末キッティング>>

これまでの各設定が完了している状態で、Zero-touch 端末のキッティング（アクティベート時）に、Zero-touch ポータルで設定した内容が反映されます。

※インターネット接続無しで設定を行うと、セットアップ完了後インターネット接続をした際に端末が初期化されますのでご注意ください。

① 端末の表示に従って、キッティングを開始します。

② ネットワークの接続がない場合、WiFi の設定画面が表示されるので接続してください。

■「組織の管理者」をクリックすると、Zero-touch ポータルで事前に設定した情報が表示されます。

③ 規約に同意し、設定を続けます。

④ 仕事用端末の設定が行われます。

⑤ 「同意する」をタップします。

■SPPM Agent 登録方法について

「SPPM Agent」の登録方法は”Android企業登録”の種類によって異なります。

下記から環境に合わせた方法を確認し、登録を行ってください。

「G Suiteアカウント/Google管理者アカウント」での登録方法はこちら

「Managed Google Play アカウント」での登録方法はこちら

⑥ SPPM Agent が起動します。

このとき DPC 補足情報に入力したグループキーが自動挿入されます。

なお、DPC 補足情報に″zero_touch_enrollment″:″enable″を設定すると、

ライセンス有効化画面を閉じたり、端末のバックキーで戻ったりすることができなくなります。

また、STAR-MDM への登録完了後に、端末の権限要求画面が表示されます。

4 Android Enterprise 機能 / ポリシー

1. 各管理モードにおけるAndroid Enterprise機能 概要

Android Enterprise 端末では各ポリシーにおいて通常の機能に加え、Android Enterprise 専用の機能を利用できます。各ポリシーの詳細な設定方法は「STAR-MDM 管理者マニュアル（Android 版）」をご確認ください。
また、Android Enterprise 端末では管理モードにより利用できるポリシーが異なります。
※ポリシーによっては通常機能からAndroid Etnerprise専用の機能に切り替わります。
※E-SDK/E-API機能はAndroid Enterprise機能とは併用できません。

【管理モード別対応ポリシー表】

	WorkManagedDevice	WorkProfile	Comp (WorkProfile)
サーバ端末間通信	○	○	
緊急時	○	○	○
異常検知・通報	○	○	
Agent 管理	○	○	
パスワード管理	○	○	
デバイス制御	○	○	○
発着信番号履歴	○		
発着信番号制限	○		
位置情報取得	○	○	
アプリ配信	○		
利用アプリ制限	○		
アプリ一覧	○	○	
Wi-Fi 接続先制限	○		
接続先 URL 制限	○		
ファイル配布	○		
Wi-Fi 設定	○	○	
SIM 監視	○		
メッセージ配信	○	○	
電話帳配信	○		
アプリアンインストール制限	○	○	
動態管理	○		
利用統計	○		

※Android OS 依存により利用できないポリシーや AndroidEnterprise で利用する必要のない端末暗号義務化ポリシーは一覧から省かれています。
※Comp (WorkProfile)は Comp 端末において Work Managed Device に加え Work Profile で利用できるポリシーです。Work Profile 単体での利用時と利用できる機能が異なるためご注意下さい。

Work Managed Device

■緊急時ポリシー

Android OS 6.0 以降の端末でもWi-Fi情報のデータ消去が有効です。

E-API機能による外部メモリのデータ消去が有効です。※SPPM Agent v3.43以降対応

ハードリセット指示時に「ファクトリーリセット保護の無効化」を選択できます。※SPPM Agent v3.40以降対応

※ファクトリーリセット保護の詳細についてはデバイス制御「ファクトリーリセット保護」をご確認ください。

■パスワード管理ポリシー

パスワード更新催促画面が閉じられてから端末ロックが実施されるまでの時間を設定できます。

Android OS 7.0 以降の端末でもパスワード初期化指示が有効です。

■デバイス制御ポリシー

Android Enterprise専用の各制御項目を設定できます。詳細はこちら。

※通常の[Android]デバイス制御項目との併用は非対応です。

■位置情報取得ポリシー

ポリシー適用時に、[位置情報設定有効義務化]で選択された項目によって

端末設定内の位置情報取得方法が自動設定されます。

■利用アプリ制限ポリシー

制限対象となるアプリを2つの制御モードから選択し、通常のブロック画面制限より強力な制限ができます。

ホワイトリストで許可されているアプリのアンインストール制限を設定できます。

※SppmHome、apk展開の許可設定、制限アプリの無効化/アンインストール催促機能は非対応です。

※ホームアプリを全て制限しているとホーム画面が正常に表示されなくなるためご注意ください。

※非常用節電モード/緊急省電力モードは利用アプリ制限ポリシーでは制御できません。

関連情報☞「非常用節電モード/緊急省電力モードを許可する」

※PlayStoreのログインアカウントをAndroid Entereprise管理外のGoogleアカウントを端末に切り替えた場合、通常のPlayStoreを表示します。

そのため、Googleアカウントの追加をデバイス制御ポリシーで禁止することを推奨します。

※設定方法の詳細はAndroid管理者マニュアルをご確認ください。

■アプリアンインストール制限ポリシー

パッケージ名を指定したアプリのアンインストールを禁止します。

Work Profile

■緊急時ポリシー

従来とは緊急指示画面の表示や動作が異なります。

端末ロック⇒Work Profile(仕事領域)ロック

ハードリセット⇒Work Profile(仕事領域)の削除

【Work Profile ロック】

仕事用アプリの利用が制限されます。また、ロック中でも個人領域は普段どおりに利用できます。

※仕事用のGooglePlayストアは制限できません。ただし、ロック中であれば仕事用GooglePlayストアから
インストールされたアプリは全て利用が制限されます。

【データ消去】

仕事領域のデータのみ消去対象となります。個人領域で作成されたデータは削除されません。

【Work Profile 削除指示】

従来のハードリセット機能とは異なり、端末の初期化ではなく作成されたWork Profileが削除されます。

①緊急指示画面で「Work Profile 削除指示」ボタンを押下

②確認画面で「はい」を押

■パスワード管理ポリシー

端末本体（個人領域）と仕事領域のパスワード制御を個別に行うことができます。

■デバイス制御ポリシー

Android Enterprise専用の各制御項目を設定できます。詳細はこちら。

※通常の[Android]デバイス制御項目との併用は非対応です。

■アプリー覧ポリシー

仕事用アプリー覧を取得できます。

※個人領域のアプリ情報は取得できません。

■アプリアンインストール制限ポリシー

パッケージ名を指定した仕事用アプリのアンインストールを禁止します。

Comp （Work Profile）

■緊急時ポリシー

端末ロックとハードリセット（仕事領域の削除）機能のみ有効です。

【端末ロック】

Android OS 8.0 においてWork Managed Deviceと同様にWork Profileのアプリが制限されます。

※Work Managed DeviceとWork Profileのロック指示は個別に発令できません。

※緊急時ポリシー（WP）の設定は「ハードリセット」のみ有効です。「端末ロック」の発動条件等の設定はWork Managed Deviceと共通となります。

【ハードリセット】

従来のハードリセット機能とは異なり、端末の初期化ではなく作成されたWork Profileが削除されます。

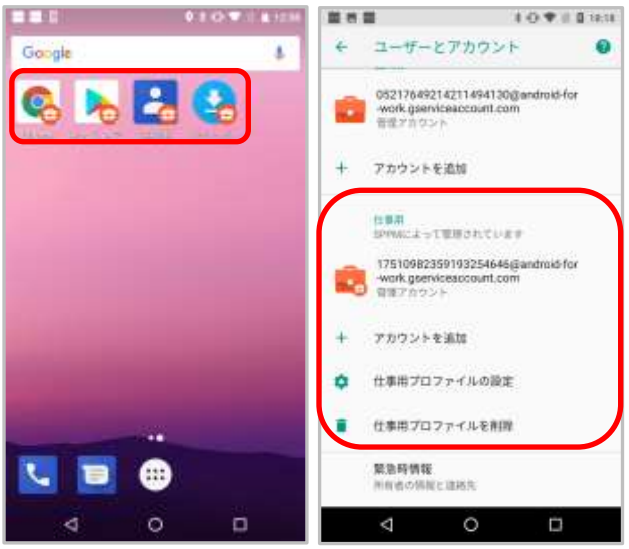
また、管理画面の緊急指示はハードリセットを選択後に、「ハードリセット指示（端末初期化）」と「Work Profile削除指示（仕事領域削除）」のどちらかを選択可能です。

①緊急指示画面で
「ハードリセット」ボタンを押下

②選択画面に遷移後、
「Work Profile 解除指示」を押下

③確認画面で「はい」を押下

ハードリセット前



ハードリセット後

■デバイス制御ポリシー

Android Enterprise専用の各制御項目を設定できます。詳細はこちら。

※通常の[Android]デバイス制御項目との併用は非対応です。

Comp（WorkProfile）ではWorkProfileポリシーで対応している機能のみご利用可能です。

個人領域の電話帳配信ポリシーで配信した連絡先は仕事領域の電話帳アプリでは閲覧できません。

Work Profile [企業所有]

■緊急時ポリシー

従来とは緊急指示画面の表示や動作が異なります。

端末ロック⇒個人領域も合わせてロックする(Android11以降のWork Profile[企業所有]のみ有効)

ハードリセット⇒個人領域も合わせてハードリセット(ワイプ)する(Android11以降のWork Profile[企業所有]のみ有効)

【Work Profile ロック】

・緊急時ポリシー＞「個人領域も合わせてロックする」にチェックがない場合

仕事用アプリの利用が制限されます。また、ロック中でも個人領域は普段通りに利用できます。

※仕事用のGooglePlayストアは制限できません。ただし、ロック中であれば仕事用GooglePlayストアからインストールされたアプリは全て利用が制限されます。

・緊急時ポリシー＞「個人領域も合わせてロックする」にチェックがある場合

仕事領域と個人領域のアプリの利用が制限されます。

※仕事用のGooglePlayストアは制限できません。ただし、ロック中であれば仕事用GooglePlayストアからインストールされたアプリは全て利用が制限されます。

【データ消去】

仕事領域のデータのみ消去対象となります。個人領域で作成されたデータは削除されません。

【Work Profile 削除指示】

・緊急時ポリシー＞「個人領域も合わせてハードリセット(ワイプ)する」にチェックがない場合

従来のハードリセット機能とは異なり、端末の初期化ではなく作成されたWork Profileが削除されます。

① 緊急指示画面で「Work Profile 削除指示」ボタンを押下

②確認画面で「はい」を押下

・緊急時ポリシー＞「個人領域も合わせてハードリセット(ワイプ)する」にチェックがある場合
従来のハードリセット機能と同様に、端末の初期化が実行されます。

② 緊急指示画面で「Work Profile 削除指示」ボタンを押下　　②確認画面で「はい」を押下

■パスワード管理ポリシー

端末本体(個人領域)と仕事領域のパスワード制御を個別に行うことができます。

■デバイス制御ポリシー

Android Enterprise専用の各制御項目を設定できます。詳細はこちら。

※通常の[Android]デバイス制御項目との併用は非対応です。

■アプリー覧ポリシー

仕事用アプリー覧を取得できます。

※個人領域のアプリ情報は取得できません。

■アプリアンインストール制限ポリシー

パッケージ名を指定した仕事用アプリのアンインストールを禁止します。

2. パスワード管理ポリシー

パスワード管理ポリシーでは従来の制御に加え、管理モードによって端末本体（個人領域）と仕事領域のパスワード制御を個別に行うことができます。
また、Android Enterprise 専用の制限項目として、パスワード更新催促画面が閉じられてから端末ロックが実施されるまでの時間を設定できます。（パスワード更新タイムアウトのロック）

管理モード別　パスワード制御対象

■パスワード管理画面

パスワード管理ポリシーにおいて下記の 2 項目がパスワード管理項目となります。
管理モードにより対応しているパスワード管理項目が異なります。
・Android / Android Enterprise(Work Managed Device)
・Android Enterprise(Work Profile)

管理モード	対応パスワード管理項目	端末動作
Work Managed Device	Android / Android Enterprise(WorkManagedDevice)	端末本体（個人領域）のパスワード制御を行えます。
Work Profile	Android / Android Enterprise(WorkManagedDevice)	端末本体（個人領域）のパスワード制御を行えます。
	Android Enterprise(WorkProfile)	仕事領域のパスワード制御を行えます。
Comp	Android / Android Enterprise(WorkManagedDevice)	端末本体（個人領域）のパスワード制御を行えます。 ※仕事領域のパスワード制御は対応していません。
Work Profile [企業所有]	Android / Android Enterprise(WorkManagedDevice)	端末本体（個人領域）のパスワード制御を行えます。
	Android Enterprise(WorkProfile)	仕事領域のパスワード制御を行えます。

Work Profileパスワード制御

【概要】

Work Profile を作成すると、端末内に「仕事用プロファイルのセキュリティ」が表示されます。

端末のセキュリティ　　：　従来通り端末自体（個人領域）のパスワードを設定します。

仕事用プロファイルのセキュリティ　：　仕事用アプリを利用する際に求められるパスワードを設定します。

端末設定画面

仕事用パスワード認証画面

※仕事用アプリは、一度仕事用パスワード認証すると、次に端末自体が画面ロックされるまで
　再度パスワード認証を求められることはありません。

※仕事用パスワード認証画面は、WorkProfile の SPPM Agent によるダイアログに対しても表示されます。

Android12 以降は、個人領域に対してパスワードを設定することができません。

【統一ロックについて】

≪概要≫

仕事領域のパスワードは仕事用プロファイルのセキュリティの「統一ロックを使用」をオンにすることで、
「端末のロック＝仕事用プロファイルのロック」という扱いになります。
端末自体のパスワード認証を行うと、仕事領域のパスワードも認証されたと判断され、
仕事用パスワード認証画面は表示されません。

≪パスワード管理ポリシーとの併用≫

「統一ロックを使用」をオンの状態ではパスワード管理ポリシーの「Android / Android Enterprise(Work Managed Device)」と「Android Enterprise(Work Profile)」の要求強度が高い設定が、端末のパスワード制限として適用されます。そのため、端末のパスワード設定が、どちらか一方の要求強度に満たない場合は、パスワードの変更が要求されます。

このとき「統一ロックのパスワード」としてではなく「端末パスワード」「仕事領域パスワード」別々に変更がダイアログで要求されるため、「統一ロックを使用」がオフになります。

Android12 以降の場合は、「Android / Android Enterprise(Work Managed Device)」の要求強度が高い場合でも、Android Enterprise(Work Profile)の設定が優先されます。

Android Enterprise端末向け設定

【パスワード更新タイムアウトのロック】

下記のポップアップを閉じてから指定の時間が過ぎると端末にロックがかかります。

・端末に設定されているパスワードより厳しいパスワードを要求するポリシーを適用した際に端末上に
　表示されるパスワード設定を要求するポップアップ
・パスワード更新義務化によるパスワード期限のポップアップ

本設定により端末ロックが実施されると「パスワード更新タイムアウトによる端末ロックを実施しました。」と
ログ管理画面に表示されます。

【強力な認証の要求】

非強力な認証を利用している場合に、強力な認証（パターン/PIN/パスワード）を指定時間ごとに要求します。
一度、強力な認証による解除を実施することで、非強力な認証による解除が再度利用可能になります。
※本機能は、OS8以降で利用可能です。
※指定時間のカウントは、強力な認証を最後に利用したタイミングから実施されます。
※本機能の利用が無い端末でも、OS 仕様により強力な認証が求められる場合があります。（再起動後など）

強力な認証が必要な場合のアイコン
（南京錠が閉まっている）

仕事領域アプリをタップした場合の画面表示
（WorkProfile 端末専用の動作）

3. デバイス制御ポリシー

Android Enterprise 専用のデバイス制御ポリシー設定を利用できます。

※ [Android]の設定項目はご利用いただけません。

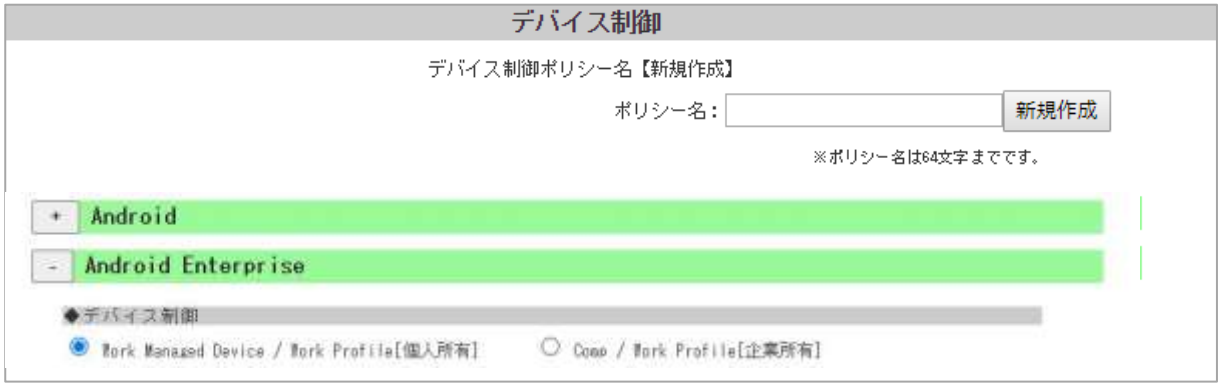
設定方法について

【ポリシー作成画面】

デバイス制御ポリシー内の「Work Managed Device / Work Profile[個人所有]」と「Comp / Work Profile[企業所有」のラジオボタンで、それぞれの設定画面を切り替えることが可能です。

使用する管理モードに適した項目を選択し、ポリシーを作成してください。

※同一のポリシーで両方の設定項目は保持できないため、「Work Managed Device / Work Profile[個人所有]」と「Comp / Work Profile[企業所有]」で、それぞれポリシーを作成してください。



一度ポリシーを作成すると後から切り替えは行えません。
新しくポリシーを作成し直す必要があります。

【端末情報編集画面（ポリシー適用操作画面）】

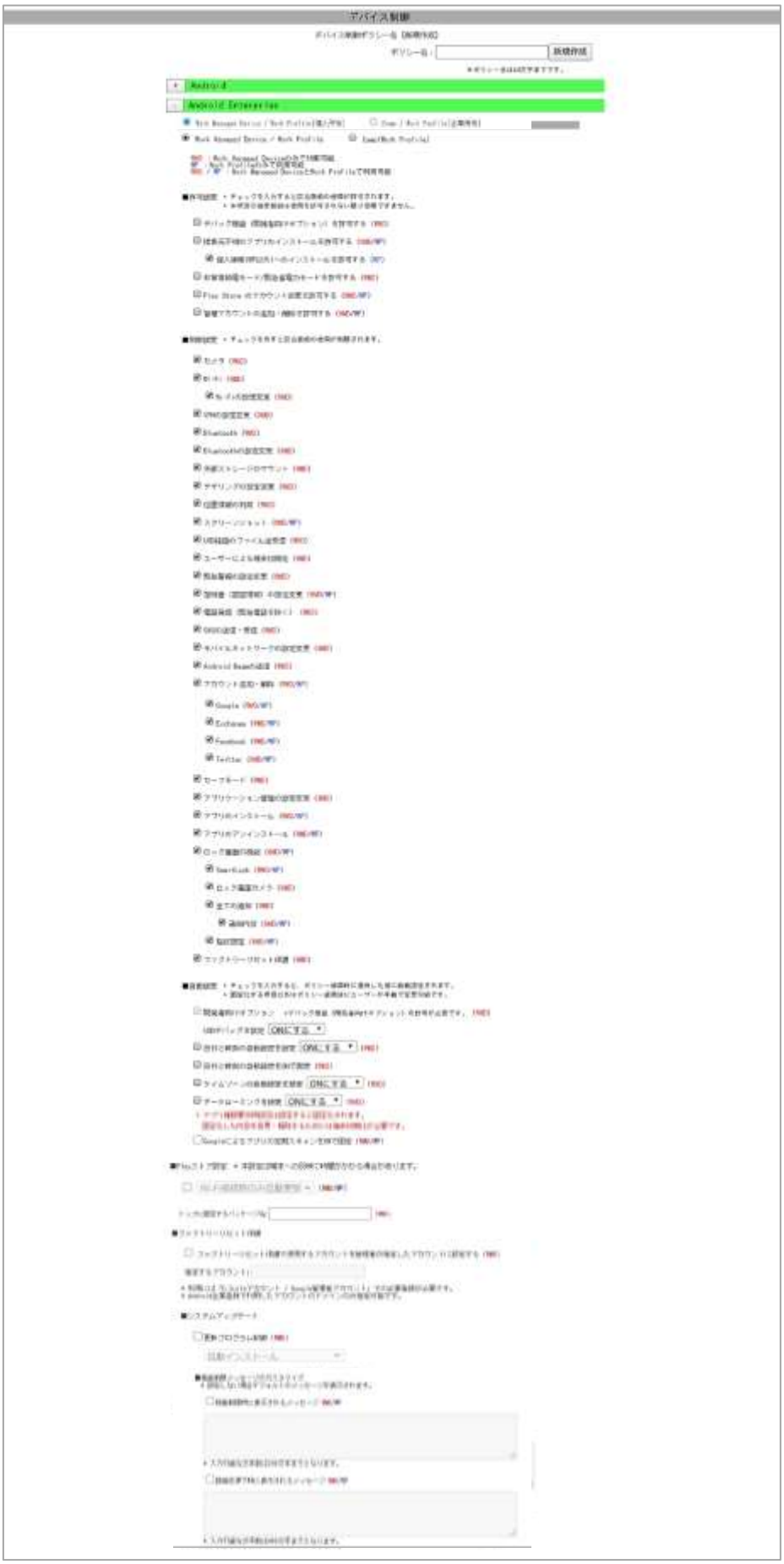
Comp 端末では個人領域と仕事領域で別々のポリシーを適用できますが、デバイス制御ポリシーのプルダウンにはその領域が制御対象のポリシーのみ表示されます。

【ポリシー情報】＞デバイス制御
「Work Managed Device / Work Profile」で作成されたデバイス制御ポリシーのみ選択できます。

【ポリシー情報(Comp_WorkProfile)】＞デバイス制御
「Comp(Work Profile)」で作成されたデバイス制御ポリシーのみ選択できます。

Work Managed Device/Work Profile[個人所有]

Work Managed Device のデバイス制御ポリシー設定を利用できます。



デバイス制御ポリシー項目一覧

▼対応機能種別▼

WMD　：Work Managed Device のみで利用可能

WP　：Work Profile[個人所有]のみで利用可能

WMD / WP　：Work Managed Device と Work Profile[個人所有]で利用可能

■許可設定

項目名	機能概要	種別
デバッグ機能（開発者向けオプション）を許可する	開発者向けオプションの利用を許可します。	WMD
提供元不明のアプリのインストールを許可する	提供元不明のアプリのインストールを許可します。	WMD/WP
個人領域（WP以外）へのインストールを許可する	個人領域への提供元不明アプリのインストールを許可します。	WP
非常用節電モード/緊急省電力モードを許可する	非常用節電モード/緊急省電力モードを許可します。	WMD
Play Store のアカウント変更を許可する	Play Store のアカウント変更を許可します。	WMD/WP
管理アカウントの追加・削除を許可する	管理アカウントの追加・削除を許可します。	WMD/WP

■機能制御

カメラ	カメラの利用を制限します。	WMD/WP
Wi-Fi	Wi-Fiの利用を制限します。	WMD
Wi-Fiの設定変更	Wi-Fiの設定変更を制限します。	WMD
VPNの設定変更	VPNの設定変更を制限します。	WMD
Bluetooth	Bluetoothの利用を制限します。	WMD
Bluetoothの設定変更	Bluetoothの設定変更を制限します。	WMD
外部ストレージのマウント	外部ストレージのマウントを制限します。	WMD/WP
テザリングの設定変更	テザリングの設定変更を制限します。	WMD
位置情報の利用	位置情報の利用を制限します。	WMD
スクリーンショット	スクリーンショットの利用を制限します。	WMD/WP
USB経由のファイル送受信	PCとのUSB経由のファイル送受信を制限します。	WMD
ユーザーによる端末初期化	端末設定からの端末初期化を制限します。	WMD
緊急警報の設定変更	緊急警報の設定変更を制限します。	WMD
証明書（認証情報）の設定変更	証明書（認証情報）の設定変更を制限します。	WMD/WP
電話発信（緊急電話を除く）	緊急通報を除く電話発信を制限します。	WMD
SMSの送信・受信	SMSの送信・受信を制限します。	WMD
モバイルネットワークの設定変更	モバイルネットワークの設定変更を制限します。	WMD
Android Beamの送信	Android Beamの送信を制限します。	WMD
アカウント追加・削除	アカウントの追加と削除を制限します。	WMD
Google,Exchange,Facebook,Twitter	各アカウント毎の追加と削除の制限を設定します。	WMD/WP
セーフモード	セーフモードの利用を制限します。	WMD

アプリケーション管理の設定変更	アプリケーション管理の設定変更を制限します。	WMD
アプリのインストール	アプリのインストールが制限されます。	WMD/WP
アプリのアンインストール	アプリのアンインストールが制限されます。	WMD/WP
ロック画面の機能	ロック画面関連の制限項目を全て制限します。	WMD/WP
SmartLock	SmartLockの利用を制限します。	WMD/WP
ロック画面カメラ	ロック画面のカメラの利用を制限します。	WMD
全ての通知	ロック画面に表示される全ての通知を制限します。	WMD
通知内容	ロック画面に表示される通知の内容を制限します。	WMD
指紋認証	指紋認証の利用を制限します。	WMD
ファクトリーリセット保護	ファクトリーリセット保護を制限します。	WMD

■自動設定

開発者向けオプション USBデバッグを設定	開発者向けオプションの項目の設定を適用します。	WMD
日付と時刻の自動設定を設定	日付と時刻の自動設定の設定を適用します。	WMD
日付と時刻の自動設定をONで固定	日付と時刻の自動設定をONで固定します。	WMD
タイムゾーンの自動設定を設定	タイムゾーンの自動設定の設定を適用します。	WMD
データローミングを設定	データローミングの設定を適用します。	WMD
アプリ権限要求時設定	アプリから使用権限が要求される際に自動で設定されます。	WMD/WP
GoogleによるアプリのスキャンをONで固定	アプリの定期スキャンをONで固定します。	WMD/WP

■Playストア設定

Playストアの自動更新制御	自動更新の実行タイミングの操作を行います。	WMD/WP

■シングルアプリモード

トップに固定するパッケージ名	指定したアプリを端末最前面に固定します。	WMD

■ファクトリーリセット保護

ファクトリーリセット保護で使用するアカウントを管理者が指定したアカウントに設定する	アプリの定期スキャンを ON で固定します。	WMD

■システムアップデート

更新プログラム制御	システムアップデートの実行タイミングの操作を行います。	WMD
30 日間インストールをブロック	システムアップデートのインストールをブロック	WMD

■機能制限メッセージのカスタマイズ

機能制限時に表示されるメッセージ	機能制限時に表示されるメッセージを作成します	WMD/WP
詳細を押下時に表示されるメッセージ	アプリ管理画面に表示されるメッセージを作成します	WMD/WP

■許可設定

Android Enterpriseによりデフォルトで禁止されている機能を許可します。

※チェックを入力すると該当機能の使用が許可されます。

※本項目の端末機能は使用を許可されない限り使用できません。

【デバッグ機能（開発者向けオプション）を許可する（WMD）】

表示場所　>>>　「端末設定」→(「端末情報」ビルド番号連打)→「開発者向けオプション」

「デバッグ機能(開発者向けオプション)」機能の利用許可を設定することができます。

チェックを付けると、「デバッグ機能（開発者向けオプション）」が利用可能になります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【提供元不明のアプリのインストールを許可する（WMD/WP）】

表示方法 >>> 「端末設定」→「ロック画面とセキュリティ(セキュリティ)」→「提供元不明のアプリ」

「提供元不明のアプリのインストールを許可する」ことができます。

チェックをつけると、デフォルトで禁止されていた提供元不明のアプリのインストールを許可できます。

※当項目を許可すると、個人領域へのインストールも併せて許可されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【個人領域（WP 以外）へのインストールを許可する】

チェックをつけると、個人領域への提供元不明アプリのインストールを許可することができます。

※当機能は、「提供元不明のアプリのインストールを許可する」項目を許可した場合、
　併せて許可状態になります。

≪非許可時の端末側の制限について≫

当機能を禁止したポリシーを適用した場合、端末のOSバージョンにより制限方式が異なります。

・OS10未満

・端末設定内の「提供元不明アプリのインストール」の項目は、
　ユーザによる ON/OFF の操作が可能です。

・端末設定にて該当項目を ON（許可）に変更しても、
　インストール操作時に制限画面が表示され、インストールは実施されません。

・アプリ毎に個別で「提供元不明アプリのインストール」を許可に変更しても、
　インストール操作時に制限画面が表示され、インストールは実施されません。

・OS10以降

・個人領域および仕事領域の全てのアプリの「不明なアプリのインストール」が「無効」で固定されます。

項目一覧へ戻る

【非常用節電モード/緊急省電力モードを許可する(WMD)】

■非常用節電モード

表示方法 >>> 「電源ボタン長押し」→「電源メニュー」→「非常用節電モード/緊急省電力モード」
または「端末設定」→「バッテリー」→「非常用節電モード/緊急省電力モード」

「非常用節電モード/緊急省電力モードを許可する」ことができます。

チェックをつけると、デフォルトで禁止されていた非常用節電モード/緊急省電力モードを許可できます。

※機種やAndroid OSバージョンによって起動方法が異なります。

項目一覧へ戻る

【Play Store のアカウント変更を許可する（WMD/WP）】

表示場所　>>>　「Playストア」→左上の「≡」→アカウント切り替えのプルダウン

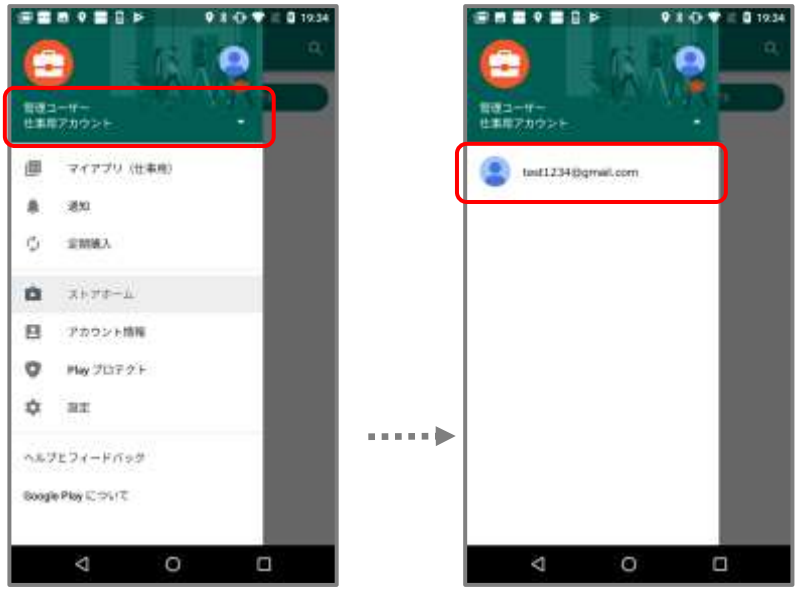
「Play Store のアカウント変更を許可する」ことができます。

チェックをつけると、デフォルトで禁止されていたPlay Storeのアカウント切り替えを許可できます。

デフォルト状態（制限状態）

プルダウンが非表示になり、アカウントの切り替えができません。

許可状態



プルダウンが表示され、アカウントの切り替えが可能です。

項目一覧へ戻る

【管理アカウントの追加・削除を許可する（WMD/WP)】

表示場所　>>>　「端末設定」→「アカウント(アカウントと同期)」

「管理アカウントの追加・削除を許可する」ことができます。

チェックをつけると、管理アカウントの追加・削除を許可できます。

※「管理アカウント」は Managed Google Playアカウントで企業登録している場合に、
　端末に追加されるアカウントです。

※この設定は Managed Google Playアカウントで企業登録している場合のみ有効です。
　Gsuiteで企業登録されている場合は、Googleアカウントの追加・削除制御にて同様の制限が可能です。

「管理アカウント」を削除すると、Android Enterprise のサイレントインストール/アンインストール、アプリ設定、PlayStore レイアウト設定機能が利用できなくなります。
また、一度「管理アカウント」を削除すると、端末を初期化した上での再キッティングが必要となるため、
「管理アカウントの追加・削除を許可する」の設定は無効に設定することを推奨します。

◆アカウント追加

デフォルト状態（制限状態）

許可状態

◆アカウント削除

デフォルト状態（制限状態）

許可状態

項目一覧へ戻る

■制限設定

端末の機能をAndroid Enterpriseにより制御します。

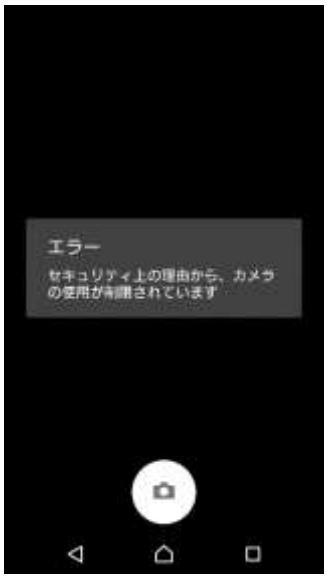
※チェックを外すと該当機能の使用が制限されます。

【カメラ（WMD/WP）】

「カメラ」機能の利用禁止を設定することができます。

チェックを外すとカメラ起動時にカメラの使用ができない旨のメッセージが表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。



【個人領域でのカメラ使用を許可する】

チェックをつけると、個人領域でのカメラ使用を許可することができます。

※当機能は、「カメラ」項目を許可した場合、併せて許可状態になります。

項目一覧へ戻る

【Wi-Fi（WMD）】

「Wi-Fi」の利用禁止を設定することができます。

チェックを外すとWiFiをONにしていた場合は自動でOFFになり、その後手動でONにできなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【Wi-Fiの設定変更（WMD）】

ユーザーによる「WiFiの設定変更」を禁止することができます。

チェックを外すと、WiFiの接続先変更やその他の設定変更が制限されます。

※WiFiのON/OFFの切り替えは可能です。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【VPNの設定変更（WMD）】

表示方法 >>> 「端末設定」→「もっと見る(その他の設定)」→「VPN」

ユーザーによる「VPNの設定変更」を禁止することができます。

チェックを外すと端末設定内のVPNの項目がグレーアウトし、VPNの新規作成や設定変更が制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【Bluetooth（WMD）】

「Bluetooth」の利用禁止を設定することができます。

チェックを外すとBluetoothをONにしていた場合は自動でOFFになり、その後手動でONにできなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【Bluetooth の設定変更（WMD）】

ユーザーによる「Bluetoothの設定変更」を禁止することができます。

チェックを外すと、Bluetoothの接続先変更やその他の設定変更が制限されます。

※BuluetoohのON/OFFの切り替えは可能です。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります

項目一覧へ戻る

【外部ストレージのマウント（WMD/WP）】

表示場所　>>>　「端末設定」→「ストレージ」→「SDカード」

「外部ストレージのマウント」を禁止することができます。

チェックを外すと、外部ストレージをマウントしようとした際に許可されていない旨のメッセージが表示されます。

※ポリシー適用時にマウント状態であった場合、マウントは自動で解除されません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【テザリングの設定変更（WMD）】

表示場所　>>>　「端末設定」→「もっと見る(その他の設定)」→「テザリング」

ユーザーによる「テザリングの設定変更」を禁止することができます。

チェックを外すと端末設定内のテザリングの項目がグレーアウトし、設定内容の変更が制限されます。

※本機能はテザリングの利用制限を直接行う機能ではございません。テザリングがONの状態の端末に
　本設定を適用した場合は、テザリングが利用可能な場合がございます。

※OS9の端末に本制限を適用した場合、端末側のWiFiの項目も併せて制限される場合があります。

※再起動時に通知メニューのテザリングアイコンが非表示になります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【位置情報の利用（WMD）】

「位置情報の利用」を禁止することができます。

チェックを外すと位置情報をONにしていた場合は自動でOFFになり、その後手動でONにできなくなります。

※位置情報取得ポリシーをご利用する場合は制限しないでください。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【スクリーンショット（WMD/WP）】

「スクリーンショット」機能の利用禁止を設定することができます。

チェックを外すと、撮影時にスクリーンショットを撮影/保存できない旨のメッセージが表示されます。

※撮影方法は機種によって異なります。

※WorkProfileでは仕事用アプリのスクリーンショットのみ制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

Android 12以降の場合、チェックを外すと撮影時に黒い画面が撮影/保存されます。

◆Xperia 機種の場合

通知領域にメッセージが表示されます。

◆Galaxy 機種の場合

画面下部にメッセージが表示されます。

項目一覧へ戻る

【USB経由のファイル送受信（WMD）】

「USB経由のファイル送受信」を禁止することができます。

チェックを外すと、USB接続によるPCとのファイル送受信ができなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【ユーザーによる端末初期化（WMD）】

表示場所　>>>　「端末設定」→「バックアップとリセット」→「データの初期化」

「ユーザーによる端末初期化」を禁止することができます。

チェックを外すと、端末初期化を行おうとした際に許可されていない旨のメッセージが表示されます。

※緊急指示の「ハードリセット」指示による初期化は可能です。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【緊急警報の設定変更（WMD）】

表示場所　>>>　「端末設定」→「もっと見る(その他の設定)」または「音」→「緊急警報」

ユーザーによる「緊急警報の設定変更」を禁止することができます。

チェックを外すと、端末設定内の緊急警報の項目がグレーアウトし設定変更ができません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【証明書（認証情報）の設定変更（WMD/WP）】

表示場所　>>>　「端末設定」→「ロックとセキュリティ（セキュリティ）」→「認証ストレージ」

ユーザーによる「証明書（認証情報）の設定変更」を禁止することができます。

チェックを外すと、端末設定内の認証情報ストレージの項目がグレーアウトし設定変更ができません。

※「信頼できる認証情報」はひとつ進んだページで操作ボタンがグレーアウトしています。

※WorkProfileでは仕事領域の設定変更のみ制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【電話発信（緊急電話を除く）（WMD）】

「電話発信(緊急電話を除く)」の利用禁止を設定することができます。

チェックを外すと、電話発信を行おうとした際に許可されていない旨のメッセージが表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【SMSの送信・受信（WMD）】

「SMSの送信・受信」機能の利用禁止を設定することができます。

チェックを外すと、「メッセージ」アプリを起動した際に許可されていない旨のメッセージが表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【モバイルネットワークの設定変更（WMD）】

表示場所　>>>　「端末設定」→「もっと見る(その他の設定)」→「モバイルネットワーク」

ユーザーによる「モバイルネットワークの設定変更」を禁止することができます。

チェックを外すと、端末設定内のモバイルネットワークの項目がグレーアウトし設定変更ができません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【Android Beam の送信（WMD）】

表示場所　>>>　「端末設定」→「もっと見る(その他の設定)」→「NFC/おｻｲﾌｹｰﾀｲ設定」→「Androidビーム」

「Android Beamの送信」の利用禁止を設定することができます。

チェックを外すと、端末設定内のAndroidビームの項目がグレーアウトし利用できません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【アカウント追加・削除（WMD）】

表示場所　>>>　「端末設定」→「アカウント(アカウントと同期)」

ユーザーによる「アカウント追加・削除」を禁止することができます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

※WorkProfileでは仕事領域のアカウントのみ制限されます。

※Galaxy端末でアカウントの追加・削除を制限すると、「指紋認証」が設定できなくなる場合があります。

≪全体のアカウント追加・削除を禁止する≫

「アカウント追加・削除」のチェックを外すと、全般のアカウント追加・削除の項目がグレーアウトします。

◆アカウント追加

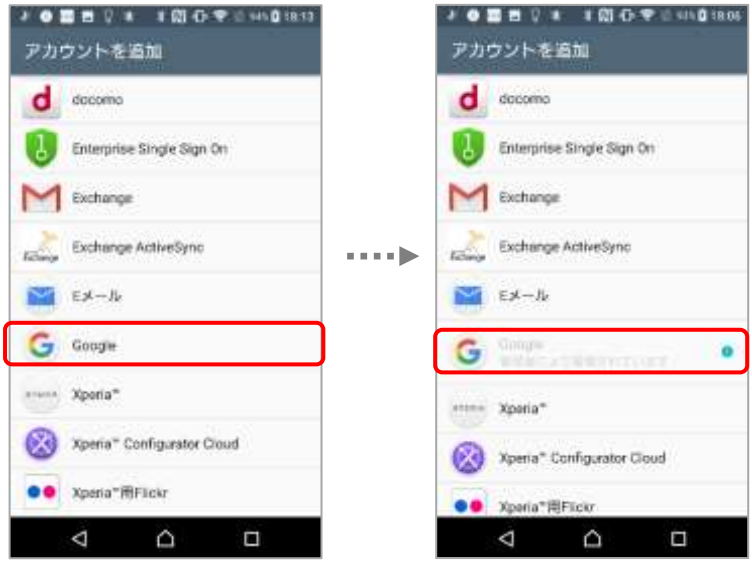
◆アカウント削除

≪アプリ毎のアカウント追加・削除を禁止する≫

「アカウント追加・削除」の項目傘下のアプリ毎のチェックを外すと、該当のアプリのアカウント追加・削除を禁止できます。

※Googleを除き、アプリ内からのアカウント追加は制限状態でも可能です。

◆アカウント追加



◆アカウント削除

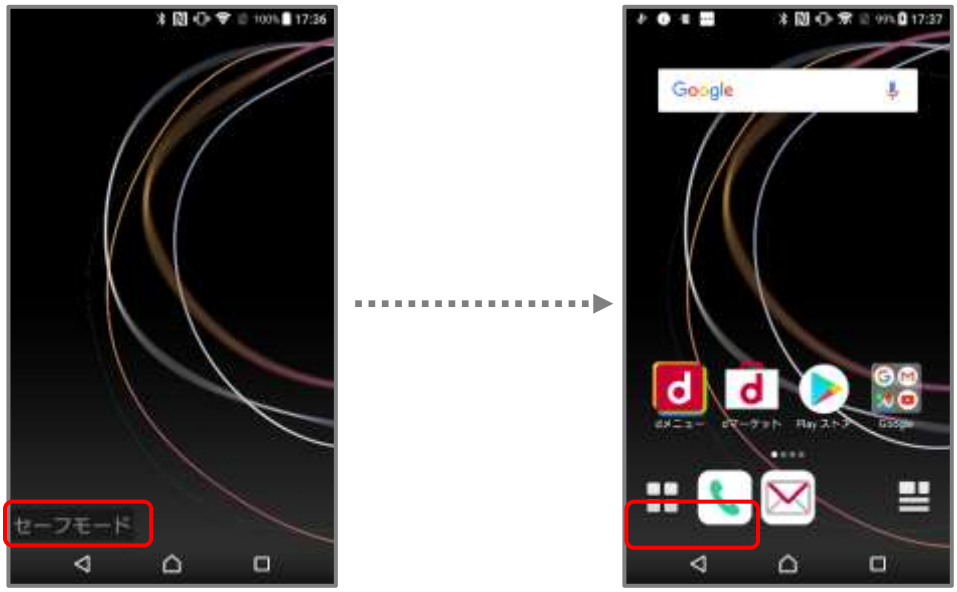
【セーフモード（WMD）】

端末を「セーフモード」で起動することを禁止できます。チェックを外すとセーフモードで起動できなくなります。

※セーフモードの起動手順は端末ごとに異なります。

※セーフモード起動状態ではSTAR-MDMは起動しませんが、デバイス制御ポリシーによる制限は有効のままです。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。



項目一覧へ戻る

【アプリケーション管理の設定変更（WMD）】

表示場所　>>>　「端末設定」→「アプリ」→任意のアプリタップ→「アプリ情報画面」

ユーザーによる「アプリケーション管理の設定変更」を禁止することができます。

チェックを外すと、アプリ情報の「無効にする」「強制終了（強制停止）」「データを削除」「キャッシュを削除」を行おうとした際に許可されていない旨のメッセージが表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「無効にする」/「強制終了（強制停止）」

◆「データを削除」/「キャッシュを削除」

項目一覧へ戻る

【アプリのインストール（WMD/WP）】

ユーザーによる「アプリのインストール」を禁止することができます。

チェックを外すと、全てのアプリがインストールできなくなります。

※PlayStoreからのインストール、管理画面からのアプリ配信/サイレントインストールが制限されます。

※提供元不明のアプリのインストール設定が制限されます。

※WorkProfileでは仕事用アプリのインストールのみ制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【アプリのアンインストール（WMD/WP）】

ユーザーによる「アプリのアンインストール」を禁止することができます。

チェックを外すと、全てのアプリがアンインストールできなくなります。

※PlayStoreからのアンインストール、管理画面からのサイレントアンインストールも制限されます。

※WorkProfileでは仕事用アプリのアンインストールのみ制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆アプリ情報画面からのアンインストール

項目一覧へ戻る

【ロック画面の機能（WMD）】

端末認証に関連する以下の機能をすべてまとめて禁止することができます。

※チェックを外すと、ロック画面上での機能が原則全て使用できなくなります。

※各制御内容は次項をご覧ください。

・SmartLock（WMD/WP）
・ロック画面カメラ（WMD）
・全ての通知（WMD）
・通知内容(WMD / WP)

【SmartLock（WMD）】

「SmartLock」の利用を禁止することができます。チェックを外すと、「SmartLock」が無効化されます。

※「認証済みの顔」はパスワード義務化状態では本制限を適用していなくても制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【ロック画面カメラ（WMD）】

端末の認証画面から起動できる「カメラ」の利用を禁止することができます。

チェックを外すと、「カメラ」が無効化されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

※Android 14以降では、端末のロック画面から起動できるカメラは制御できません。デバイス制御ポリシーで「カメラ」を制限することで制御可能です。

項目一覧へ戻る

【全ての通知（WMD）】

端末の認証画面に表示される通知を非表示にすることができます。

※WorkProfileでは仕事用アプリの通知のみ制限されます。

※認証後の画面では通知は表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【通知内容（WMD）】

端末の認証画面に表示される通知内容を非表示にすることができます。

※一部のアプリ(システムアプリ等)では表示される場合があります。

※WorkProfileでは仕事用アプリの通知のみ制限されます。

※認証後の画面では通知内容は表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

【指紋認証（WMD）】

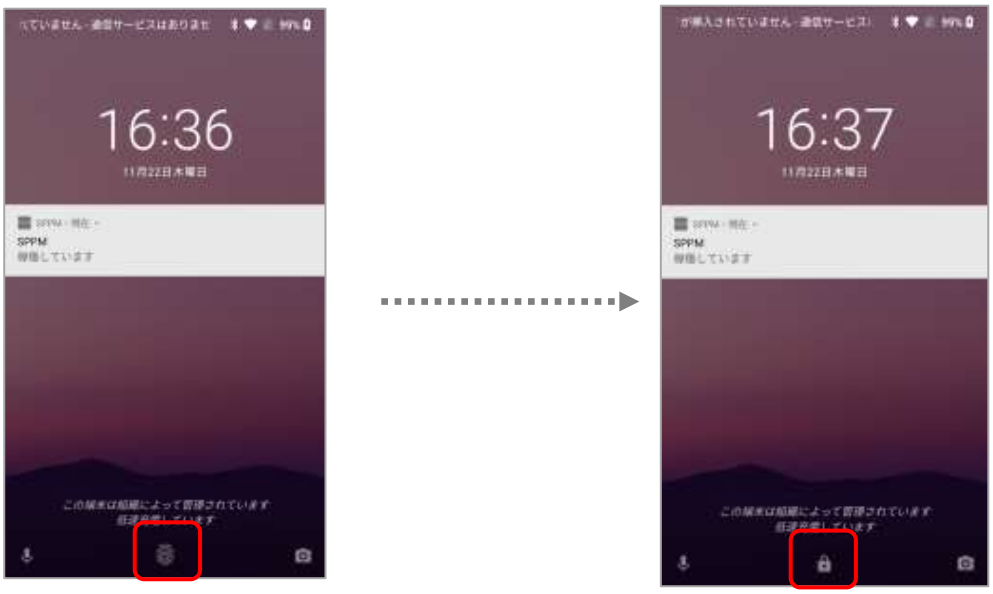
指紋認証での端末認証解除を禁止できます。

チェックを外すと指紋マークが鍵マークに変わり、指紋認証できなくなります。

※指紋認証を設定していても指紋認証による解除ができなくなります。

※WorkProfileでは仕事用プロファイルのパスワード認証画面で指紋認証が禁止されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。



項目一覧へ戻る

【ファクトリーリセット保護（WMD）】

Android EnterpriseではGoogleアカウントにログイン状態の端末にハードリセット指示を行った場合、

ファクトリーリセット保護機能により、次に端末初期設定する際に初期化前にログインしていたGoogleアカウントの入力が必要です。

チェックを外した端末にハードリセット指示を行うと「ファクトリーリセット保護」が無効になり、

端末初期設定する際に初期化前にログインしていたGoogleアカウントの入力が不要となります。

※開発者向けオプション＞OEMロック解除がON（ロック解除状態）の場合、ファクトリーリセット保護は有効になりません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

■自動設定

端末の機能のON/OFFの切り替え、および固定化ができます。

※チェックを入力すると、ポリシー適用時に選択した値に自動設定されます。

※固定化する項目以外はポリシー適用時にユーザーが手動で変更可能です。

【開発者向けオプション（WMD）】

表示場所　>>>　「端末設定」→「開発者向けオプション」

「開発者向けオプション」内の項目を自動で設定します。

「USBデバッグを設定」を「ONする」設定にしていた場合は開発者向けオプションも自動でONとなります。

※予め設定内で開発者向けオプションが表示された状態になっている必要があります。

≪USBデバッグを設定≫

「USBデバッグ」のON/OFFの切り替えが管理画面側からできます。

※デバッグ機能(開発者向けオプション)を許可にしている場合のみ使用可能な機能です。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「OFF にする」にした場合

◆ 「ON にする」 にした場合

項目一覧へ戻る

【日付と時刻の自動設定を設定（WMD）】

表示場所　>>>　「端末設定」→「日付と時刻」

「日付と時刻の自動設定」のON/OFFの切り替えが管理画面側からできます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「OFF にする」にした場合

◆ 「ON にする」 にした場合

項目一覧へ戻る

【日付と時刻の自動設定をONで固定（WMD）】

表示場所　>>>　「端末設定」→「日付と時刻」

「日付と時刻の自動設定をONで固定」することができます。

チェックを付けると、端末設定内の日付と時刻の自動設定の項目がONで固定され、OFFにできなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

・Android 11　以降

「日付と時刻の自動設定をONで固定」を有効にすると、 ポリシー反映時点の「タイムゾーン」設定で固定化されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「タイムゾーン」を OFF で適用した場合

無効で固定化されます。

◆「タイムゾーン」を ON で適用した場合

有効で固定化されます。

項目一覧へ戻る

【タイムゾーンの自動設定を設定（WMD）】

表示場所　>>>　「端末設定」→「日付と時刻」

「タイムゾーンの自動設定を設定」のON/OFFの切り替えが管理画面側からできます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「OFF にする」にした場合

◆ 「ON にする」 にした場合

項目一覧へ戻る

【データローミングを設定（WMD）】

表示場所　>>>　「端末設定」→「もっと見る(その他の設定)」→「モバイルネットワーク」→「データローミング」

「データローミングを設定」のON/OFFの切り替えが管理画面側からできます。

≪注意≫

・「データローミングを設定」をONまたはOFFにするポリシーを適用しても自動でONまたはOFFにならない場合があります。

・「データローミングを設定」をOFFにするポリシーを適用すると、設定がOFFに固定され端末操作では変更できなくなる場合がありますが、「データローミングを設定」をONにするポリシーを適用することで固定が解除されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

◆「OFF にする」にした場合

◆ 「ON にする」 にした場合

項目一覧へ戻る

【アプリ権限要求時設定（WMD/WP）】

表示場所　>>>　「端末設定」→「アプリ」→任意のアプリをタップ→「権限(許可)」

「アプリ権限要求時設定」を行うことができます。

※「管理画面＞その他＞アプリ設定」のアプリ毎の権限設定が優先されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

≪注意≫

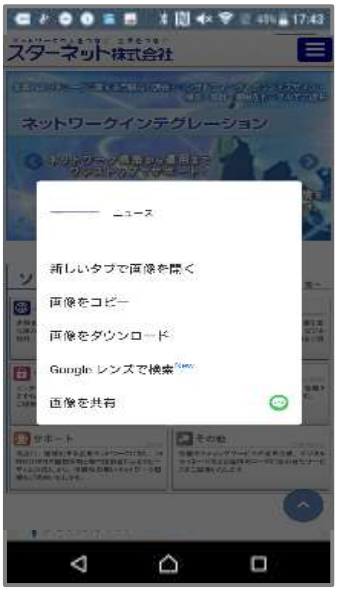
・設定値が反映されるのは権限が要求されたタイミングです。

・一度固定化されるとデバイス制御ポリシーの項目のチェックを外したり、未設定にしても解除されません。

・すでに権限が許可された状態では、権限の要求が発生しないため固定化できません。

例）Chromeのストレージ権限が要求されるタイミング

①ブラウザの画像を長押しする



②「画像をダウンロード」をタップする

③権限が求められる

◆「アプリ権限要求時設定」のチェックを外している場合

権限は固定されず、ON/OFFの切り替えが可能です。

◆「アプリ権限要求時設定」を「全て許可」に設定している場合
権限要求のタイミングで権限は求められず、自動で権限が許可固定されます。

例)ストレージの権限が要求された場合

Android12以降のWork Profileの場合、要求された権限が固定されません。

◆「アプリ権限要求時設定」を「全て禁止」に設定している場合
権限要求のタイミングで権限は求められず、自動で権限が禁止固定されます。

例)ストレージの権限が要求された場合

項目一覧へ戻る

【Google によるアプリの定期スキャンを ON で固定（WMD/WP）】

表示場所　>>>　「端末設定」→「Google」→「セキュリティ 」→「アプリの確認」

「Googleによるアプリの定期スキャンをONで固定」することができます。

チェックをつけると、端末設定内の「スキャンしてセキュリティ上～」の項目がONで固定されます。

※WorkProfile で制限した場合でもOS仕様により個人領域の項目が制限されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

項目一覧へ戻る

■Play ストア設定（WMD）

Play ストアのアプリの自動更新設定を制御することができます。

※本設定は、端末への反映に時間がかかる場合があります。

※本設定を行うと、項目がグレーアウト（固定）され操作不可になります。

◆Wi-Fi 接続時のみ自動更新

Wi-Fi に接続している場合のみ、自動で更新を行います。

◆常に自動更新

ネットワークの状況に関わらず、常に自動更新を行います。

◆自動更新しない

自動での更新を制御し、ユーザーのタイミングで自動更新を行います。

■シングルアプリモード(WMD)

アプリのパッケージ名を入力することで、そのアプリが端末最前面に固定されます。

※固定するアプリがシングルアプリモードに対応されている必要があります。

≪シングルアプリモード対応アプリに必要な開発≫

前提条件

1　当該アプリのパッケージが Android Enterprise (Work Managed Device) で動作すること。

2　MDM のように特別な管理権限を有しないアプリ単体で動作させること。

ドキュメントでは手動での固定化の次にプログラム的に画面の固定化に対応するための記載があります。

https://developer.android.com/about/versions/android-5.0.html?hl=ja　⇒「画面固定」の項目

固定化対象アプリケーションについて、以下の対応が必要です。

1　アプリケーション

1.1　Activityを継承した起動時のアクティビティを定義

1.2　onResumeメソッドで以下を行う。

1.2.1　Android 6.0以上が対象でアクティビティマネージャのgetLockTaskModeState()の値がActivityManager.LOCK_TASK_MODE_NONE以外の場合、startLockTask()を実行する。

1.3　onCreateメソッドで以下を行う。**(注意:意図的に停止させないアプリでは不要)**

1.3.1　ボタンなどをクリックされた際に以下を行う

stopLockTask()を実行する。

2　マニフェストファイル(AndroidManifest.xml)への記載

※lockTaskMode を定義する。(if_whitelistedを指定するとパッケージに許可が与えられていれば自動的にロックタスクモードで起動する)

```
<activity>
                android:name=".policy.locktask.パッケージ名"
                android:launchMode="singleInstance"
```

```
            android:lockTaskMode="if_whitelisted"
            android:enabled="false">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.HOME"/>
            <category android:name="android.intent.category.DEFAULT"/>
        </intent-filter>
</activity>
```

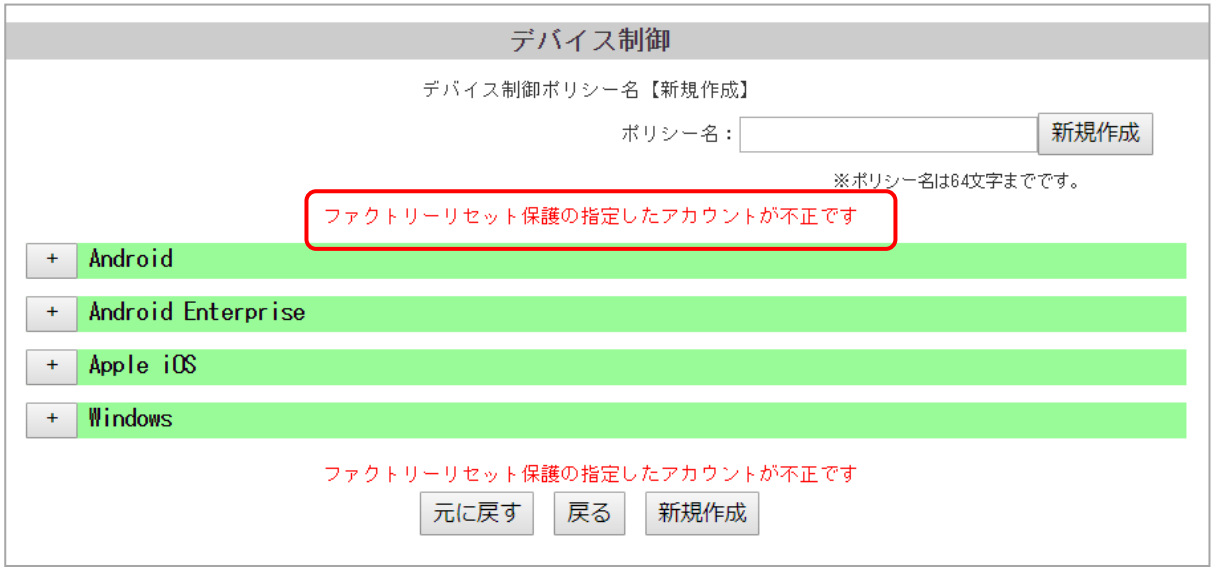
■ファクトリーリセット保護(WMD)

ファクトリーリセット保護で使用するアカウントを管理者が指定したアカウントに設定するを入力することが可能です。

※利用には「G Suiteアカウント / Google管理者アカウント」での企業登録が必要です。

※Android企業登録で利用したアカウントのドメインのみ指定可能です。

※G-Suite環境でのみ対応しているため、Managed Google Playアカウントで企業登録された管理画面では
ポリシー作成時に以下のようなエラーが表示され、ポリシー作成ができません。



■システムアップデート

システムアップデートの実行タイミングの設定を行います。

【更新プログラム制御(WMD)】

◆「自動インストール」

システムアップデートが利用可能になり次第、すぐに更新プログラムを自動インストールします。

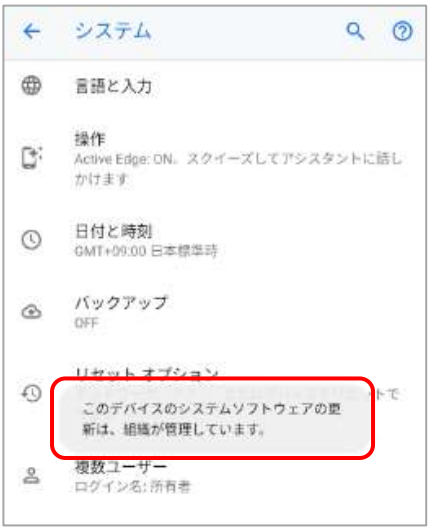
◆「30 日間インストールをブロック」

本ポリシーを適用した日から 30 日間インストールをブロックし、さらに手動によるインストールを制御します。

※30 日経過後はブロックは行われず、手動によるシステムアップデートのインストールが可能な状態になります。（端末により 30 日以上ブロックされる場合があります。）
※セキュリティパッチの更新は制御対象外です。
※アップデート内容に重大な更新を含むと Google 等が判断した場合、指定時間以外のタイミングでもシステムアップデートが実施される可能性があります。

◆「自動インストールの時刻を指定」
システムアップデートの自動インストールを行う時間帯を設定します。
※当機能の設定は 30 日間有効です。30 日経過後はブロックは行われず、手動によるシステムアップデートのインストールが可能な状態になります。
※セキュリティパッチの更新は制御対象外です。
※アップデート内容に重大な更新を含むと Google 等が判断した場合、指定時間以外のタイミングでもシステムアップデートが実施される可能性があります。

≪アップデート制御された端末動作≫
・システムアップデートの通知が非表示になります。
・端末設定内のシステムアップデート項目をタップした場合、「このデバイスのシステムソフトウェアの更新は、組織が管理しています。」というブロックが表示されます。
・端末によってブロック表示ではなく、画面の遷移が制御される場合もあります。



■機能制限メッセージのカスタマイズ

機能制限時のメッセージやデバイス管理アプリ画面に表示するメッセージを作成できます。メールアドレスや URL 等はリンクが作成されます。
※本機能は、OS 7 以上で利用可能です。

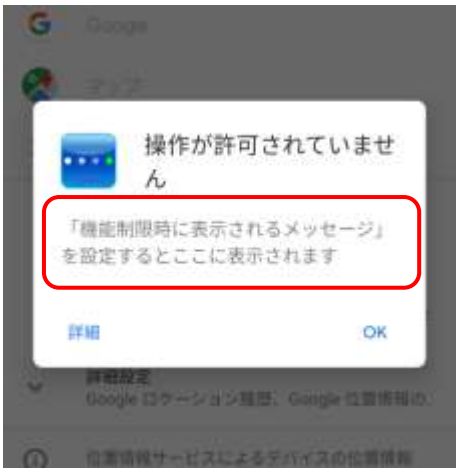
≪メッセージ表示について≫
・端末側の仕様により、設定したメッセージが表示される場合と表示されない場合があります。

設定したメッセージが表示されない場合は、デフォルトメッセージが表示されます。

・端末側の仕様により、メールアドレス/電話番号/URL のリンクが表示されない場合があります。

例：URL より前に文字がある場合 ／ URL の途中で改行している場合

【機能制限時に表示されるメッセージ（WMD/WP）】



デバイス制御ポリシー等で制限している機能を利用した場合に表示される、制限メッセージを設定します。

文字数の上限は 200 文字です。

※1 つの改行は 2 文字に計算されます。

【詳細を押下時に表示されるメッセージ（WMD/WP）】

機能制限時に表示されるメッセージ内の「詳細」を押下後、

遷移先の画面で表示されるメッセージを設定します。

※デバイス管理アプリに関する説明文の下に、メッセージが表示されます。

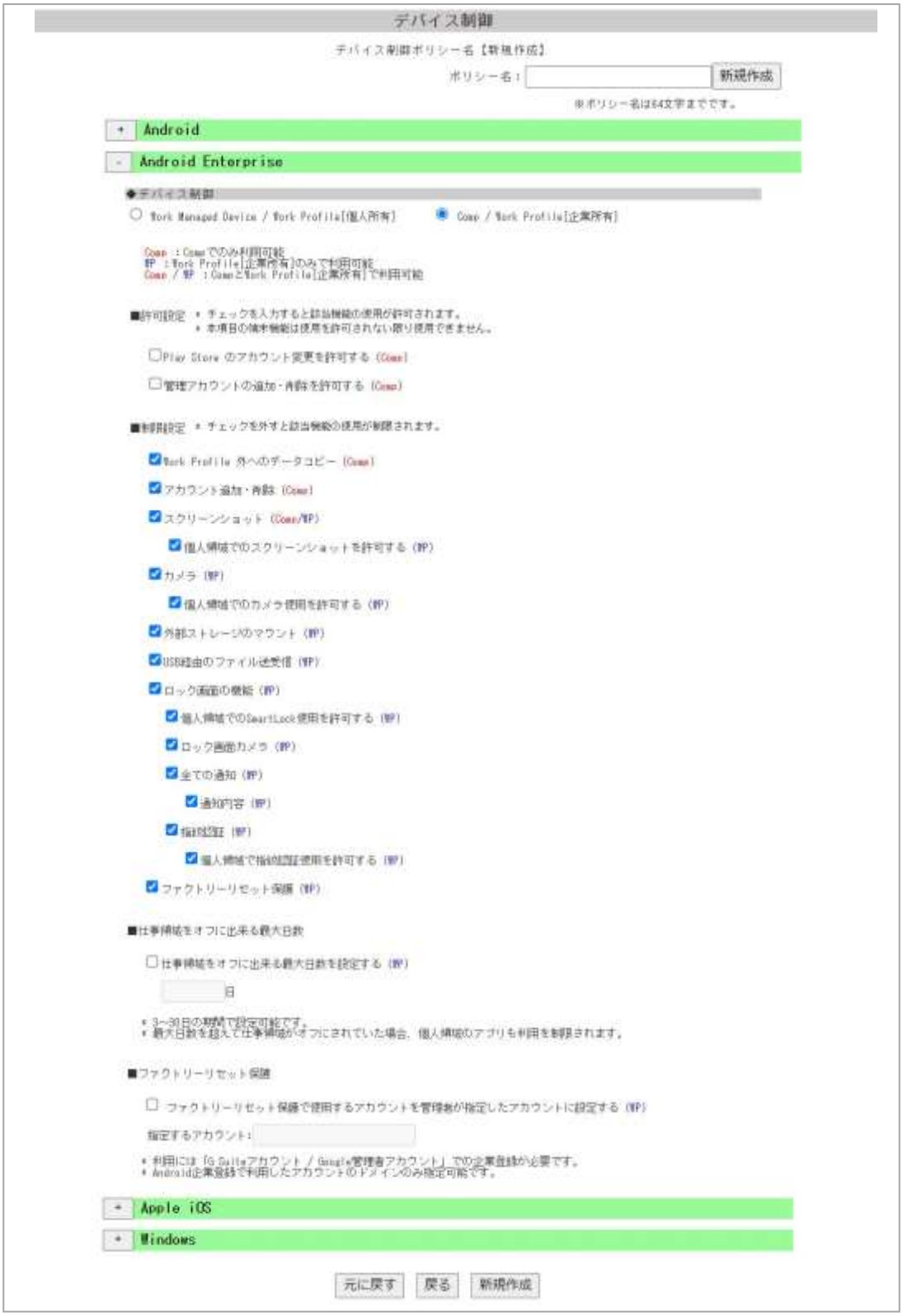
文字数の上限は 400 文字です。

※1 つの改行は 2 文字に計算されます。

項目一覧へ戻る

Comp/Work Profile[企業所有]

Comp/Work Profile[企業所有]のデバイス制御ポリシー設定を利用できます。



デバイス制御ポリシー項目一覧

▼対応機能種別▼

Comp ：Comp でのみ利用可能
WP ：Android11 以降の Work Profile[企業所有]のみで利用可能
Comp / WP ：Comp と Work Profile[企業所有]で利用可能

デバイス制御ポリシー項目一覧

■許可設定

項目名	機能概要	種別
Play Store のアカウント変更を許可する	仕事領域のPlay Store のアカウント変更を許可します。	Comp
管理アカウントの追加・削除を許可する	仕事領域の管理アカウントの追加・削除を許可します。	Comp

■制限設定

Work Profile外へのデータコピー	仕事領域のデータを仕事領域外にコピーすることを制限します。	Comp
アカウント追加・削除	仕事領域のアカウントの追加と削除を制限します。	Comp
スクリーンショット	外部ストレージのマウントを制限します。	Comp/WP
個人領域でのスクリーンショットを許可する	個人領域でのスクリーンショットを制御します。	WP
カメラ	カメラの利用を制限します。	WP
個人領域でのカメラ使用を許可する	個人領域でのカメラの利用を制限します。	WP
外部ストレージのマウント	外部ストレージのマウントを制限します。	WP
USB経由のファイル送受信	PCとのUSB経由のファイル送受信を制限します。	WP
ロック画面の機能	ロック画面関連の制限項目を全て制限します。	WP
個人領域でのSmartLock使用を許可する	個人領域でのSmartLock使用を制御します。	WP
ロック画面カメラ	ロック画面のカメラの利用を制限します。	WP
全ての通知	ロック画面に表示される全ての通知を制限します。	WP
通知内容	ロック画面に表示される通知の内容を制限します。	WP
指紋認証	指紋認証の利用を制限します。	WP
個人領域での指紋認証使用を許可する	個人領域での指紋認証使用を制御します。	WP
ファクトリーリセット保護	ファクトリーリセット保護を制限します。	WP

■仕事領域をオフにする最大日数

仕事領域をオフにする最大日数を設定する	仕事領域をオフにする最大日数を設定します。	WP

■ファクトリーリセット保護

ファクトリーリセット保護で使用するアカウントを管理者が指定したアカウントに設定する	-	WP

■許可設定

Android Enterpriseによりデフォルトで禁止されている機能を許可します。

※チェックを入力すると該当機能の使用が許可されます。

※本項目の端末機能は使用を許可されない限り使用できません。

【Play Store のアカウント変更を許可する(Comp)】

表示場所 >>> 「Playストア」→左上の「アイコン」

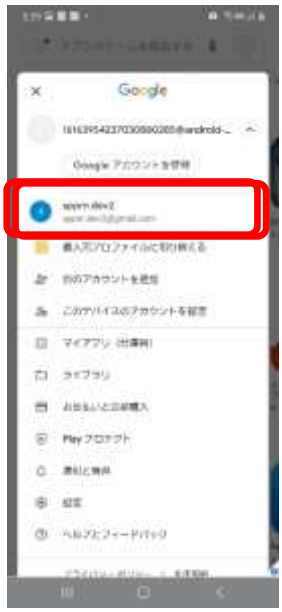
「Play Store のアカウント変更を許可する」ことができます。

チェックをつけると、デフォルトで禁止されていたPlay Storeのアカウント切り替えを許可できます。

デフォルト状態(制限状態)

プルダウンをタップしてもアカウントが表示されず、切り替えができません。

許可状態



アカウントが表示され、切り替えが可能です。

【管理アカウントの追加・削除を許可する（Comp）】

表示場所　>>>　「設定」→「アカウント」→「仕事領域」

「管理アカウントの追加・削除を許可する」ことができます。

チェックをつけると、デフォルトで禁止されていた管理アカウントの追加・削除を許可できます。

※端末によって表示場所は異なる場合があります。

■制限設定

端末の機能をAndroid Enterpriseにより制御します。

※チェックを外すと該当機能の使用が制限されます。

【Work Profile外へのデータコピー（Comp）】

Work Profile（仕事領域）内のテキストなどのデータをWork Profile（仕事領域）外へコピーすることを禁止することができます。

例）バッジ付きのChrome上でテキストをコピーし、バッジの付いていないChrome上でテキストを貼り付けようとすると「貼り付け」という選択肢が表示されずペーストができません。

・「貼り付け」が選択できる状態

・「貼り付け」が選択できない状態

項目一覧へ戻る

【アカウント追加・削除（Comp）】

表示場所　>>>　「端末設定」→「アカウント(アカウントと同期)」

ユーザーによる、仕事領域全般およびアプリ毎のアカウント追加・削除を禁止することができます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

※WorkProfileでは仕事領域のアカウントのみ制限されます。

※Galaxy端末でアカウントの追加・削除を制限すると、「指紋認証」が設定できなくなる場合があります。

≪全体のアカウント追加・削除を禁止する≫

「アカウント追加・削除」のチェックを外すと、仕事領域全般のアカウント追加・削除の項目がグレーアウトします。

◆アカウント追加

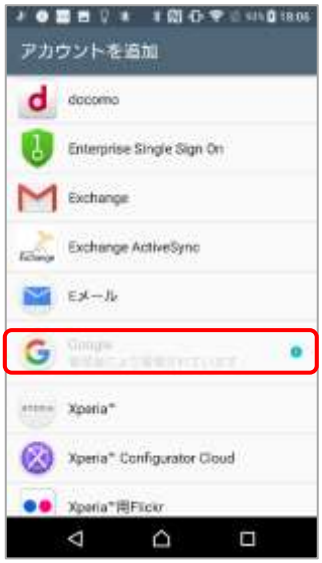
◆アカウント削除

≪アプリ毎のアカウント追加・削除を禁止する≫

「アカウント追加・削除」の項目傘下のアプリ毎のチェックを外すと、該当のアプリのアカウント追加・削除を禁止できます。

※Googleを除き、アプリ内からのアカウント追加は制限状態でも可能です。

◆アカウント追加



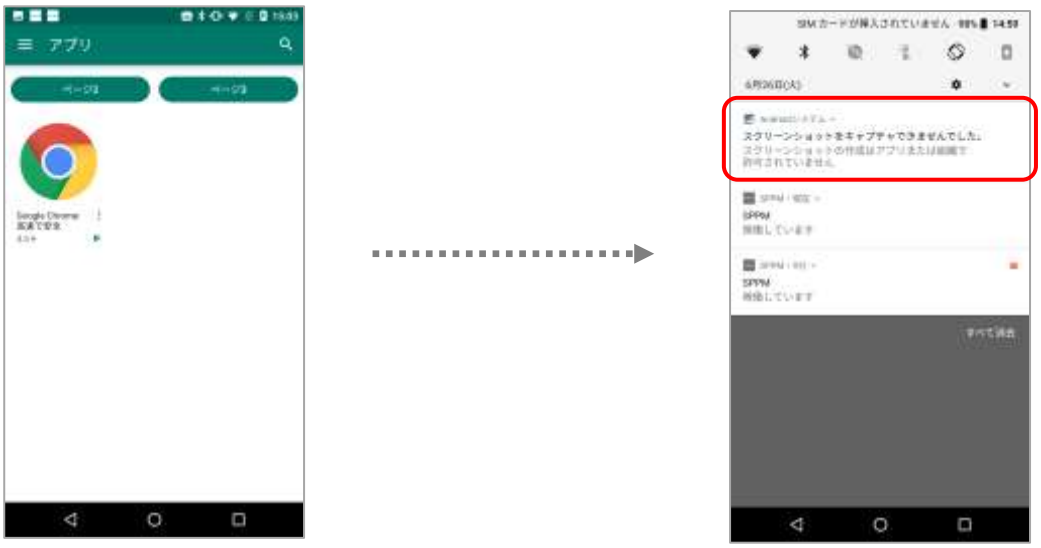
◆アカウント削除

【スクリーンショット（WP）】

Work Profile（仕事領域）上での「スクリーンショット」機能の利用禁止を設定することができます。

チェックを外すと、仕事用バッジの付いたアプリ画面での撮影時、通知領域にスクリーンショットを撮影/保存できない旨のメッセージが表示されます。

※撮影方法は機種によって異なります。



Android 12 の場合、チェックを外すと撮影時に黒い画面が撮影/保存されます。

【個人領域でのスクリーンショットを許可する（WP）】

チェックをつけると、個人領域でのスクリーンショットを許可することができます。

Android 13 の場合、個人領域を制御すると、仕事領域のスクリーンショットも制御されます。

【カメラ（WP）】

「カメラ」機能の利用禁止を設定することができます。

チェックを外すとカメラ起動時にカメラの使用ができない旨のメッセージが表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【個人領域でのカメラ使用を許可する（WP）】

チェックをつけると、個人領域でのカメラ使用を許可することができます。

【外部ストレージのマウント（WP）】

表示場所　>>>　「端末設定」→「ストレージ」→「SDカード」

「外部ストレージのマウント」を禁止することができます。

チェックを外すと、外部ストレージをマウントしようとした際に許可されていない旨のメッセージが表示されます。

※ポリシー適用時にマウント状態であった場合、マウントは自動で解除されません。

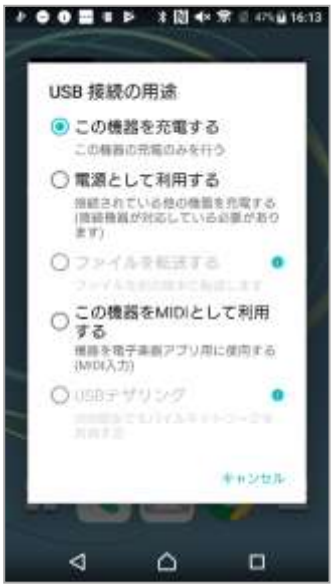
※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【USB経由のファイル送受信（WP）】

「USB経由のファイル送受信」を禁止することができます。

チェックを外すと、USB接続によるPCとのファイル送受信ができなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。



【ロック画面の機能(WP)】

端末認証に関連する以下の機能をすべてまとめて禁止することができます。

※チェックを外すと、ロック画面上での機能が原則すべて使用できなくなります。

※各制御内容は次項をご覧ください。

・個人領域でのSmartLock 使用を許可する(WP)
・ロック画面カメラ(WP)
・全ての通知(WP)
・通知内容(WP)
・指紋認証(WP)
・個人領域で指紋認証を使用を許可する(WP)

【個人領域でのSmartLock使用を許可する(WP)】

個人領域での「SmartLock」の利用を禁止することができます。

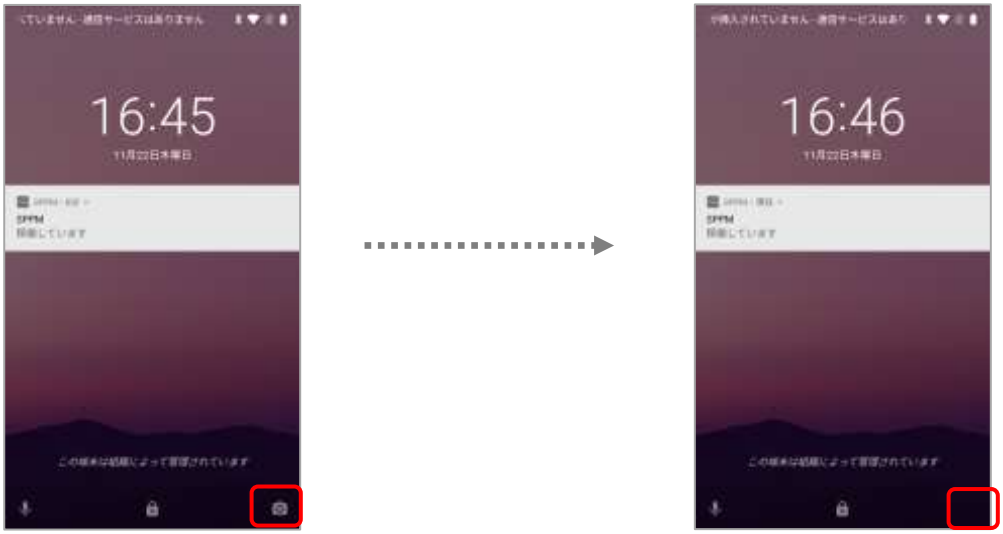
チェックを外すと、「SmartLock」が無効化されます。

【ロック画面カメラ(WP)】

端末の認証画面から起動できる「カメラ」の利用を禁止することができます。

チェックを外すと、「カメラ」が無効化されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。



項目一覧へ戻る

【全ての通知（WP）】

端末の認証画面に表示される通知を非表示にすることができます。

※WorkProfileでは仕事用アプリの通知のみ制限されます。

※認証後の画面では通知は表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【通知内容（WP）】

端末の認証画面に表示される通知内容を非表示にすることができます。

※一部のアプリ（システムアプリ等）では表示される場合があります。

※WorkProfileでは仕事用アプリの通知のみ制限されます。

※認証後の画面では通知内容は表示されます。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【指紋認証（WP）】

仕事領域の指紋認証での端末認証解除を禁止できます。

チェックを外すと指紋マークが鍵マークに変わり、指紋認証できなくなります。

※指紋認証を設定していても指紋認証による解除ができなくなります。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

【個人領域での指紋認証使用を許可する（WP）】

チェックをつけると、個人領域での指紋認証使用を許可することができます。

「統一ロックを使用」をオンに設定かつ【指紋認証（WP）】が無効の場合、
「個人領域で指紋認証使用を許可する」を有効にしても個人領域の指紋認証は利用できません。

項目一覧へ戻る

【ファクトリーリセット保護（WP）】

個人領域にGoogleアカウントがある場合のみ、使用可能です。

Android EnterpriseではGoogleアカウントにログイン状態の端末にハードリセット指示を行った場合、

ファクトリーリセット保護機能により、次に端末初期設定する際に初期化前にログインしていたGoogleアカウントの入力が必要です。

チェックを外した端末にハードリセット指示を行うと「ファクトリーリセット保護」が無効になり、

端末初期設定する際に初期化前にログインしていたGoogleアカウントの入力が不要となります。

※当機能は、制限設定内の「ファクトリーリセット保護」項目を許可した場合、併せて許可状態になります。

※開発者向けオプション＞OEMロック解除がON（ロック解除状態）の場合、ファクトリーリセット保護は有効になりません。

※機種やAndroid OSバージョンによって制限時の画面表示が異なります。

■仕事領域をオフにする最大日数

【仕事領域をオフにする最大日数を設定する(WP)】

端末の仕事領域をオフにする日数を設定することができます。

オフに設定すると、仕事領域全般が利用できなくなります。

指定日数を経過すると、個人領域のアプリがSuspend制御されます。

仕事領域をオンにすることによって、仕事領域および個人領域のSuspend制御が解除され、アプリや機能等の使用が可能になります。

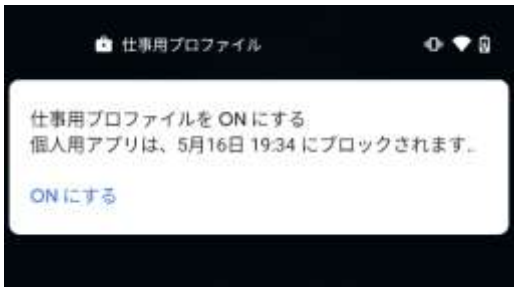
※一部アプリは制御されません。

指定日数経過後

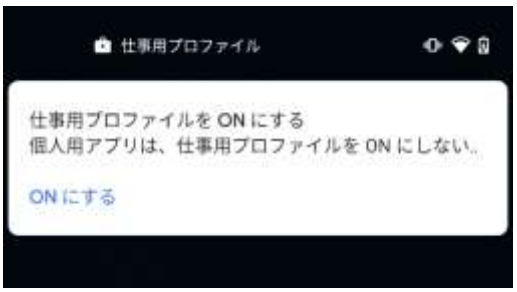
▪▪▪▪▪▶

指定日数の1日前と当日になると、個人用アプリがブロックされる通知が表示されます。

・指定日数1日前



・指定日数当日



■ファクトリーリセット保護

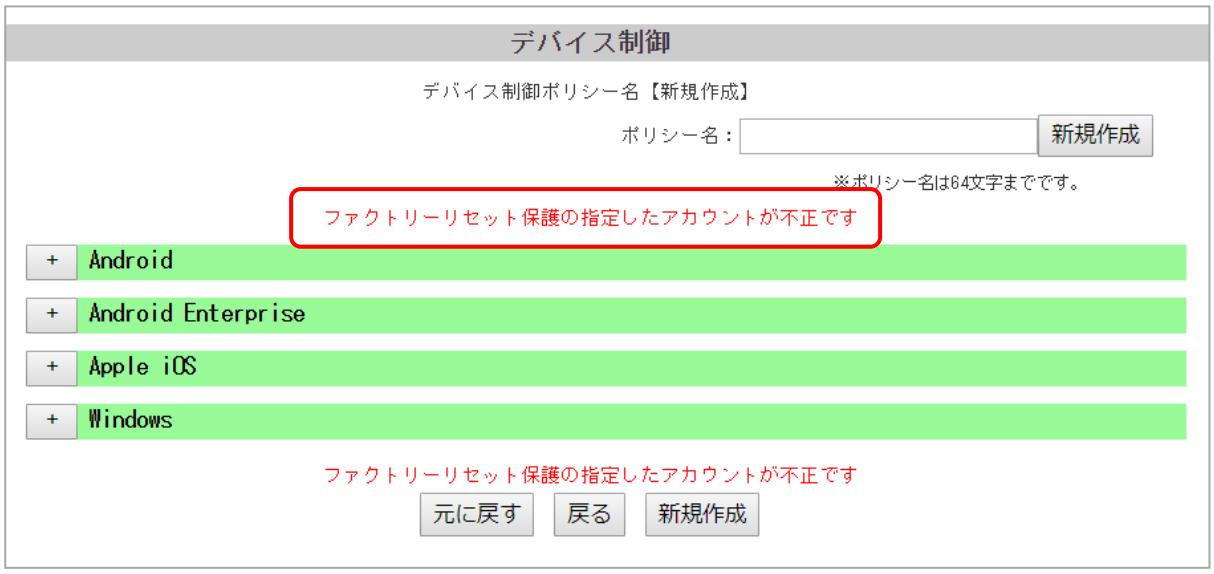
【ファクトリーリセット保護で使用するアカウントを管理者が指定したアカウントに設定する（WP）】

ファクトリーリセット保護で使用するアカウントを管理者が指定したアカウントに設定するを入力することが可能です。

※利用には「G Suiteアカウント ／ Google管理者アカウント」での企業登録が必要です。

※Android企業登録で利用したアカウントのドメインのみ指定可能です。

※G-Suite環境でのみ対応しているため、Managed Google Playアカウントで企業登録された管理画面ではポリシー作成時に以下のようなエラーが表示され、ポリシー作成ができません。



項目一覧へ戻る

4. キオスク管理ポリシー

【概要】

Work Managed Device モードの Android Enterprise 端末にキオスク管理ポリシーを適用することで、業務専用のアプリケーションのみを表示させ、そのほかの操作を禁止することが可能です。（以下、キオスクモードと記載）
この機能を利用することで、端末を「単一業務のみに活用するデバイス」として管理することができます。

キオスク管理ポリシーの詳細については弊社までお問い合わせください。

【稼働環境】

・対応 OS

Android OS v7.x ～ v10.x

・対応 SPPM Agent

v3.54～

※Android OS9 の端末は、SPPM Agent v3.46 以降で利用可能です。

5 Android Enterprise 機能 / Google

1. 概要

管理画面のメニューバー[その他]から「Android Entreprise」を利用した各機能をご利用できます。

■SafetyNet 設定

SafetyNet 機能の端末登録時と定期実施時に関する設定を行えます。

■Google アカウント管理

Google 管理者アカウントを管理画面上で管理できます。

■Comp / Work Profile[企業所有] 設定

Comp 端末における Work Profile のキッティングや、制御内容の設定ができます。

■承認アプリ管理

GooglePlay から Android Enterprise でする利用アプリを選択し承認できます。

■サイレントインストール / アンインストール

Android Enterprise 端末を選択し、承認したアプリのサイレントインストール/アンインストールを行えます。

■アプリ設定

承認したアプリの権限設定や設定項目の設定値を登録できます。

■Play ストア設定

管理対象 Android Enterprise 端末に表示される GooglePlay ストア内のレイアウトや表示アプリを設定できます。

■証明書配布

Android Enterprise 端末に証明書の配布ができます。

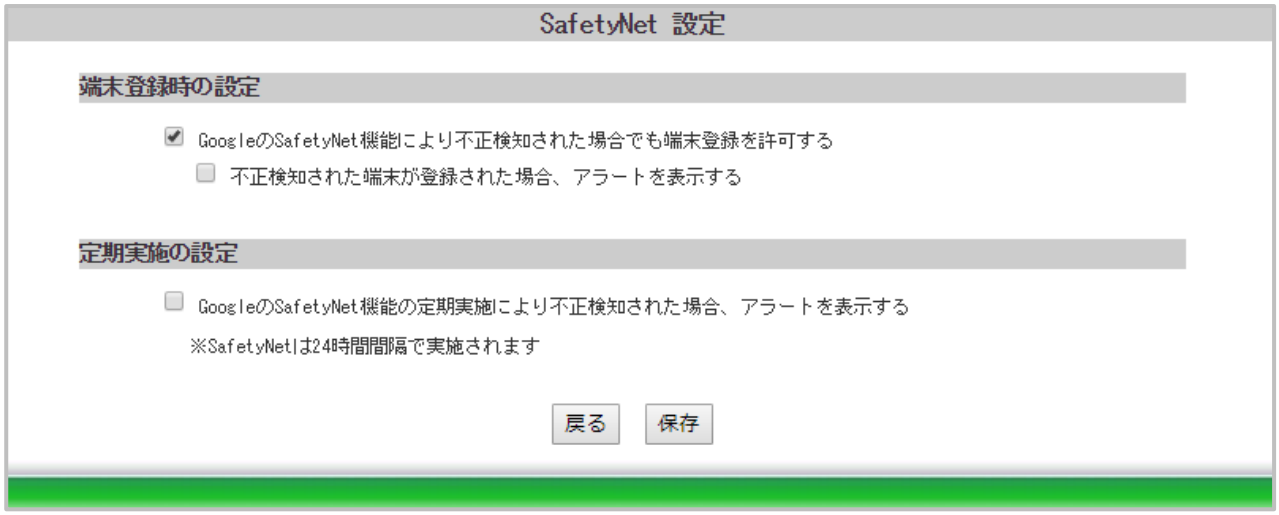
■デバッグログ一覧

Android Enterprise 端末から受け取ったデバッグログを、ダウンロードすることができます。

詳細については STAR-MDM 管理者マニュアル Android 版 をご確認ください。

2. SafetyNet設定

SafetyNet 機能の端末登録時と定期実施時に関する設定を行えます。

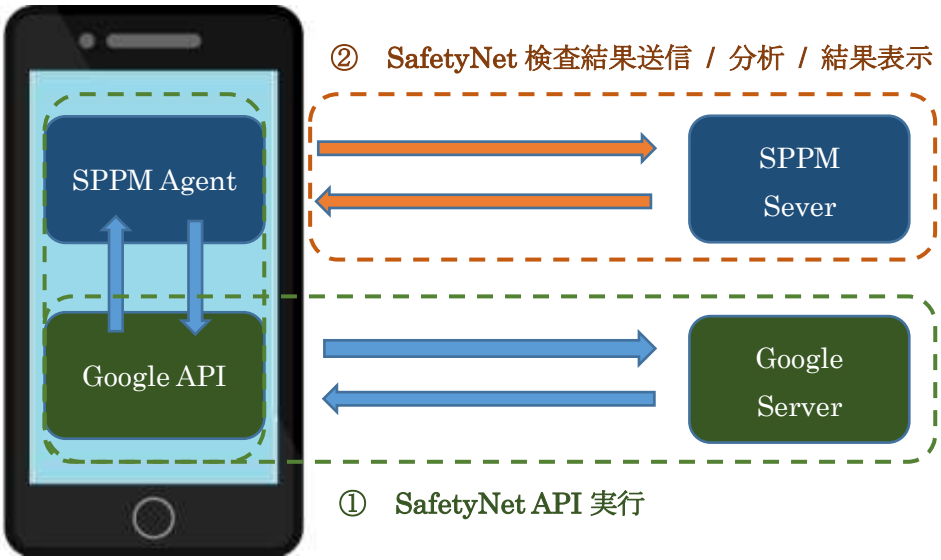


【SafetyNet 機能概要】

SafetyNet 機能では Google API により端末のソフトウェア/ハードウェアのセキュリティ検査を行えます。

検査は Android Enterprise 端末の登録時と 24 時間間隔で定期的に実行されます。

※SPPM Agent v3.40 以降対応



① SafetyNet API 実行

SPPM Agent から SafetyNet API を実行し、Google Server から検査結果を取得します。

② SafetyNet 検査結果送信 / 分析 / 結果表示

取得した SafetyNet の検査結果を STAR-MDM サーバへ送信し、分析を行い結果を表示します。

結果は STAR-MDM 管理画面の「ログ管理」と「アラート(異常時のみ)」に表示されます。

また、端末登録時の検査では「端末登録時の設定」により異常時のみ Agent に結果が表示されます。

【端末登録時の設定】

■Google の SafetyNet 機能により不正検知された場合でも端末登録を許可する

端末登録時には必ず SafetyNet 機能により検査が実行されます。

このとき下記のように正常ではない検査結果となった場合に、登録を許可するかを設定できます。

・不正端末と検知された。

・SafetyNet の検査実行に失敗した。

≪端末登録時　検査実行と不正検知≫

「Google の SafetyNet 機能により不正検知された場合でも端末登録を許可する」の設定がオフであり、SafetyNet 検査による結果が異常だった場合に、端末は管理画面に登録されません。

※端末画面には検査結果が異常だった場合のみ結果が表示されます。

※WorkProfile では異常結果により登録不可だった場合、グループキー入力画面に戻らず、仕事領域の削除と SPPM Agent の再インストールが必要です。

このとき STAR-MDM 管理画面には、登録を行ったライセンスのステータス列に、「SafetyNet 違反」または「SafetyNet 検査失敗」が表示されます。

※このステータスが表示されたライセンスは、該当端末以外の登録を受け付けない状態となっているため、ライセンスを解放するには「ライセンスキーリセット」を行ってください。

※「SafetyNet 検査失敗」と結果が表示された場合は、端末登録時の通信不良や GoogleServer 等の外部起因により検査が失敗している可能性があります。時間をおいて再度登録をお試しください。

■不正検知された端末が登録された場合、アラートを表示する

「Google の SafetyNet 機能により不正検知された場合でも端末登録を許可する」の設定がオンだった場合、SafetyNet 検査による検査結果が異常であっても端末が登録されます。

このとき管理画面にアラートを表示するかを設定できます。

【定期実施の設定】

■Google の SafetyNet 機能の定期実施により不正検知された場合、アラートを表示する

SafetyNet 機能は約 24 時間間隔で定期的に実施され、端末のセキュリティ検査を行います。

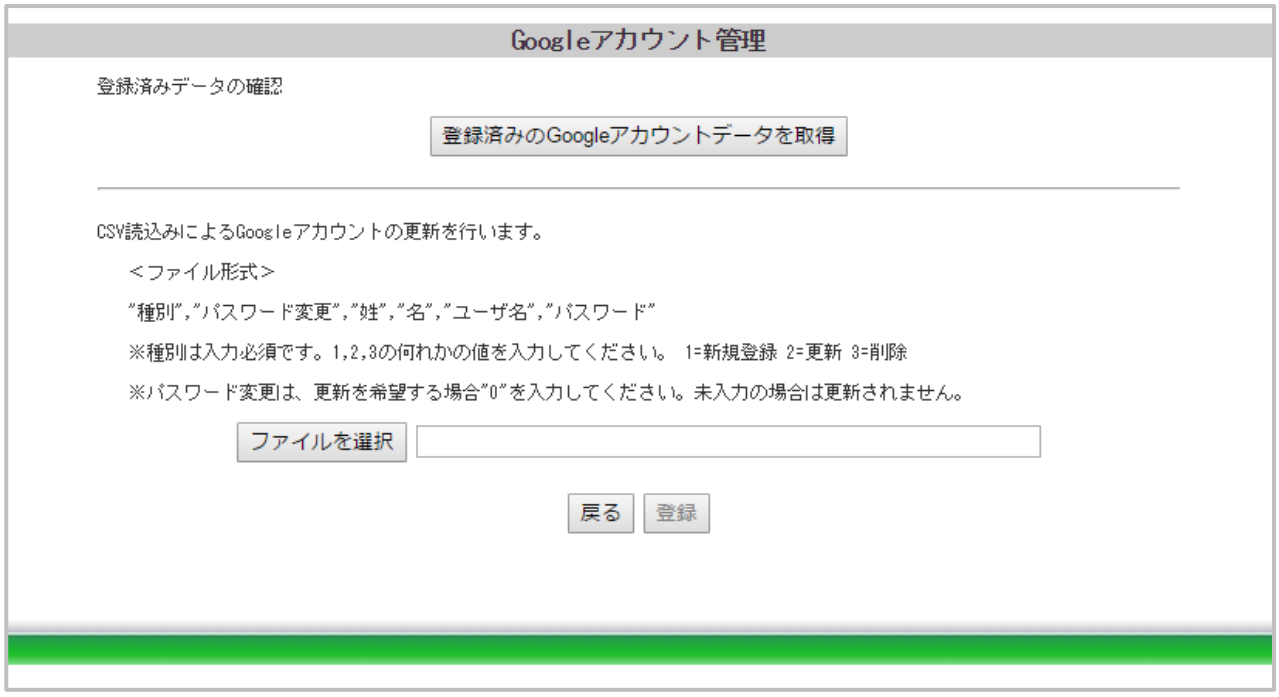
このとき、不正端末と検知された場合に「アラート」を表示するかを設定できます。

定期実施はAndroid OSの節電機能等の影響により実行タイミングが前後します。

3. Googleアカウント管理

管理ドメイン内の Google アカウントの新規作成／更新／削除が管理画面上から行えます。

※G Suite アカウント/Google 管理者アカウントで Android 企業登録した場合のみご利用いただけます。

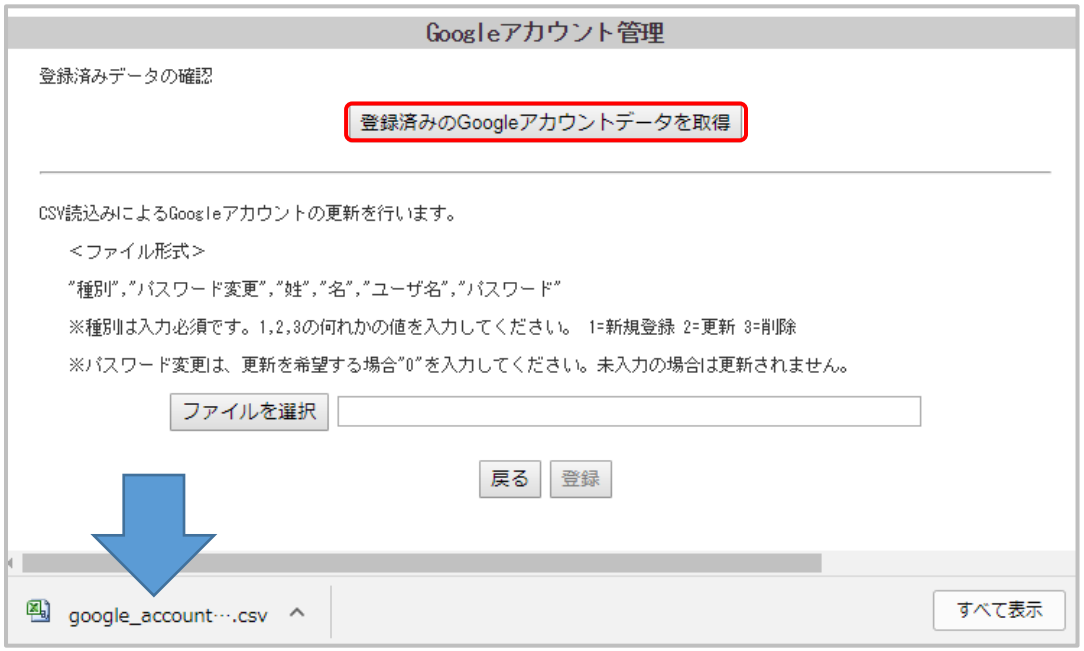


≪登録済みのデータの確認≫

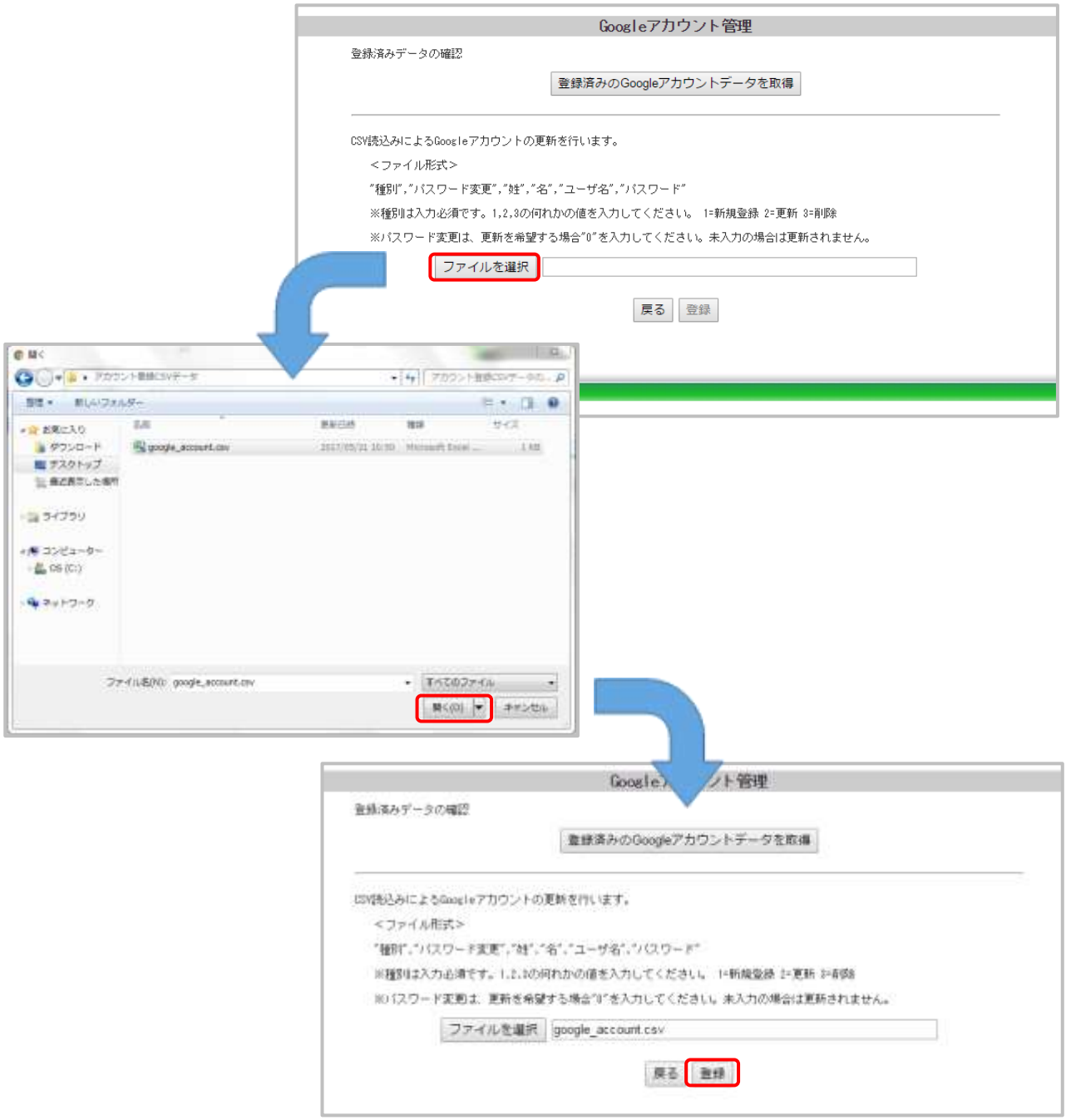
「登録済みの Google アカウントデータを取得」ボタンを押下すると、現状登録されているアカウントのデータが CSV 形式で書き出され、PC にダウンロードされます。

【CSV 読込みによる Google アカウントの更新方法】

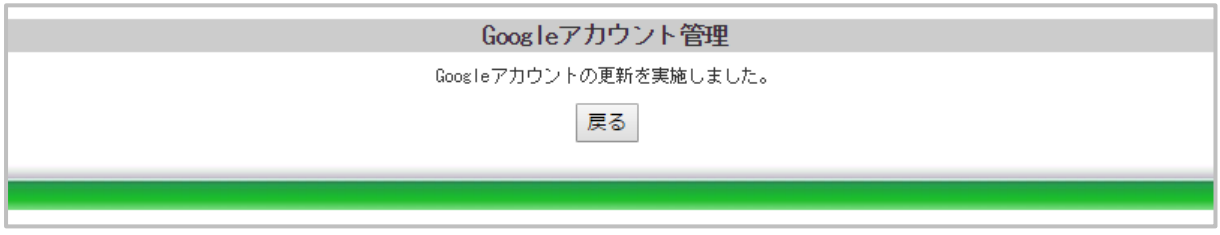
「登録済みの Google アカウントデータを取得」ボタン押下で CSV データをダウンロードします。



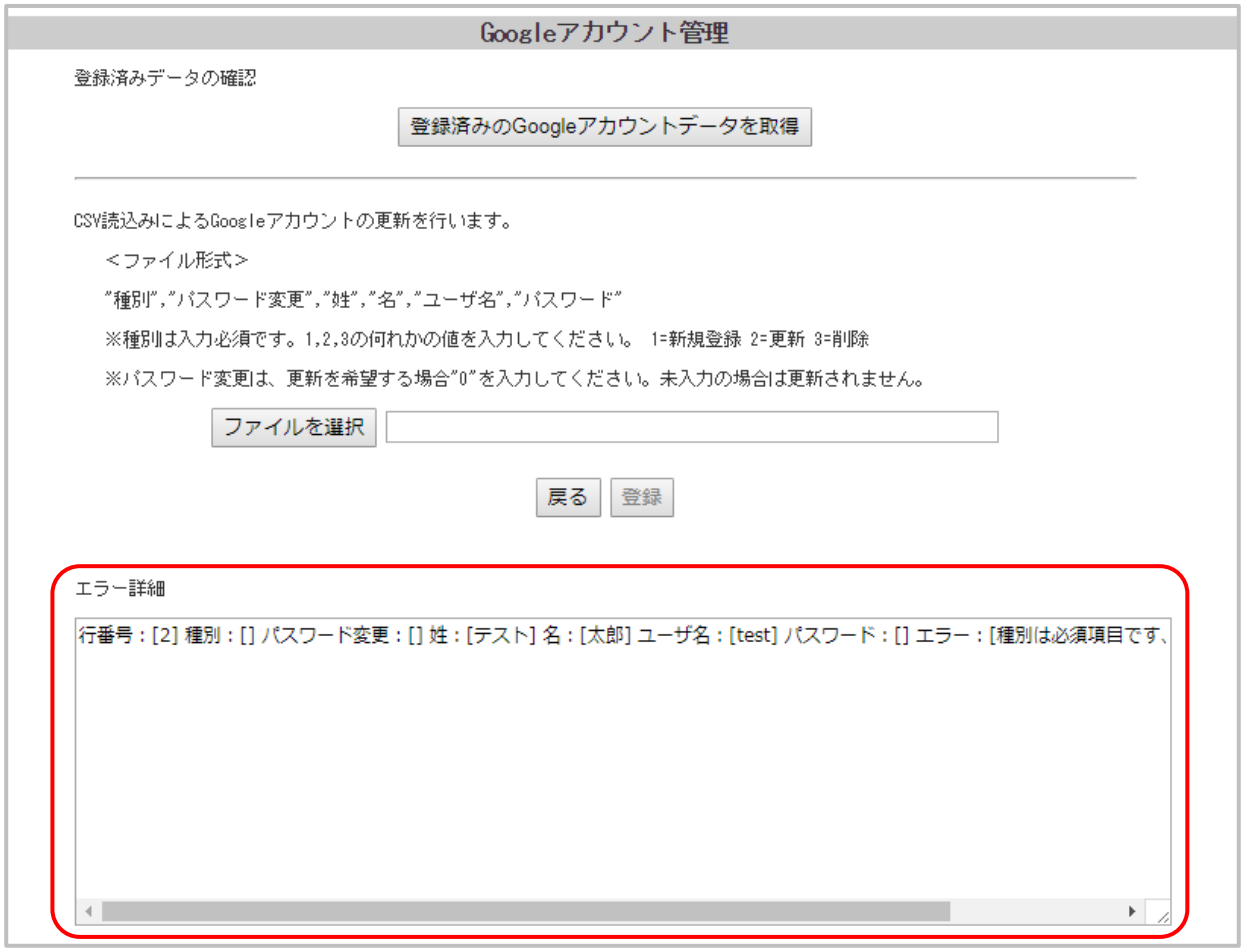
ダウンロードした CSV を編集し「ファイルを選択」でファイルをアップロードし登録を押下します。



データに問題がなければ登録完了画面に遷移し、Google アカウントの変更/更新が更新されます。



データ内容が不足していたり、正しくない値が入力されているとエラー詳細が表示されます。



≪注意≫

種別は入力必須です。1,2,3の何れかの値を入力してください。 1=新規登録 2=更新 3=削除

パスワード変更は、更新を希望する場合"0"を入力してください。未入力の場合は更新されません。

4. Comp / Work Profile[企業所有] 設定

Work Profile のキッティング時の設定や、Work Profile の制御ができます。

※本設定は Managed Google Play アカウントで企業登録された環境でのみ設定可能です。

Comp設定

Comp 端末における Work Profile のキッティングや、制御内容の設定ができます。

【キッティング設定】

■Work Managed Device 端末で Work Profile 作成機能を有効化する

この項目をチェックありにすると Work Managed Device 端末でユーザーによる Work Profile の作成ができるようになります。

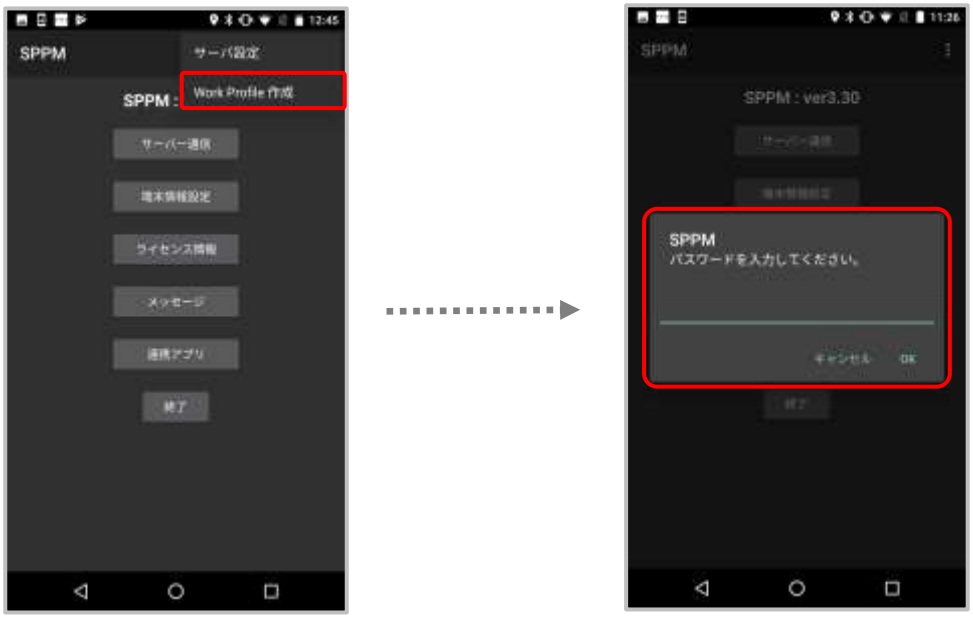
※Agent 画面右上の「：」ボタンから Work Profile 作成が行えるようになります。

■Work Profile 作成時に Work Managed Device 側の管理アカウントを削除する

この項目をチェックありにすると、Work Profile 作成が行われた際に Work Managed Device 側の管理アカウントが自動的に削除されます。

■Work Profile 作成時にパスワード認証を求める

この項目にチェックを入れ、任意のパスワードを設定すると、Work Profile 作成時にパスワード要求ダイアログが表示されます。



【Work Profile 制御】

■端末操作による Work Profile の削除を許可する

この項目をチェックありにすると、ユーザー操作による Work Profile の削除ができるようになります。

チェックなし　　**チェックあり**

■Work Profile が削除されたことを検知し、自動で Work Profile を再作成する

※再作成してもインストールしていた Work Profile アプリなどの元データは復元しませんのでご注意ください。

※パスワード設定が有効の場合でもパスワード入力は不要で自動作成されます。

クロスプロファイル権限設定

クロスプロファイル権限設定で登録したアプリが端末の仕事領域・個人領域両方にインストールされている場合、アプリ間での権限の共有、互いのデータへのアクセスを許可する設定が可能になります。

※クロスプロファイル権限設定を行った後に、端末側での操作も必要となります。

※仕事領域・個人領域間で共有できるアプリは端末によって異なります。

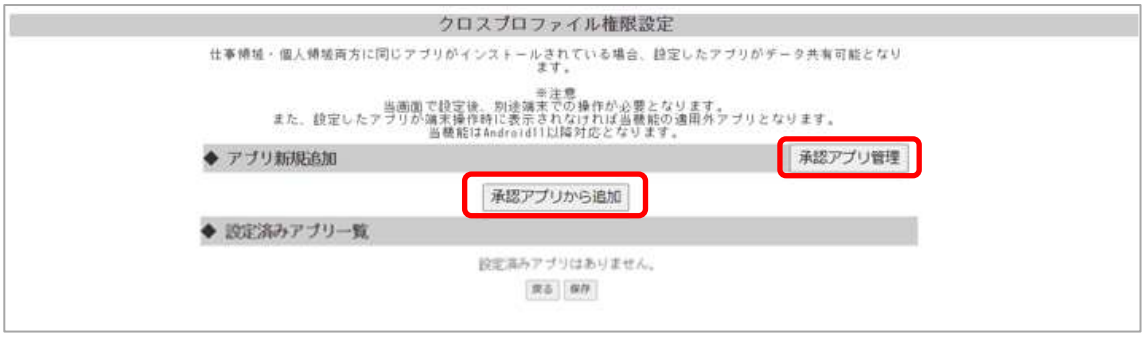
「Comp / Work Profile[企業所有] 設定」にて共通で利用可能なアプリを
クロスプロファイル権限設定を利用して、「承認アプリ管理から追加」から任意のアプリを選択し設定をします。

【アプリ新規追加】

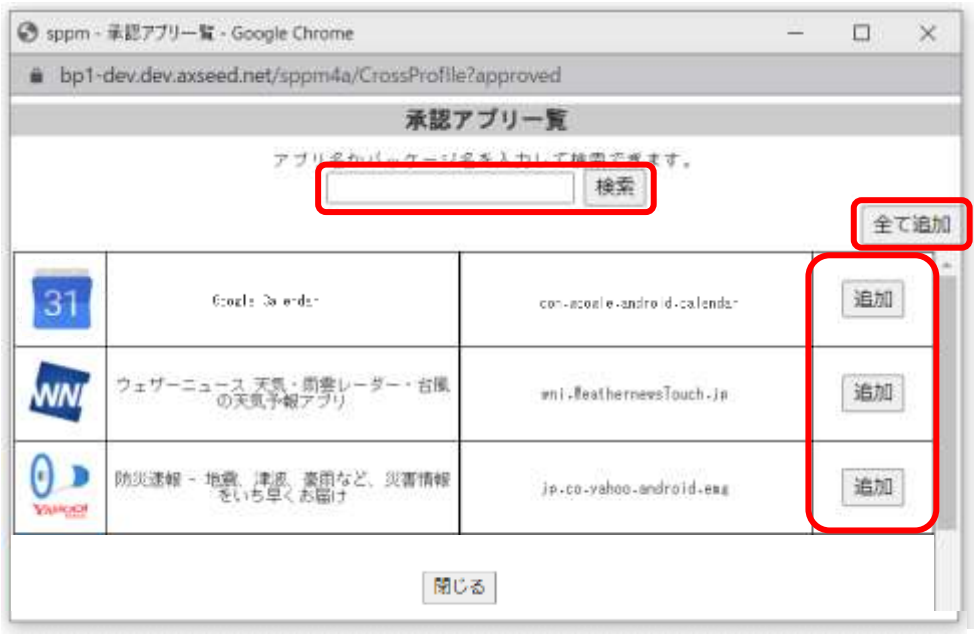
「承認アプリから追加」をクリックすると、アプリ追加画面が別ウィンドウで表示されます。

承認されていないアプリがある場合は「承認アプリ管理」から承認してください。

関連情報☞「承認アプリ管理」



アプリ名やパッケージ名から検索して追加する場合は、検索ワードを入力し「検索」をクリックします。
アプリ毎に追加する場合は、該当のアプリの「追加」をクリックしてください。
全てのアプリを追加したい場合は、「全て追加」をクリックしてください。



追加したアプリは設定済みアプリ一覧の下に表示されます。
最後に「保存」をクリックすると追加が完了です。

クロスプロファイル権限設定完了後、端末設定内の「シングルプロファイルモード」にて対象アプリを接続済みにする事により、アプリデータの共有が可能となります。
※対象アプリが個人領域と仕事領域に両方インストールされている必要があります。

アプリや端末によってデータの共有ができない場合があります。

表示例：SH-53A にカレンダーアプリをインストールした場合

5. 承認アプリ管理

GooglePlay から Android Enterprise で利用するアプリを選択します。

関連情報☞Play ストア設定

承認アプリ管理にてアプリを選択後、Play ストア設定にてアプリのレイアウトを設定しない場合、選択したアプリがすべて Play ストア上に表示されます。
Play ストア上に表示するアプリを制御したい場合、Play ストア設定＞レイアウト設定をご利用ください。

Play ストア設定しない場合、選択したアプリが端末の Play ストア上に表示されるまで時間が掛かる場合があります。

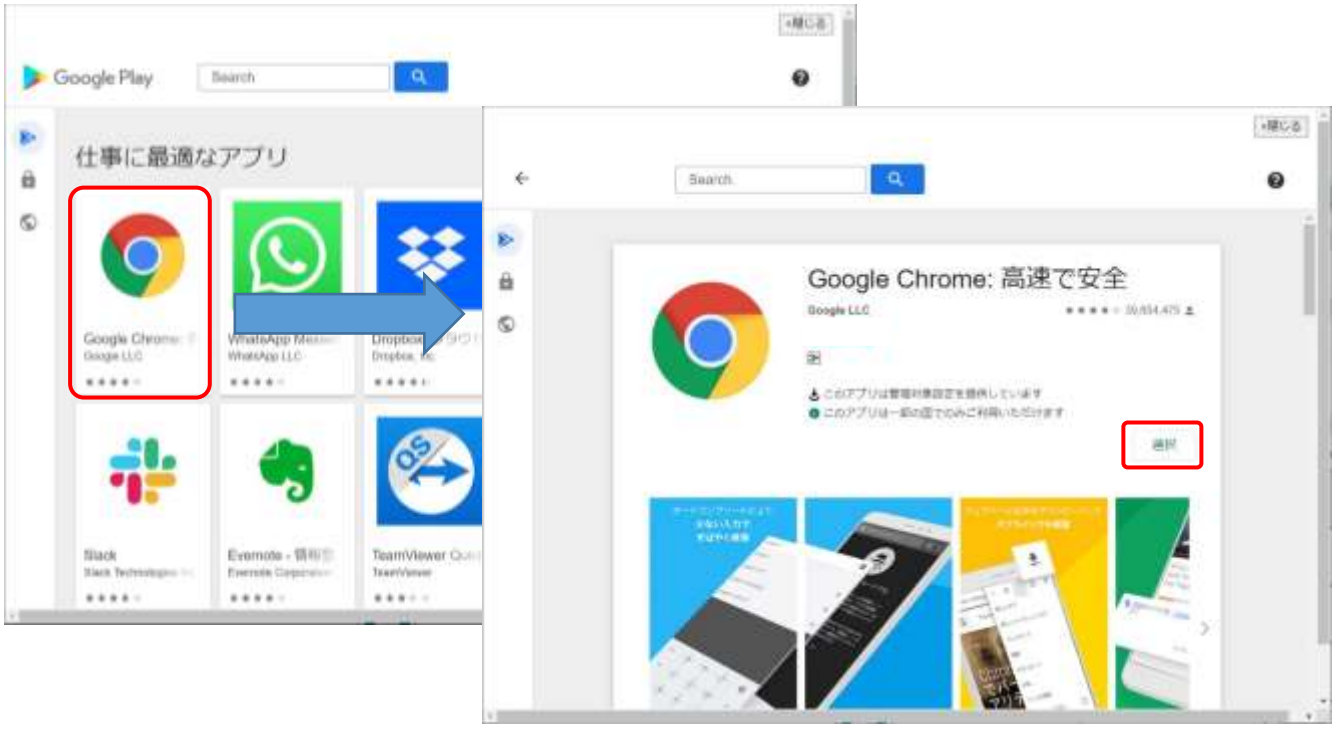
対象アプリのAPIレベル（targetSdkversion）がOSに対応していない場合、
デバイスのPlayストアに表示されないことがあります。

≪各ボタンの説明≫

【アプリの選択方法】

「GooglePlayを開く」をクリックしてください。

別ウィンドウで Google Play が開きます。任意のアプリをクリックし「アプリの詳細」画面を開き、
「選択」をクリックしてください。



確認成功のダイアログが表示されますので、「閉じる」をクリックしてウィンドウを閉じてください。

選択が完了すると承認済みアプリー覧にアプリが表示されます。
※アプリー覧が更新されない場合は「F5」キーで画面更新を行ってください。

【アプリの非承認方法】

承認済みアプリー覧の右側にある「非承認」ボタンを押下します。

非承認完了ダイアログが表示されますので「閉じる」をクリックしてください。

該当のアプリが承認済みアプリー覧から削除されます。

【アプリのアクセス権】

承認アプリのアクセス権の付与状況を確認できます。
また、Comp 機能を利用する場合はアクセス権の付与を Work Managed Device と Work Profile で分けて行うことができます。
※アクセス権をもつアプリのみ該当管理モードでインストールが可能です。

≪Work Managed Device 端末のみの利用におけるアクセス権≫

Work Managed Device 端末のみの利用ではアクセス権があるアプリのみ端末上に表示できます。

Work Managed Device のアクセス権はアプリ承認時に自動で付与されるため、操作は必要ありません。

アクセス権の設定変更設定は次項「Comp 端末の利用におけるアクセス権設定方法」を参照ください。

WMD と表示されているアプリのみ
Work Managed Device 端末で
表示させることができます。

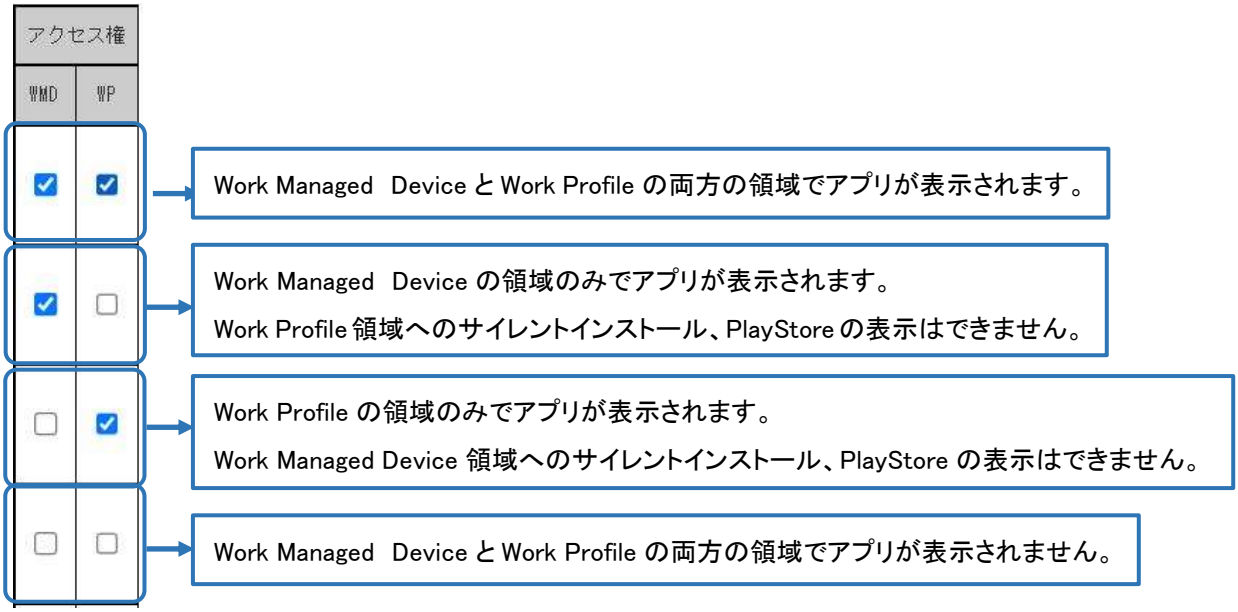
≪Comp 端末の利用におけるアクセス権設定方法≫

Comp / Work Profile[企業所有] 設定＞Comp 設定の「Work Managed Device 端末で Work Profile 作成機能を有効化する」の項目が有効になっている場合、各承認アプリのアクセス権を Work Managed Device / Work Profile 毎に設定できます。

「Work Managed Device 端末で Work Profile 作成機能を有効化する」設定については、Comp / Work Profile[企業所有] 設定をご確認ください。

関連情報☞「Comp / Work Profile[企業所有] 設定」

アクセス権の列のチェックボックスでアクセス権の設定を行うことができます。



アクセス権の設定を保存するには画面下の「保存」ボタンをクリックしてください。
※反映に時間がかかることがあります。

「Work Managed Device 端末で Work Profile 作成機能を有効化する」の項目が有効になっていない場合は、以下のように設定項目のチェックボックスがなくなり、アクセス権の設定を行えなくなります。

限定公開アプリ / ウェブアプリ

【限定アプリの作成方法】

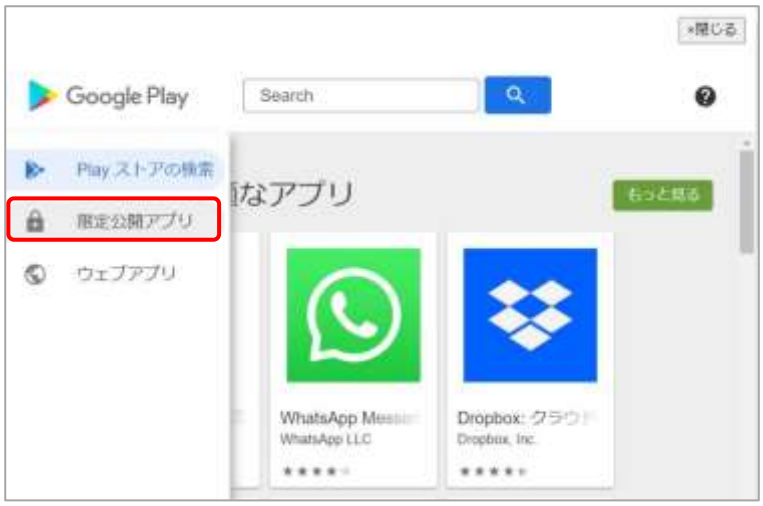
Google Play 画面から自社アプリを一般公開せずに承認アプリに追加できます。

ビジネス向け GooglePlay ヘルプ ： 限定公開アプリの公開と管理

≪追加方法≫

① 承認アプリ管理画面で「Google Play を開く」ボタンをクリックしてください。

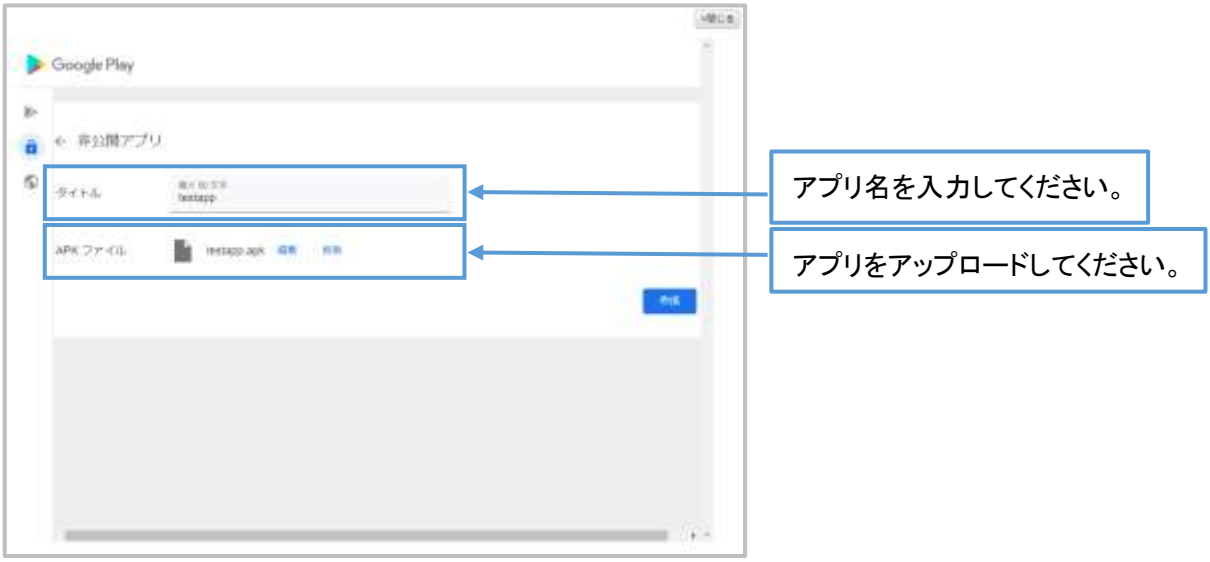
② 画面左のメニューから「限定公開アプリ」をクリックしてください。



③ 画面右下の「+」ボタンをクリックしてください。

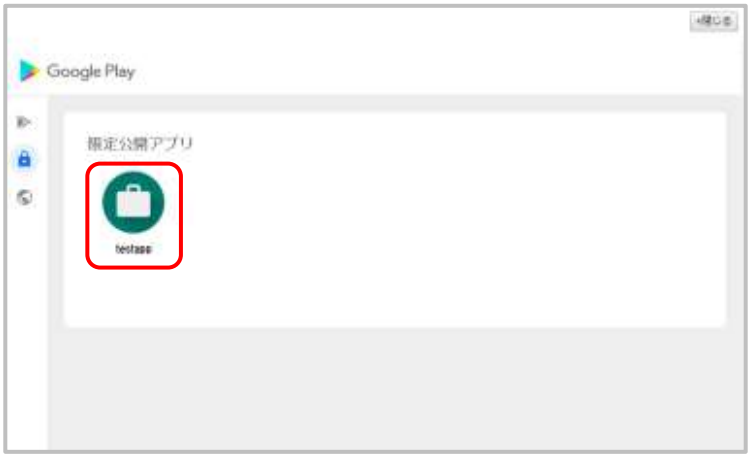
④追加画面が表示されますのでタイトルと APK ファイルのアップロードを行ってください。

※GooglePlay ストア側の規定により APK ファイルの容量は「100MB 以下」にする必要があります



⑤アップロードが成功したら「作成」ボタンをクリックしてください。

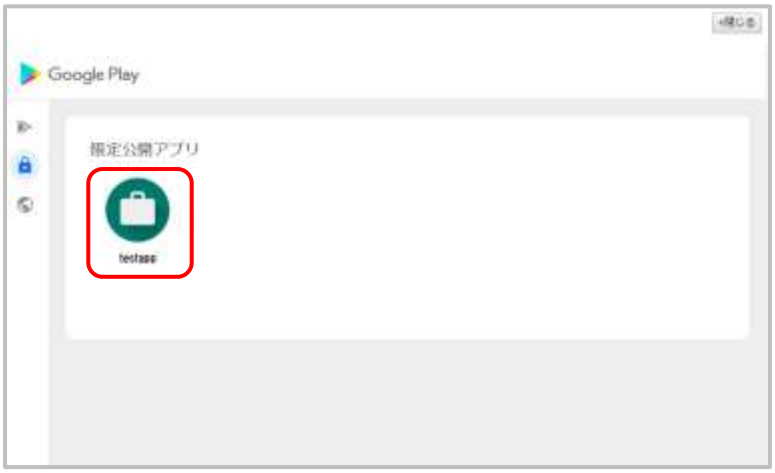
⑥登録が完了すると以下のように表示されます。



公開されるまで 10 分ほど時間がかかります。
また、Google Play ストアに既に公開されている（一般・限定問わず）同一パッケージ名の APK ファイルは登録できません。

≪編集方法≫

①限定公開アプリ一覧画面で編集するアプリをクリックしてください。



②以下の画面で「編集」ボタンをクリックしてください。

③編集が完了しましたら「保存」ボタンをクリックしてください。

反映されるまで 10 分ほど時間がかかります。

詳細な編集オプションからは詳細な説明、スクリーンショットなどを設定可能です。

また、Google Play 画面から限定公開アプリを「削除」した場合、同一パッケージ名の APK ファイルは登録できなくなるためご注意ください。

【ウェブアプリの作成方法】

Google Play 画面からウェブアプリを一般公開せずに承認アプリに追加できます。

ウェブアプリはアドレス（URL）、アイコン画像、およびタイトルを使用して作成した Android アプリです。

ウェブアプリを開くと、そのアプリの URL を Chrome ブラウザで開きます。

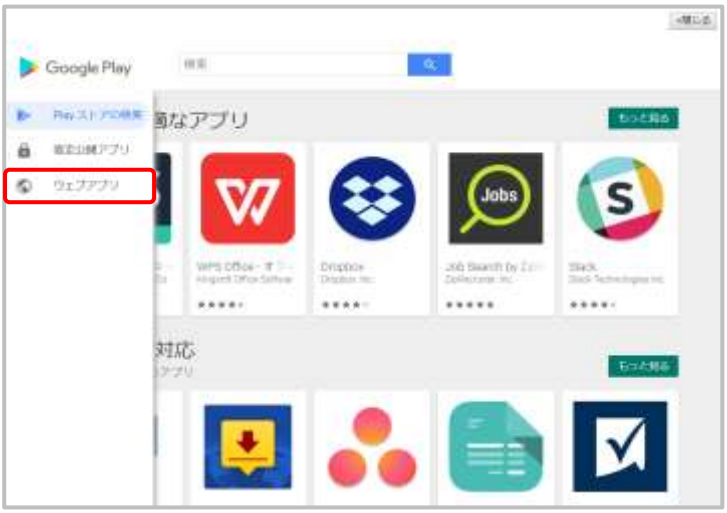
※ご利用の際は利用アプリ制限ポリシーで Chrome を制限しないようご注意ください。

ビジネス向け GooglePlay ヘルプ ： ウェブアプリを作成する

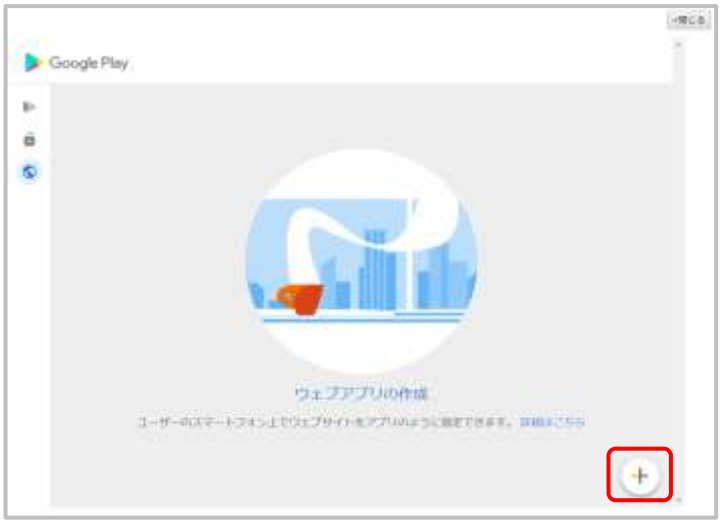
≪追加方法≫

① 承認アプリ管理画面で「Google Play を開く」ボタンをクリックしてください。

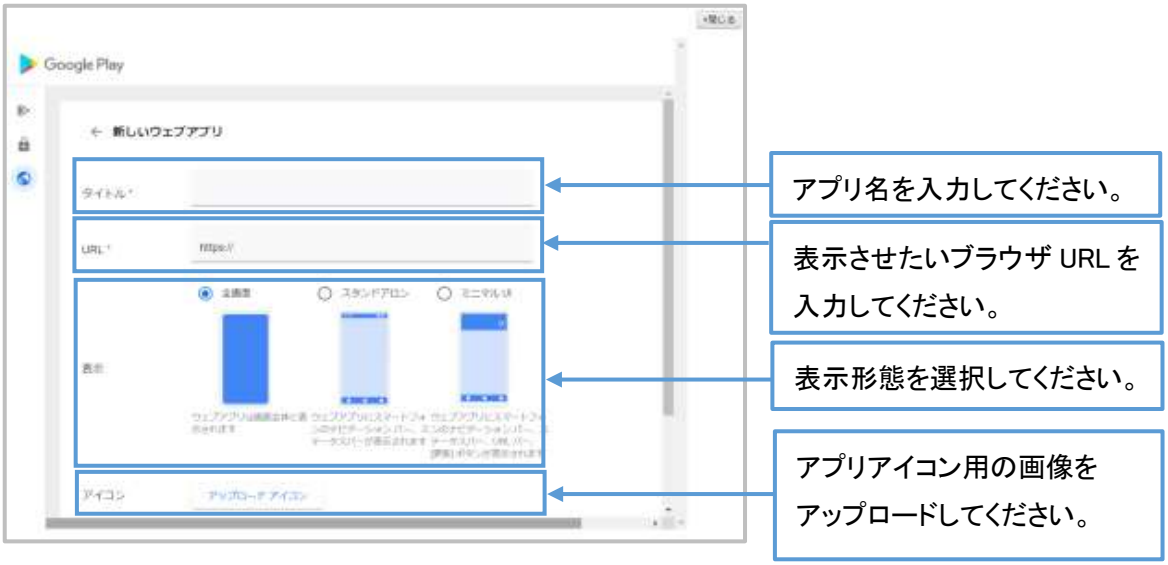
②画面左のメニューから「ウェブアプリ」をクリックしてください。



③画面右下の「+」ボタンをクリックしてください。



④追加画面が表示されますのでタイトル／URL／表示形態／アイコンのアップロードを行ってください。



⑤アップロードが成功したら「作成」ボタンをクリックしてください。

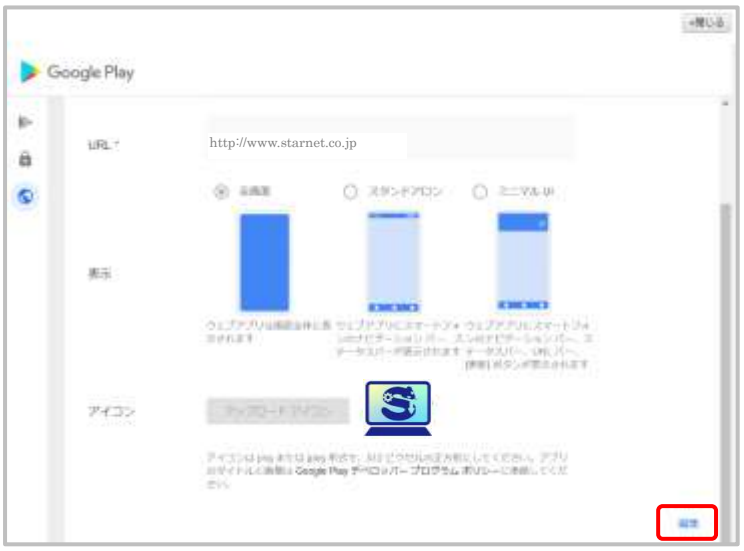
⑥登録が完了すると以下のように表示されます。

公開されるまで 10 分ほど時間がかかります。

≪編集方法≫

①ウェブアプリ一覧画面で編集するアプリをクリックしてください。

②以下の画面で「編集」ボタンをクリックしてください。



③編集が完了しましたら「保存」ボタンをクリックしてください。

反映されるまで 10 分ほど時間がかかります。

【作成した限定アプリ/ウェブアプリの承認アプリ追加方法】

① 承認アプリ管理画面で「GooglePlay を開く」ボタンを押下します。

② 「限定公開アプリ」または「ウェブアプリ」を押下します。

③ 追加したいアプリを押下します。

④ 「選択」ボタンを押下します。

⑤ 「アプリの選択に成功しました。」の画面が表示されます。
「閉じる」を押下し、画面を閉じてください。

⑥ 承認済みアプリ一覧に、登録した限定アプリやウェブアプリが表示されます。

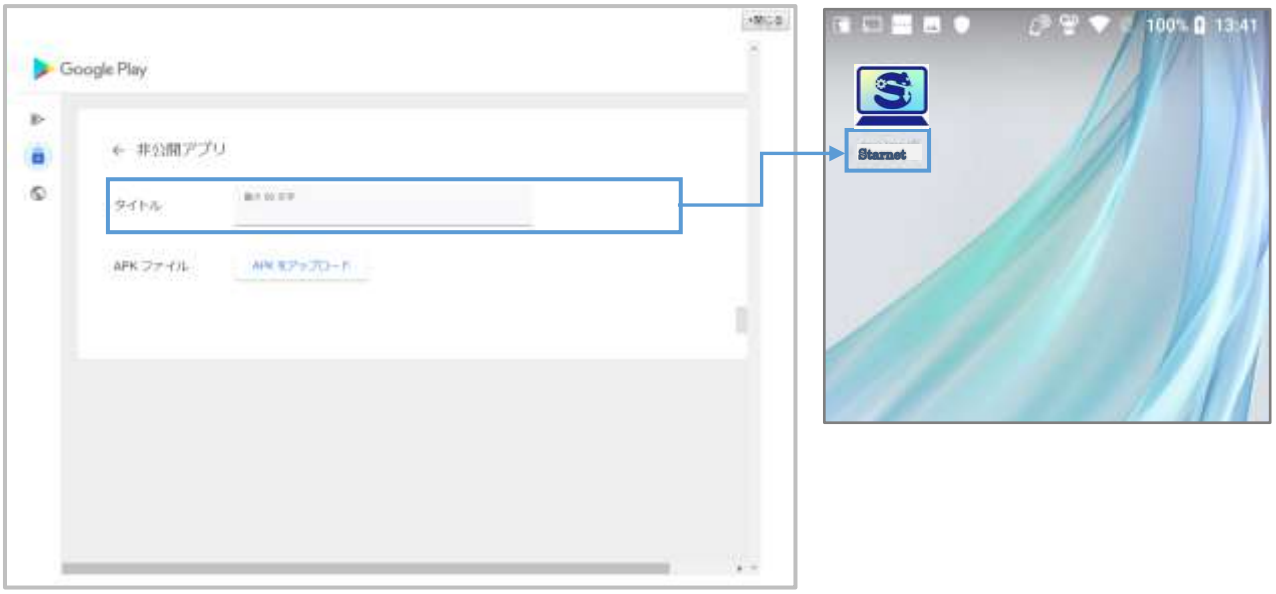
※それ以降のインストール方法は下記項目をご確認ください。

「サイレントインストール方法」

「PlayStore からのインストール方法」

【限定アプリ/ウェブアプリの端末での表示】

≪限定アプリの端末での表示≫



≪ウェブアプリの端末での表示≫

① タイトル ／ ④ アイコン

④

追加画面で「アイコン」にアップロードした画像がアプリアイコンとして表示されます。

①

追加画面で「タイトル」に入力した文字列が表示されます。

② URL

追加画面で「URL」に入力した
Web ページが表示されます。

③ 表示

画面の表示形態を 3 つのタイプから選択できます。

全画面

全画面表示

スタンドアロン

ステータスバーとナビゲーションバーを表示

ミニマル UI

画面上部に URL 表示

6. サイレントインストール / アンインストール

Android Enterprise 端末を選択し、承認アプリのサイレントインストール/アンインストールを行えます。

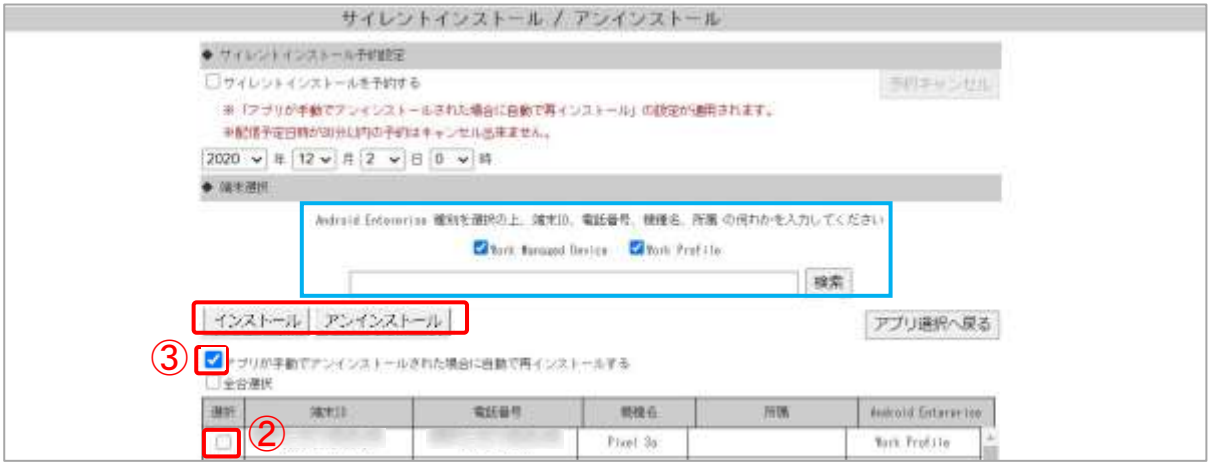
デバイス制御ポリシー「アプリのインストール」「アプリのアンインストール」を制限中の場合は、サイレントインストール/アンインストールを実施しても端末に反映されません。
「提供元不明のアプリのインストールを許可する」が ON になっていない場合でもインストールは実行されます。

対象アプリの API レベル（targetSdkversion）が OS に対応していない場合、エラーが発生し、サイレントインストールが実施できません。

【サイレントインストール/アンインストール方法】

① インストールまたはアンインストールしたいアプリを選択し「端末選択画面へ」ボタンをクリックします。
（複数選択可）

② 目的の端末を選択する。
※アプリ選択画面で、アクセス権の付与状況に沿った管理モードの端末のみ表示されます。
※CSVを利用してサイレントインストールの対象端末を指定する方法は[こちら]

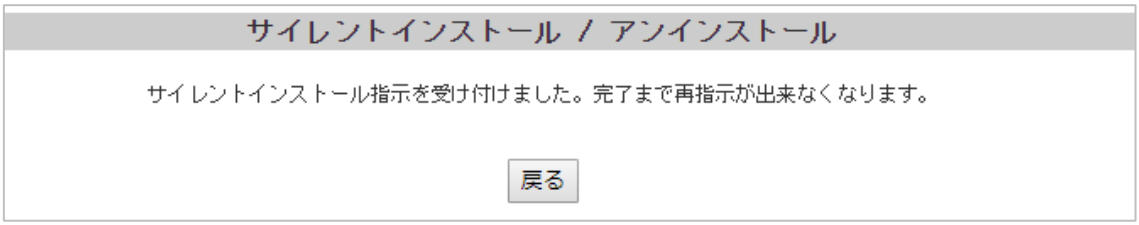


③ 必要に応じて**「アプリが手動でアンインストールされた場合に自動で再インストールする」**にチェックを入れます。チェックを入れてサイレントインストール指示を行うと、端末操作で該当アプリがアンインストールされた際に、自動で再インストールが行われます。
※サイレントインストール指示時にチェックを入れていない場合は、自動再インストールは実施されません。

④ インストールしたい場合は「インストール」ボタン、アンインストールしたい場合は「アンインストール」ボタンをクリックしてください。

⑤ インストール/アンインストール指示が実施されると受け付け完了画面に遷移します。

※Google サーバ側で指示が処理されるまで、次のサイレントインストール/アンインストールの指示を実施する事ができません。



サイレントインストールを行ったあとすぐにサイレントアンインストールの指示を行うと、ステータスやログが正常に表示されない場合があります。半日～1日以上空けてお試しください。

サイレントインストールでインストールしたアプリは、利用アプリ制限による制御ができません。
また、利用アプリ制限で制限しているアプリをサイレントインストールした場合、サイレントインストールは実行されません。
※「Chrome」は利用アプリ制限で制限されていても、サイレントインストール指示が可能です。

※検索欄から、「Work Managed Device」と「Work Profile」の絞り込み、端末ID、電話番号、機種名、所属での表示端末の絞込みが可能です。

※Comp端末の場合は、同じ端末名で「Work Managed Device」と「Work Profile」の2つが表示され、それぞれの領域に対してサイレントインストール/アンインストールが行えます。また、「Work Profile 設定」画面で「Work Profile 作成時に Work Managed Device 側の管理アカウントを削除する」が有効の場合は、Comp端末の「Work Managed Device」は一覧に表示されません。

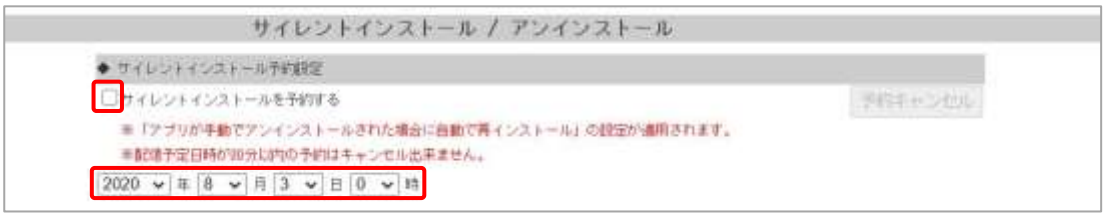
【サイレントインストール予約設定の方法】

日時を指定してサイレントインストールを行えます。

① インストールしたいアプリを選択し「端末選択画面へ」ボタンをクリックします。
（複数選択可）

② 「サイレントインストールを予約する」にチェックを入れ、配信したい日時を選択します。

・3 ヵ月先まで、1 時間単位での予約が可能です。
・予約を追加する場合、他の予約との間隔を 12 時間以上あける必要があります。



③ 端末選択から配布したい端末を選択し、「インストール」をクリックします。
※CSV で指定することも可能です。詳しくは「CSV で端末を指定してサイレントインストールを行う方法」の②以降をご確認ください。

④ 予約が完了すると、予約一覧が表示されます。
正常に予約が完了できた場合、ステータスは「配信待ち」と表示されます。

・予約状況により、指定した時刻にインストールされない場合があります。
・予約から配信されたアプリは、端末側で手動アンインストールすると自動で再インストールされます。
・配信予定日時から 30 日経過したものは、予約一覧から自動的に削除されます。

■予約キャンセル

配信予約したサイレントインストールをキャンセルすることができます。

・配信開始 30 分前の予約のキャンセルはできません。

・キャンセルを行うには、インストール時と同様にアプリを指定し予約一覧画面に進む必要があります。

※アプリの指定はキャンセルには影響しません。

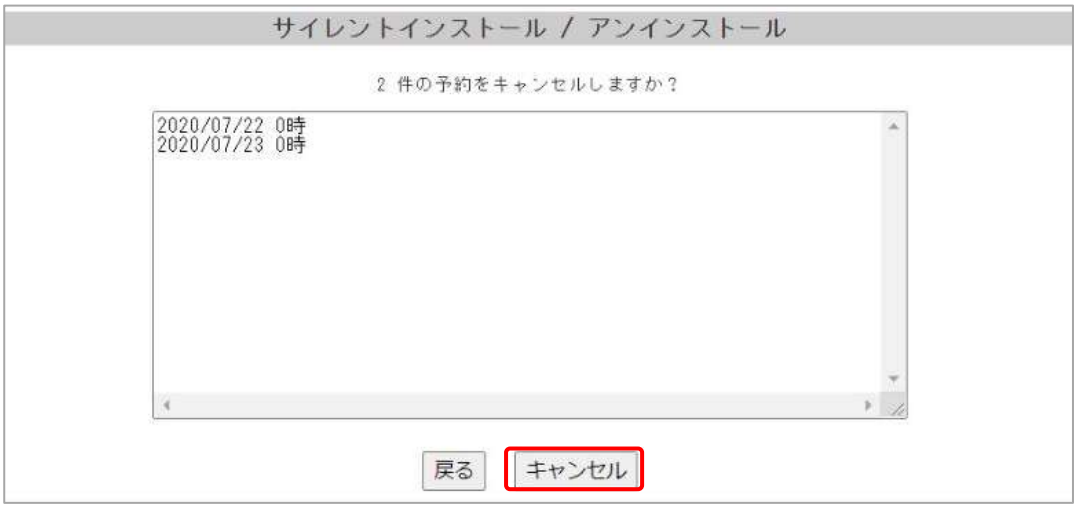
① キャンセルしたい予約を選択し、「予約キャンセル」をクリックします。

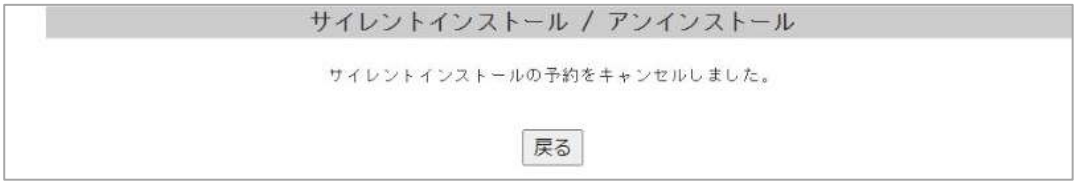
※ステータスが「配信待ち」の予約のみキャンセルすることができます。

※ステータスが「配信待ち」の場合でも、配信予定日時から 30 分以内の予約はキャンセルできません。

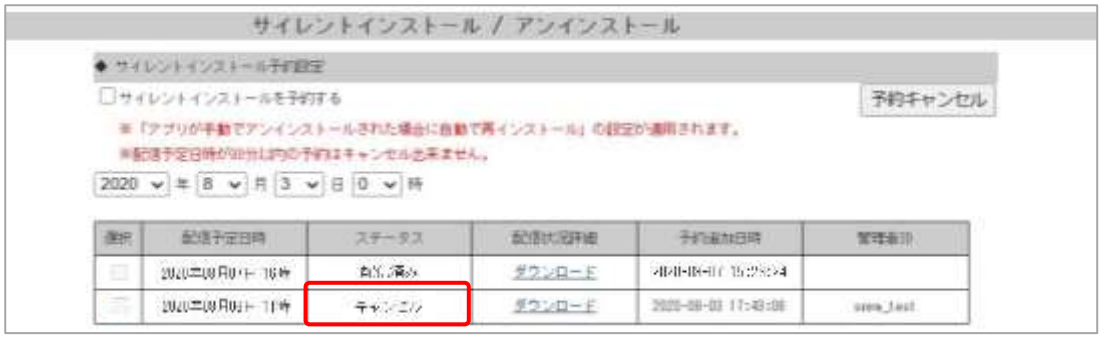
② キャンセル確認画面に選択した日時が表示されます。「キャンセル」をクリックすると、

予約のキャンセルが実行されます。





キャンセルされた予約は、ステータス欄に「キャンセル」と表示されます。



キャンセルされた予約は、30 日後に予約一覧から自動的に削除されます。

■配信状況詳細

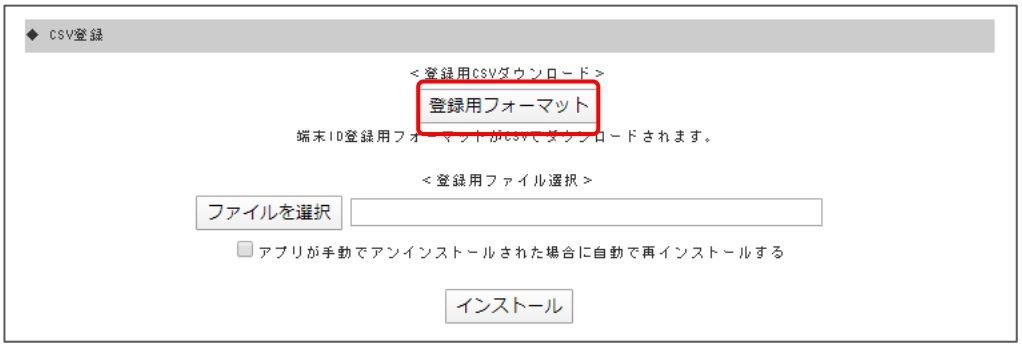
配信状況詳細のダウンロードをクリックすると CSV がダウンロードされ、現在の予約状況を確認することができます。

※予約一覧から削除された配信状況詳細の CSV ファイルをダウンロードすることはできません。

【CSV で端末を指定しサイレントインストールを行う方法】

① インストールしたいアプリを選択し「端末選択画面へ」ボタンをクリックします。(複数選択可)

② 「◆CSV 登録」の項目で登録用フォーマット(silent_install_device.csv)をダウンロードします。
※CSV 登録でもサイレントインストールの予約が可能です。「サイレントインストールを予約する」にチェックを入れてください。関連情報☞「サイレントインストールを予約する」



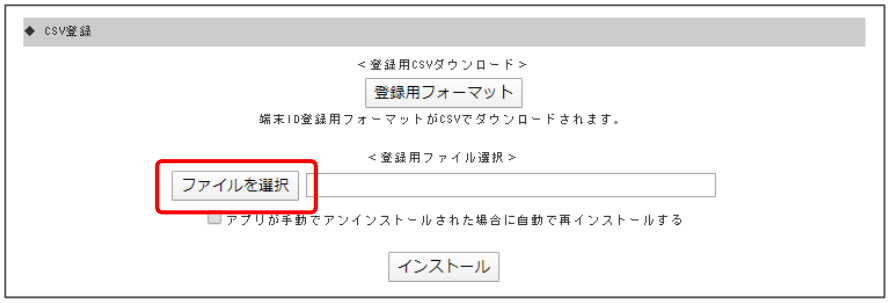
③ 対象端末の端末 ID(IMEII)を登録用フォーマットに入力し、保存します。
※ヘッダー行の「device_id」は削除しないでください

例) device_id

000000000000001

000000000000002

④ ③で作成したデータを管理画面上にアップロードします。

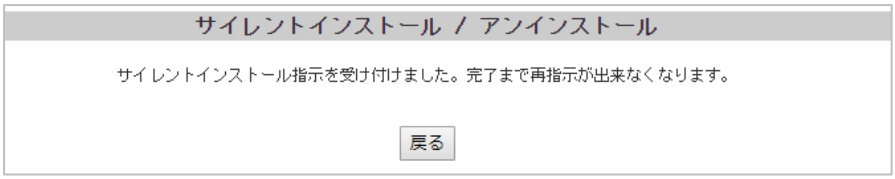


⑤ 必要に応じて**「アプリが手動でアンインストールされた場合に自動で再インストールする」**にチェックを入れます。チェックを入れてサイレントインストール指示を行うと、端末操作で該当アプリがアンインストールされた際に、自動で再インストールが行われます。

※サイレントインストール指示時にチェックを入れていない場合は、自動再インストールは実施されません。

⑥ 「インストール」ボタンを押し、インストール指示が実施されると受け付け完了画面に遷移します。

※Google サーバ側で指示が処理されるまで、次のサイレントインストールの指示を実施する事ができません。



サイレントインストールを行ったあとすぐにサイレントアンインストールの指示を行うと、
ステータスやログが正常に表示されない場合があります。半日～1日以上空けてお試しください。

CSV を利用した、Comp の WorkProfile 領域へのインストール指示は非対応です。
CSV を利用しない方法をご利用ください。

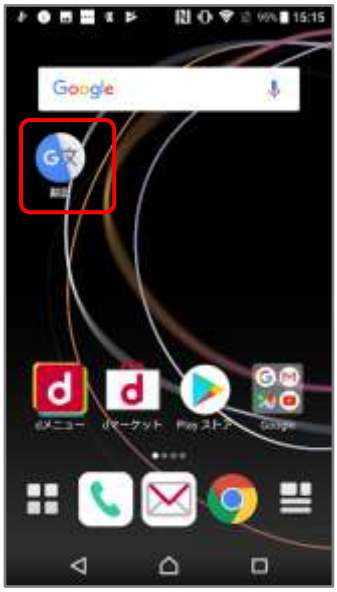
≪端末側の動き≫

■サイレントインストール

①

②

③



①サイレントインストール指示が端末に届くとインストール中の通知が表示されます。

②インストールが完了するとインストール完了の通知が表示されます。

③ホーム画面またはアプリー覧を確認するとアプリがインストールされています。

※インストール禁止設定を行っている場合、サイレントインストールを実施することはできません。

■サイレントアンインストール

①

②

①、②サイレントアンインストール指示が端末に届くと該当のアプリアイコンが削除されます。

※サイレントアンインストール時に削除完了の通知が一瞬表示されます。

※アンインストール禁止設定を行っている場合、サイレントアンインストールを実施することはできません。

≪Comp 端末の場合≫

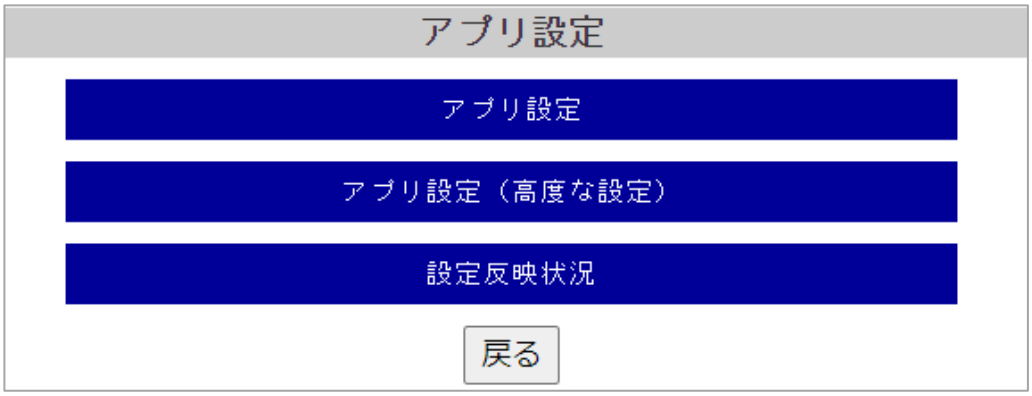
Comp 端末の場合は Work Managed Device 領域と Work Profile 領域それぞれにサイレントインストール、サイレントアンインストールが可能です。

アクセス権のない領域にはサイレントインストール/サイレントアンインストールはできません。
※端末選択画面でアクセス権のない領域の端末は表示されなくなります。

7. アプリ設定

承認アプリの権限設定や設定項目の設定値を、管理端末に適用できます。

※設定内容は Work Managed Device と Work Profile で共通しており分けることはできません。



【アプリ設定】

■ アプリ設定

承認アプリの権限設定や設定項目の設定値を、管理端末に適用できます。

■ アプリ設定（高度な設定）

「アプリ設定」では設定できない階層を持った高度な設定が行えます。ワイルドカードの利用も可能です。

※アプリによっては高度な設定のみ対応している場合があります

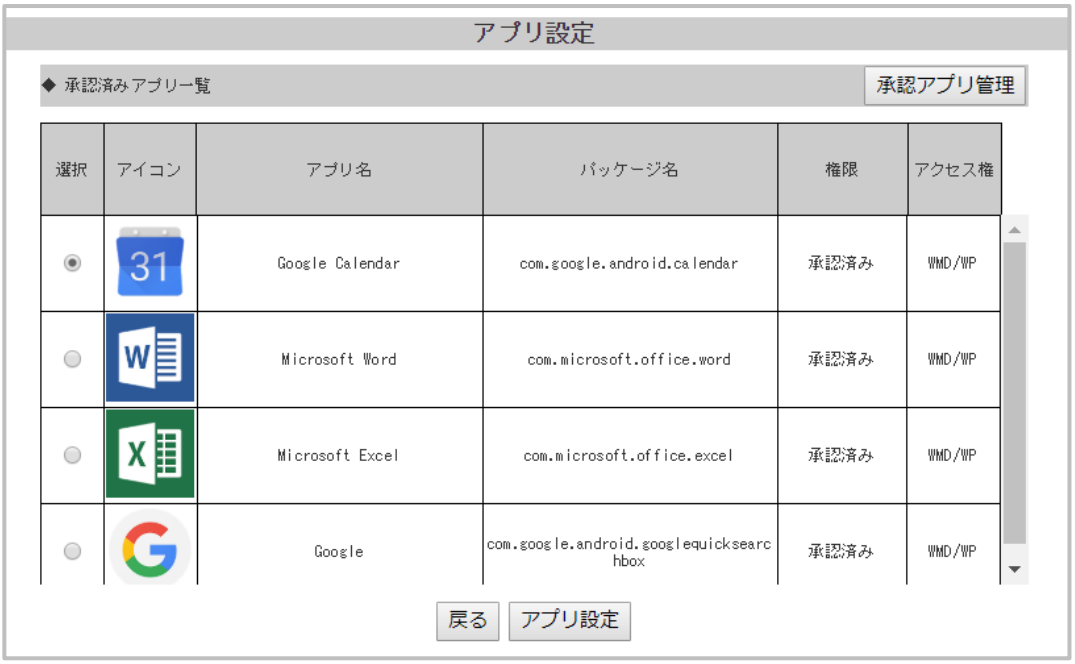
■ 設定反映状況

Android Enterprise 端末として登録されているアカウントが一覧として表示されます。

アプリ設定により設定されている情報を確認することができます。

アプリ設定

承認アプリの権限設定や設定項目の設定値を、管理端末に適用できます。



【アプリ選択】

承認アプリー覧に表示されるアプリを選択し、「アプリ設定」をクリックしてください。

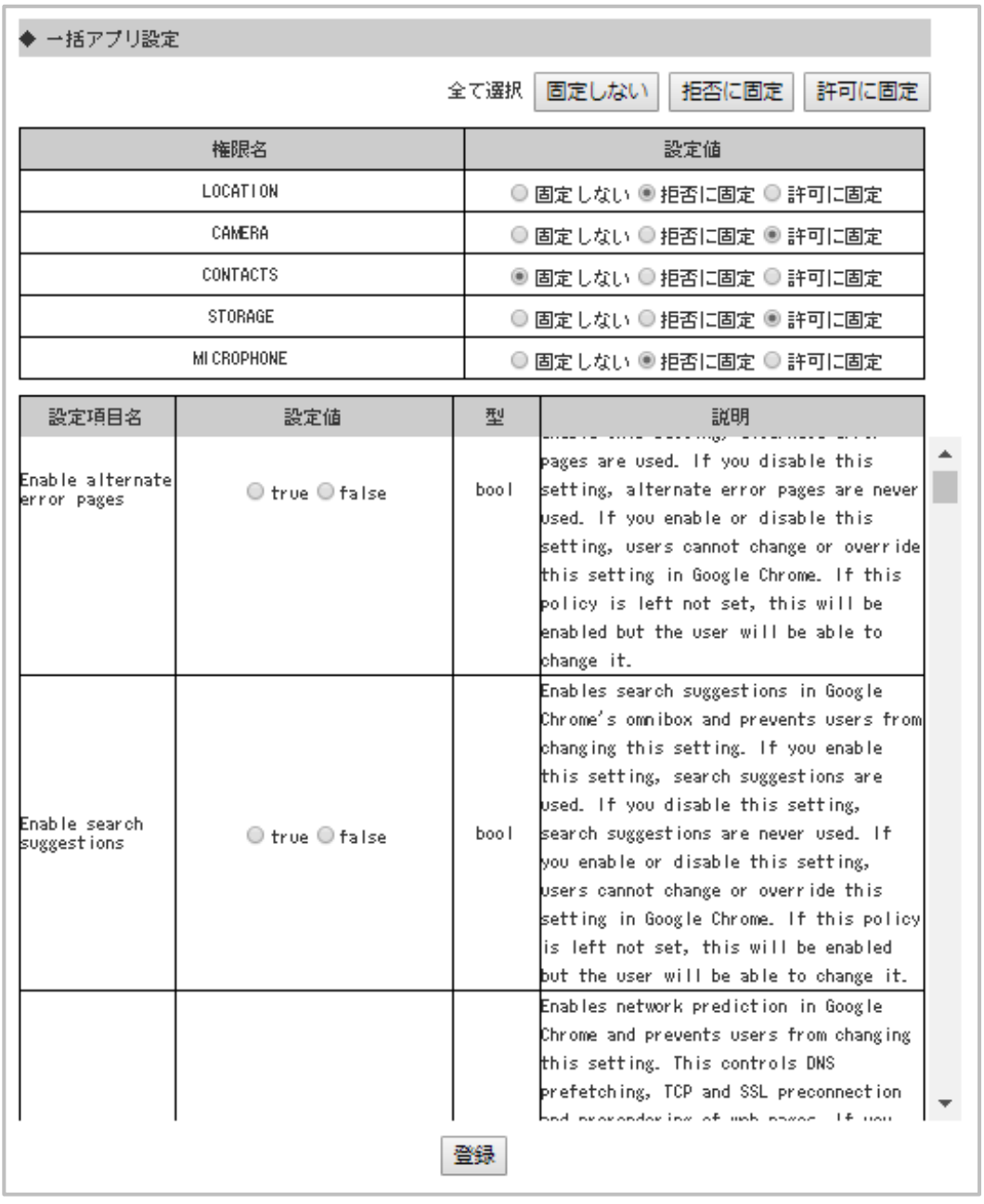
アプリの設定項目【一括アプリ設定】と【個別CSV登録】欄が読み込まれます。

【一括アプリ設定】

アプリの権限設定と各種設定項目の設定を、管理画面に登録されたAndroid Enterprise端末全台に
一括登録できます。

※一括登録した値は保存され、再度同じアプリの「アプリ設定」を開くと前回一括登録した値が表示されます。

本機能を利用する場合は、デバイス制御ポリシーの適用が必要です。



≪アプリ権限設定≫

アプリが要求する権限を「固定しない/許可に固定/拒否に固定」に設定できます。

※「全て選択」ボタンをクリックすると、表示される全ての設定値が該当項目に選択されます。

※本設定は「登録」クリック後に端末のサーバー通信により適用されます。

■**固定しない**　：アプリが必要とする権限をユーザーが自由に設定できます。

■**許可に固定**　：アプリが必要とする権限を許可に固定します。

■**拒否に固定**　：アプリが必要とする権限を拒否に固定します。

権限固定化したアプリ設定画面例

Android 11 以降の場合、「許可に固定」を適用すると「アプリに位置情報へのアクセスを許可しました」の通知が端末側に表示される場合があります。
正常な動作となりますが、通知は自動では消えないため、必要に応じて手動で削除してください。

Android 12 以降の Work Profile/Work Profile[企業所有]の場合、アプリによって「許可に固定」で以下の権限が固定されません。

カメラ、マイク、位置情報、ボディセンサー、身体活動

※通知は Android13 以降の場合のみ

Android 14 以降の場合、写真と動画の権限を「許可に固定」または「拒否に固定」すると端末設定内のアプリ権限が「許可」または「許可しない」に選択されますが、固定することができません。
※端末にて権限の操作が可能です。

≪アプリ詳細設定≫

アプリの各種設定項目を管理画面上で登録できます。
※設定項目の詳細な仕様はアプリによって異なるため、各アプリのデベロッパーにお問い合わせください。
※アプリにより設定項目に表示される言語は異なります。

例）Chromeのブックマーク編集を許可しない設定にした場合

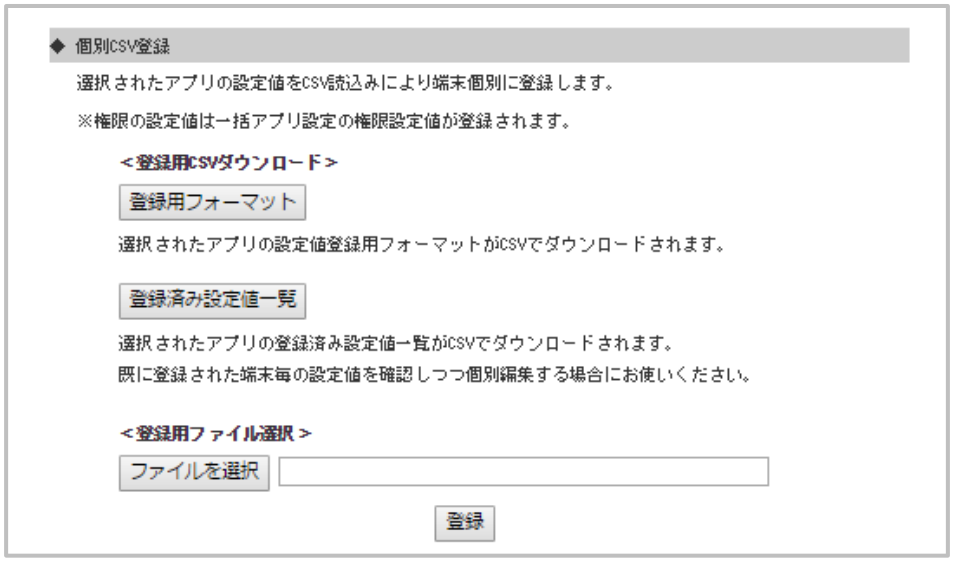
設定項目名	設定値	型	説明
Enables or disables bookmark editing	true / false	bool	Enables or disables editing bookmarks in Google Chrome. If you enable this setting, bookmarks can be added, removed or modified. This is the default also when this policy is not set. If you disable this setting, bookmarks can not be added, removed or modified. Existing bookmarks are still available.

ブックマークの編集が制限されます。

【個別 CSV 登録】

選択されたアプリの設定値を CSV 読込みにより端末個別に登録します。

※権限の設定値は一括アプリ設定欄で設定された権限設定値が登録されます。



■登録用フォーマット

「登録用フォーマット」ボタンをクリックすると、登録用のCSVフォーマットがPCにダウンロードされます。

こちらのデータを編集して端末個別のアプリ設定を行います。

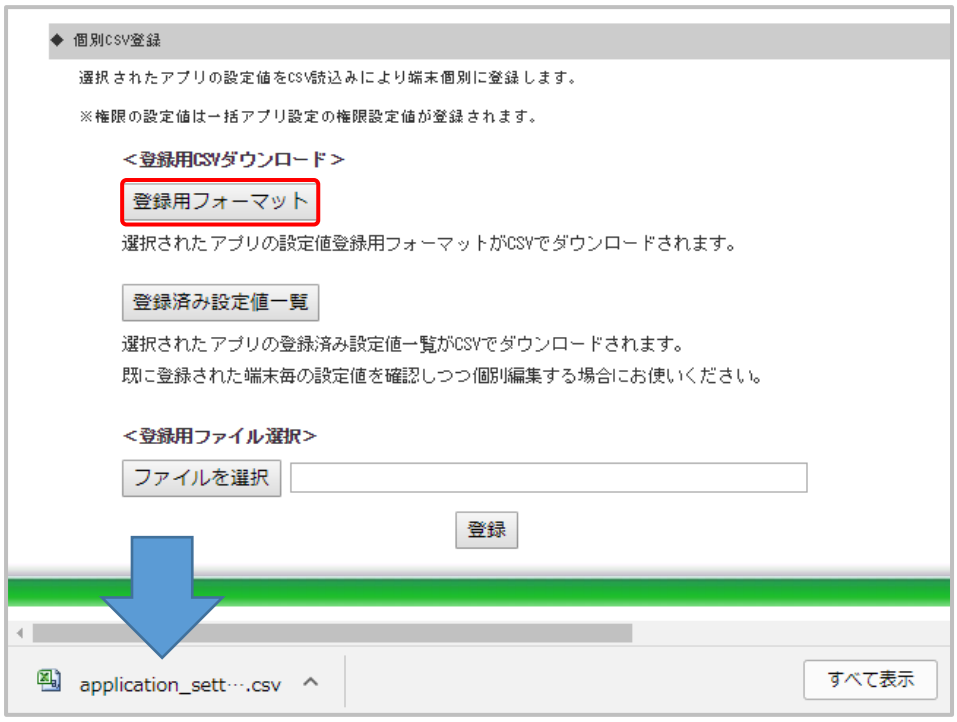
※CSVフォーマットに表示される設定項目名と管理画面に表示される設定項目名が異なる場合があります。

■登録済み設定値一覧

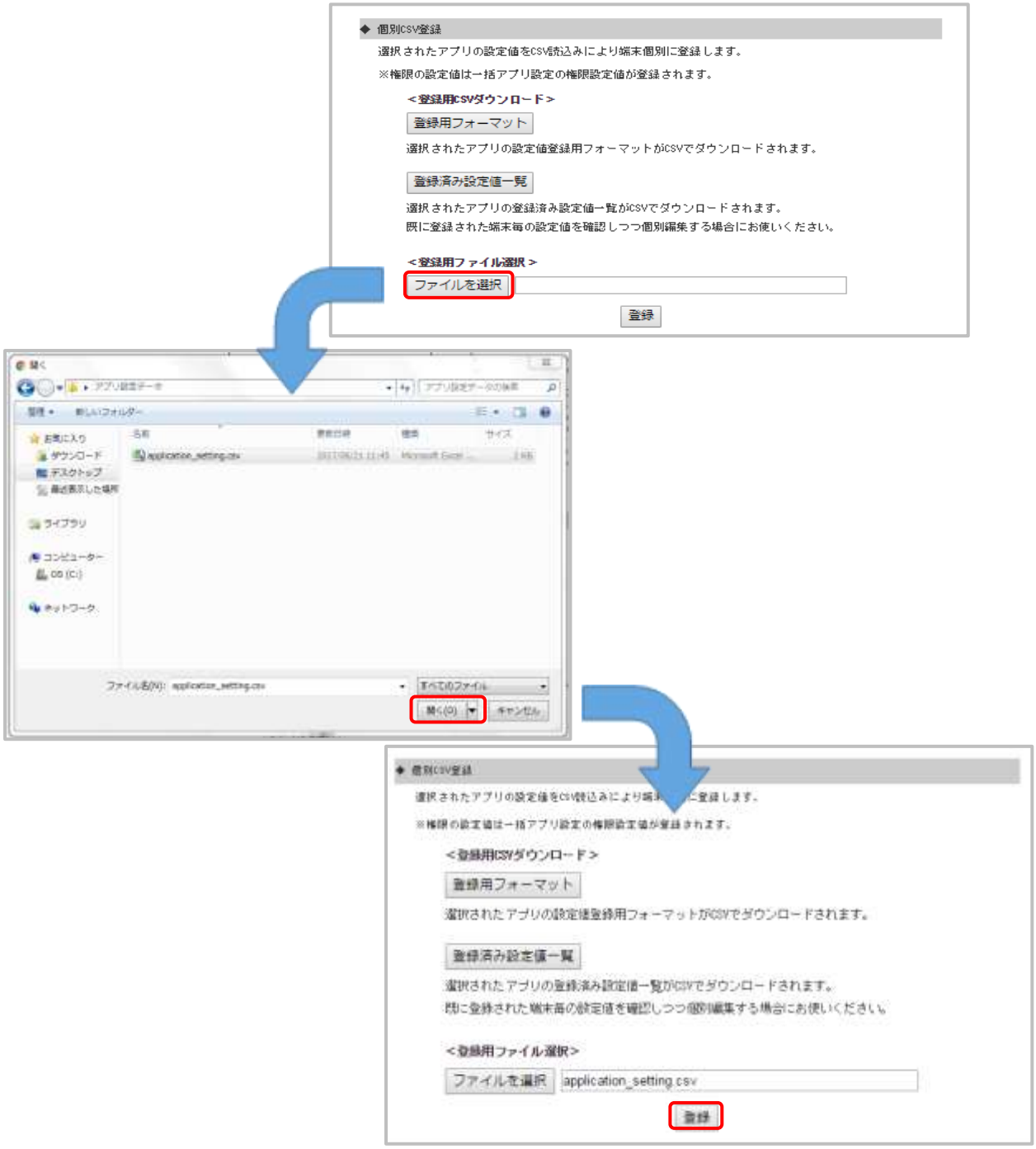
「登録済み設定値一覧」ボタンをクリックすると、登録済みの設定値データがCSV形式でダウンロードされ、端末毎の設定値が確認できます。

≪CSVによるアプリ設定方法≫

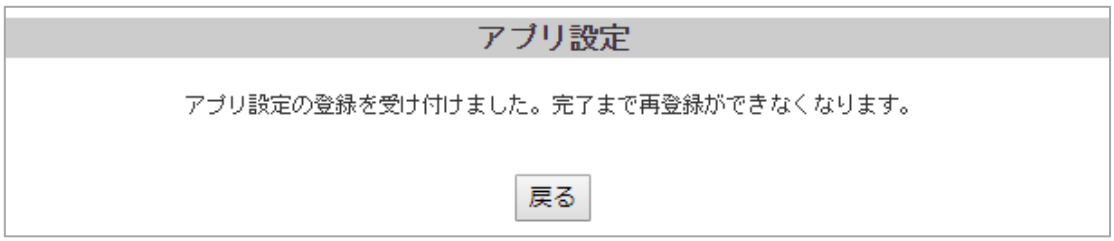
アプリを選択後、画面下の登録用フォーマットボタンをクリックし、登録用のCSVファイルをダウンロードします。



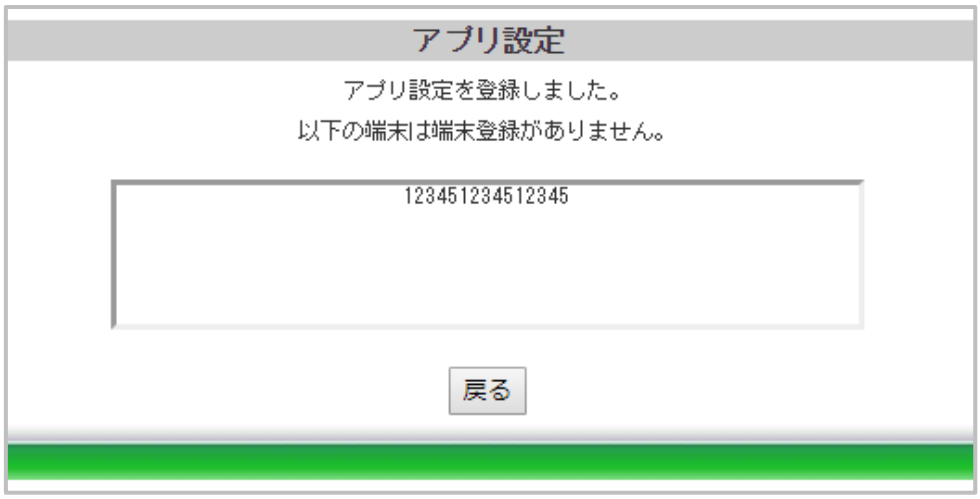
ダウンロードした CSV を編集し「ファイルを選択」でファイルをアップロードし登録を押下します。
このとき CSV の「device_id」欄に端末 ID を入力することで、任意の端末にのみ設定を行えます。



データに問題がなければ受け付け完了画面に遷移します。
※Google サーバ側で指示が処理されるまで、次のアプリ設定の指示を実施する事ができません。



存在しない端末 ID や、管理画面上に登録がない端末 ID が入力されている場合エラー画面が表示されます。



一括アプリ設定と個別 CSV 登録において、設定した項目の反映は端末に該当アプリが端末にインストールされている状態で本設定を適用したタイミングとなります。
端末に該当アプリがインストールされていない場合は、再適用が必要になります。
※アプリ権限設定については本設定を適用後に端末サーバー通信が必要です。
（定期通信、サーバー通信ボタン、ポリシー即時適用）

≪Comp 端末におけるアプリ設定≫

アプリ設定にアクセス権の有無は関係なく、Work Managed Device、Work Profile の両方の領域にアプリ設定の値が反映されますのでご注意ください。

アプリ設定（高度な設定）

【1】 アプリ選択

承認アプリー覧に表示されるアプリを選択し、「アプリ設定」をクリックしてください。

【2】 アプリ設定の作成

① 「◆アプリ設定一覧」で「新規作成」を押します

② 設定画面が別画面で開きます。設定名に任意の名称を入力した上でその他の部分の設定を入力してください。入力が完了したら「保存」を押します。

※入力項目はアプリ側で用意されている内容となり、弊社のサポート対象外となります。
不明な点はアプリの開発元にお問合せください。

③ 設定が完了すると、「◆アプリ設定一覧」に項目が追加されます。
作成した項目を編集しなおしたい場合は、選択のラジオボタンにチェックを入れ、「編集」ボタンを押すと編集が可能です。

【3】登録用ファイルを作成して登録を行う

① 対象端末やワイルドカード（変数値：$emailaddress$等）を指定するファイルを作成します。

※カンマ区切りの CSV ファイルをご用意ください

例）対象端末のみ指定する場合

```
device_id
000000000000001
000000000000002
```

例）ワイルドカードの値を指定する場合

```
device_id,$emailaddress$,$username$
000000000000001,yamada@example.com,山田太郎
000000000000002,suzuki@example.com,鈴木花子
```

② ①で作成したファイルを管理画面上で登録します。

対象の設定名のラジオボタンにチェックを入れた上でファイルをアップロードし、

「登録」ボタンを押します。

③ 設定内容は「登録」を押した後、基本的には即時で端末に反映されます。

※端末側の通信状態によっては、即時ではない場合もあります。

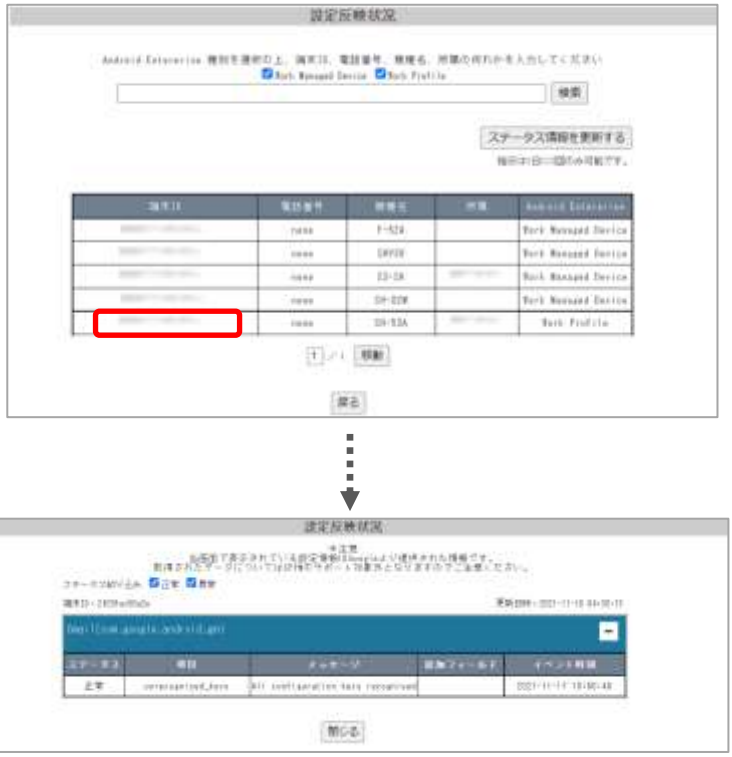
設定反映状況

アプリ設定した端末とアプリの確認が出来ます。

Android Enterprise 端末として登録されているアカウントが一覧として表示されます。

設定状況を確認したい端末の ID をクリックすると、別ウィンドウにて詳細画面が表示されます。

※アプリ設定をしていない端末の場合、設定反映状況は表示されません。



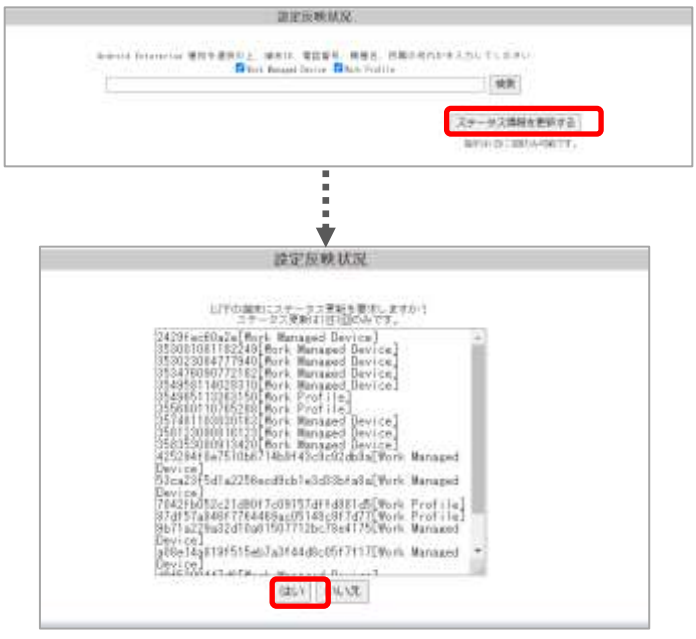
「ステータス情報を更新する」をクリックすると設定反映状況画面内の「ステータス」を

手動で更新する事が可能です。

更新を要求する確認画面が表示されるため「はい」をクリックしてください。

※「ステータス情報を更新する」ボタンによる更新は 1 日 1 回のみです。

1 度クリックすると翌日までボタンは非活性の状態となります。



8. Playストア設定

Play ストアの各種設定を行うことができます。

承認アプリ管理にてアプリを承認後、Play ストア設定にてアプリのレイアウトを設定しない場合、承認したアプリがすべて Play ストア上に表示されます。
Play ストア上に表示するアプリを制御したい場合、Play ストア設定をご利用ください。

Play ストア設定しない場合、承認したアプリが端末の Play ストア上に表示されるまで時間が掛かる場合があります。

レイアウト設定

管理対象の Android Enterprise 端末に表示される GooglePlay ストア内のレイアウトや表示アプリを設定できます。

≪レイアウト設定画面について≫

■ページ作成

「ページ作成」ボタンを押下するとページが作成されます。

■カテゴリ追加

「カテゴリ追加」ボタンを押下するとカテゴリが追加されます。

■アプリ追加

「アプリ追加」ボタンをクリックすると別ウィンドウで承認済みアプリー覧が表示されます。

承認アプリー覧で任意のアプリの「追加」ボタンをクリックするとアプリが追加されます。

端末の管理モードに関わらず、それぞれアクセス権がある領域の PlayStore にのみアプリが表示されます。これを利用し、Work Managed Device と Work Profile それぞれの PlayStore に表示するアプリを分けることが可能です。

アクセス権の設定に関しては「Comp 端末におけるアクセス権設定方法」をご確認ください。

をご確認ください。

1 ページ目には各管理モードのアクセス権を持つアプリを最低1つは追加してください。

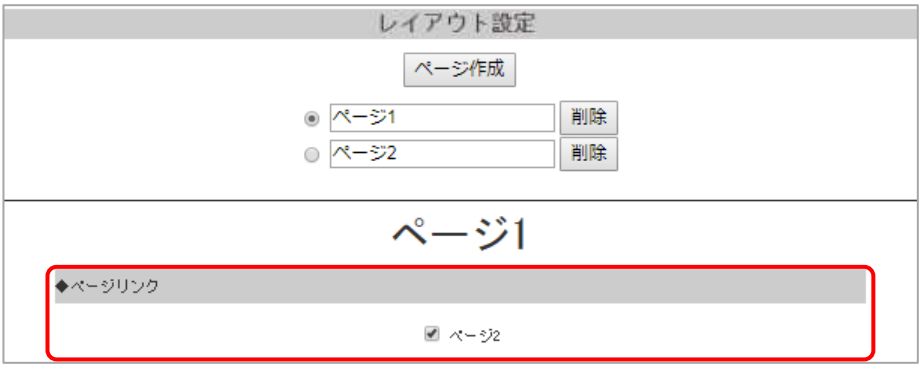
追加されていない場合は他ページへのリンクが表示されません。

■ページリンク

ページが複数ある場合、ページリンクのチェックボックスが表示されます。

ここにチェックを付けると選択したページへのリンクが作成されます。

※この画像では、「ページ 1」の中に「ページ 2」へのリンクが作成されます。



≪登録上限数≫

各項目にはOS仕様に基づき登録上限数があります。下記の上限数内に収まるよう設定してください。

- ページ数　100
- 1ページ辺りのクラスタ数　30
- 1クラスタ辺りのアプリ数　100
- 1ページ辺りのリンク数　10
- 承認アプリ数　1000

■レイアウト設定の保存

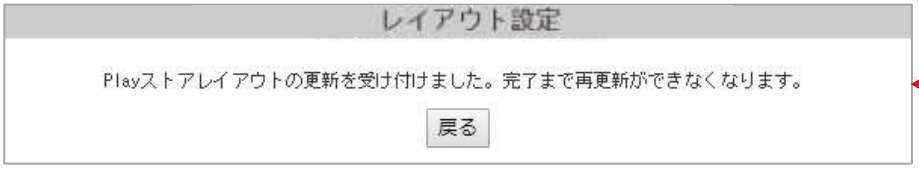
レイアウト設定が完了しましたら「保存」ボタンをクリックしてください。

※「保存」ボタンをクリック後、画面下部に読み込み中のインジケーターが表示されている状態でPC上での画面遷移や端末上でのPlayStoreのキャッシュ削除を行うと正常に反映されない場合がございます。

レイアウトの保存が受け付けられ端末への適用処理が開始されます。

※端末台数が多い場合は処理に時間がかかる場合があります。

※保存処理中はレイアウト設定画面を操作できません。



≪端末のPlayStoreの表示について≫

■ページ

PlayStoreレイアウト設定で設定したレイアウトでアプリが表示されます。

※ページが１つのみの場合、ページ名は表示されません。

※ページが複数設定されている場合、ページリンクがないと他のページに移動できません。

関連情報☞「■ページリンク」

ページ名あり（複数ページ作成）

ページ名なし（1ページのみ作成）

■カテゴリ

カテゴリが複数設定されている場合、カテゴリ名が表示されカテゴリごとに分類されて表示されます。

※カテゴリが１つのみの場合、カテゴリ名は表示されません。

➤カテゴリが複数ある場合

➤カテゴリが１つのみの場合

カテゴリ内のアプリが表示しきれない場合はアプリ表示部分を左にスワイプするか、カテゴリ名右側の「もっと見る」をタップしてカテゴリページへ移動してアプリを確認できます。

➤アプリ表示部分をスワイプ

➤カテゴリ名横の「もっと見る」をタップ

■アプリ

アプリをタップするとインストール、アンインストール、アプリの更新が可能です。

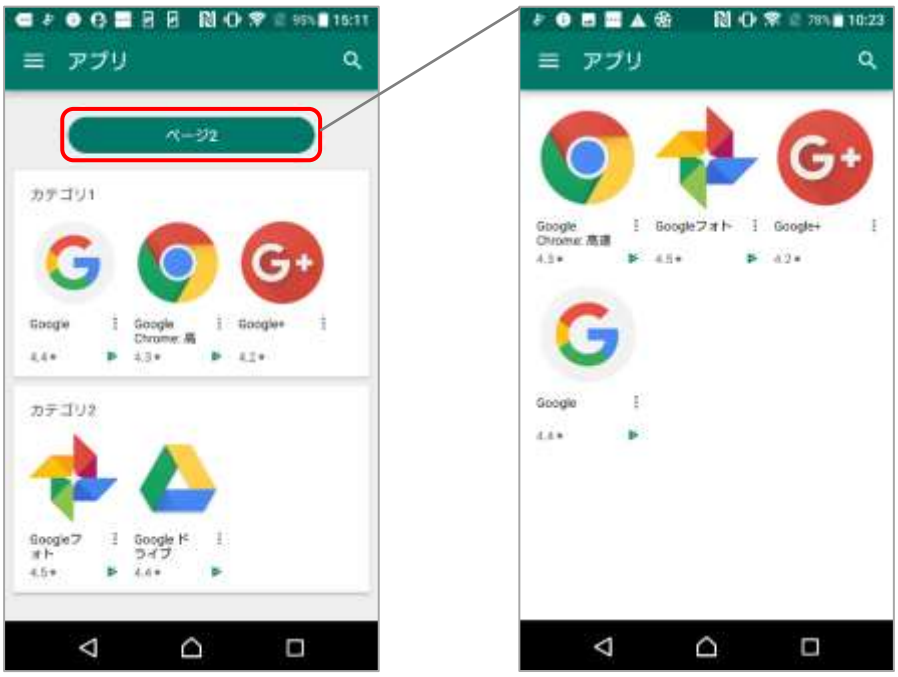
※使用方法は通常の PlayStore と同様です。

■ページリンク

ページ上部に表示されているページリンクをタップすると該当のページに遷移します。

※レイアウト設定でページリンクにチェックを入れていないと表示されません。

関連情報☞「■ページリンク」



ページリンクが複数あり表示しきれない場合はページリンク部分を左にスワイプすることですべてのページリンクを確認することができます。

➤アプリ表示部分をスワイプ

個人領域のアプリ表示設定（Work Profile[企業所有]のみ）

Work Profle[企業所有]でキッティングした端末の「個人領域上の GooglePlay ストア」に表示するアプリを制限できます。

※GooglePlay ストアには、サーバー通信や定期通信のタイミングで反映されます。

■無効にする

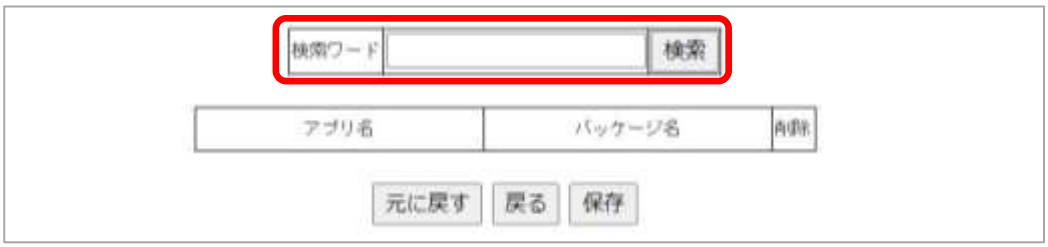
個人領域のアプリ表示設定が無効になります。保存したアプリは Play ストアに影響されません。

■有効にする

・Play ストアに一覧のアプリを表示させない（ブラックリスト制御）
　保存したアプリが Play ストア上で非表示になります。
・Play ストアに一覧のアプリのみを表示させる（ホワイトリスト制御）
　保存したアプリのみ Play ストア上に表示されます。

【設定手順】

検索ワードを入力し「検索」ボタンをクリックすると、アプリ追加画面が別ウィンドウで表示されます。

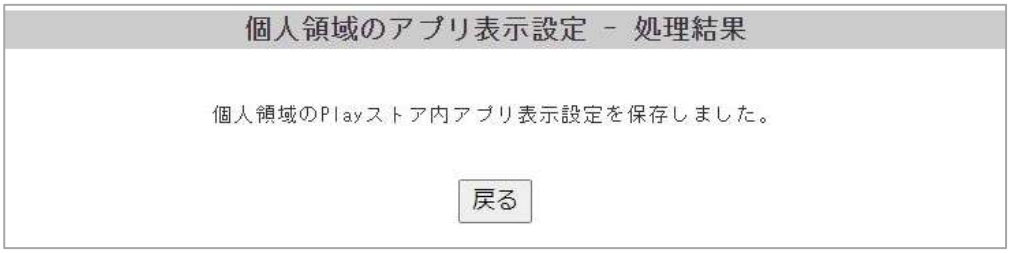


対象のアプリの「追加」ボタンをクリックしてください。

アプリ追加画面のウィンドウを閉じると、追加したアプリが表示されます。

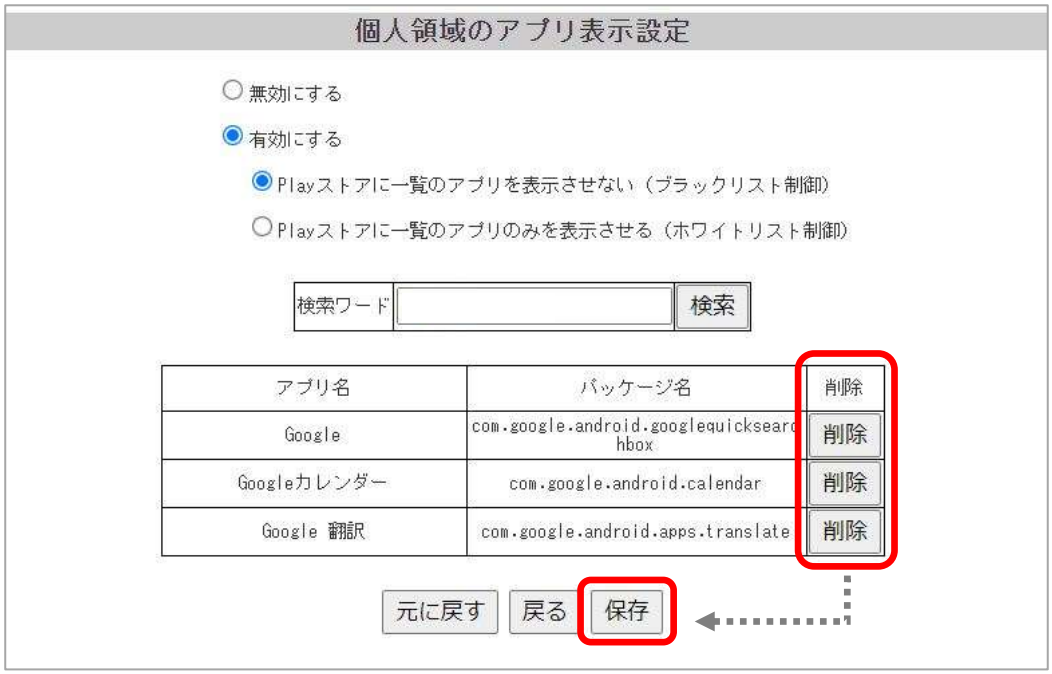
「保存」をクリックしたら登録完了です。

※管理画面に追加できるアプリの数に上限はありません。



【削除手順】

登録したアプリを削除したい場合は、「削除」ボタンをクリックして保存してください。



【表示例】

・ブラックリスト制御適用時（一覧に Google を追加）

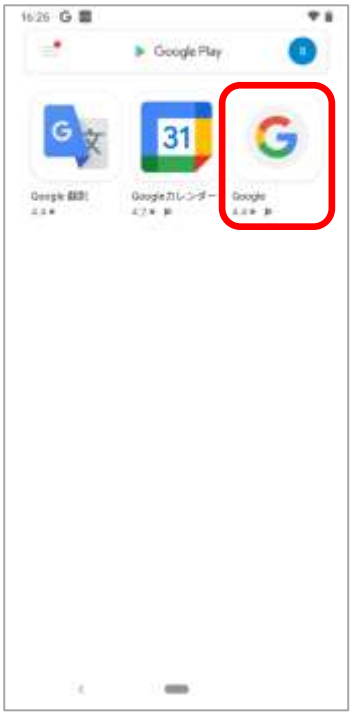
ブラックリスト制御前

Google が非表示になる

ブラックリスト制御後

・ホワイトリスト制御適用時（一覧に Google を追加）

※ホワイトリスト制御をした際、管理画面のアプリ一覧の順番と PlayStore の順番が異なる場合があります。



9. 証明書管理

端末への証明書の配布管理や EAP Wi-Fi の設定登録管理が行えます。

【配布】

証明書配布

管理対象の Android Enterprise 端末に証明書を配布・インストールすることができます。

EAP Wi-Fi 設定登録

管理対象の Android Enterprise 端末に Wi-Fi 証明書の配布・インストールと Wi-Fi の設定を登録することで、EAP Wi-Fi への接続設定を適用できます。

【管理】

配布証明書管理

「証明書配布」と「EAP Wi-Fi 設定登録」で配布した証明書を一覧表示し、各端末の配布状況を確認できます。また、配布した証明書の削除を指示できます。

EAP Wi-Fi 設定管理

「EAP Wi-Fi 設定登録」で登録した Wi-Fi 設定を一覧表示し、各端末への適用状況を確認できます。

証明書配布

管理対象の Android Enterprise 端末に証明書を配布・インストールすることができます。
SPPM Agent v3.32～：ユーザー証明書（PKCS#12 形式）対応
SPPM Agent v3.40～：CA 証明書（PEM/DER 形式）対応、アプリ指定証明書紐付け対応

管理画面に登録されている Android Enterprise 端末に証明書を配布する場合、管理画面上で証明書入りの Zip ファイルをアップロードしてからサーバと端末間で通信を行ってください。

【アップロードファイルについて】

下記ファイルを Zip ファイルに圧縮してください。
・証明書ファイル
　ユーザー証明書：PKCS#12 形式（拡張子例：.p12 / .pfx）
　CA 証明書：PEM/DER 形式（拡張子例：.pem / .der / .crt / .cer）
・配信端末指定用 CSV ファイル
※画面上部の「CSV ファイルフォーマット ダウンロード」ボタンからフォーマットをダウンロードできます。
※Zip・CSV・証明書ファイルのファイル名は半角英数字と一部記号(「-」「_」「.」)のみ対応しています。また、記号はファイル名先頭には使用できません。
※証明書のファイル名は拡張子を含めて 64 文字以内に設定してください。
※Zip ファイルのサイズ上限は 30MB です。

CSV ファイル形式 ：device_id,file_name,pass,cert_type,tagged_type,package_name
device_id(端末 ID),file_name(証明書のファイル名),pass(ユーザー証明書のパスワード),
cert_type(証明書の種類　1:ユーザー証明書、2:CA 証明書),
tagged_type(証明書の紐づけ先　空欄：関連無し、1：特定のアプリ),
package_name(証明書紐づけ先アプリのパッケージ名　空欄 or アプリパッケージ名)

例）
device_id,file_name,pass,cert_type,tagged_type,package_name
000000000000001,user_certificate_1.p12,password_1,1,,
000000000000002,ca_certificate_2.pem,,2,,
000000000000003,app_certificate_3,password_3,1,1,package_name

※CSV ファイルには上記例のようにヘッダーを指定してください。
※項目を未入力にしたい場合はカンマの間に何も入力しないでください。
※証明書を配布する端末には、パスワード・パターン・数字 PIN のいずれかが設定されている必要があります。

【証明書 zip ファイルアップロード方法】

証明書配布画面の「ファイルを選択」ボタンをクリックしファイル選択画面を開きます。

配布したい証明書が入った Zip ファイルを選択してください。

「保存」ボタンを押下すると証明書がアップロードされます。

※「保存」ボタンをクリックした時点では証明書は端末に配布されません。

サーバと端末間で通信を行ったタイミングで端末に配信されます。

証明書を配布する端末には、パスワード・パターン・数字 PIN のいずれかが設定されている必要があります。パスワードが設定されていない端末に配布を行った場合はインストール失敗となるためご注意ください。

また、インストール済みの証明書は端末パスワードを「スワイプ」または「なし」に変更すると削除されます。

※OS10 以降、端末パスワードの設定がなくても配布が可能です。

また、インストール済みの証明書は端末パスワードを「スワイプ」または「なし」に変更しても削除されません。

【端末上で証明書配布状況を確認する方法】

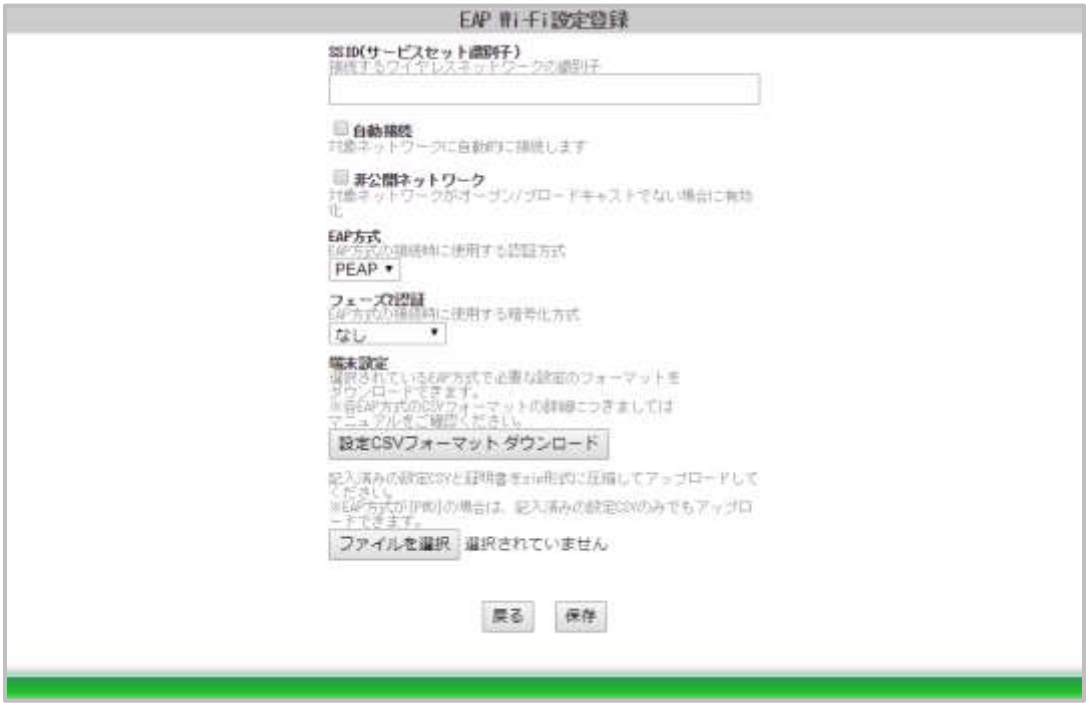
「端末設定>ロックとセキュリティ>認証情報ストレージの項目のユーザ認証情報」を確認すると配布した証明書を確認できます。

EAP Wi-Fi設定登録

管理対象の Android Enterprise 端末に Wi-Fi 証明書の配布・インストールと Wi-Fi の設定を登録することで、EAP Wi-Fi への接続設定を適用できます。

※SPPM Agent v3.40 以降対応

※Android 14 以降では、利用できません。



■SSID（サービスセット識別子）

Wi-Fi アクセスポイントの SSID を入力します。

■自動接続

対象の Wi-Fi アクセスポイントを端末が検知した際、自動接続させるにはチェックを入れます。

■非公開ネットワーク

対象の Wi-Fi アクセスポイントが非公開アクセスポイントの場合、チェックを入れます。

■EAP 方式

EAP 方式の接続時に使用する認証方式を選択します。

■フェーズ 2 認証

EAP 方式の接続時に使用する暗号化方式を選択します。

※選択した EAP 方式によっては設定が不要な場合があります。

■端末設定

「設定 CSV フォーマットダウンロード」ボタンから、

選択した EAP 方式に合わせた配信端末指定用 CSV フォーマットをダウンロードできます。

証明書ファイルと配信端末指定用 CSV ファイルを Zip ファイルに圧縮しアップロードします。

【アップロードファイルについて】

下記ファイルを Zip ファイルに圧縮してください。

・証明書ファイル

ユーザー証明書：PKCS#12 形式（拡張子例：.p12 / .pfx）

CA 証明書：PEM/DER 形式（拡張子例：.pem / .der / .crt / .cer）

・配信端末指定用 CSV ファイル

※画面上部の「CSV ファイルフォーマット ダウンロード」ボタンからフォーマットをダウンロードできます。

※Zip・CSV・証明書ファイルのファイル名は半角英数字と一部記号(「-」「_」「.」)のみ対応しています。また、記号はファイル名先頭には使用できません。

※証明書のファイル名は拡張子を含めて 64 文字以内に設定してください。

※Zip ファイルのサイズ上限は 30MB です。

≪EAP 方式別 CSV フォーマット表≫

EAP 方式	配信端末指定用 CSV 項目				
PEAP	device_id	ca_cert_name	wifi_id	wifi_anonymous_id	wifi_password
TLS	device_id	ca_cert_name	user_cert_name	user_cert_password	wifi_id
TTLS	device_id	ca_cert_name	wifi_id	wifi_anonymous_id	wifi_password
PWD	device_id	wifi_id	wifi_password		

【Android 11 以降で証明書配布状況を確認する方法】

「端末設定>セキュリティ>詳細設定>暗号化と認証情報>ユーザー認証情報」を確認すると、
配布した証明書を確認できます。

Android 11 以降は、ユーザー証明書とCA証明書を配布すると「ユーザー認証情報」にCA証明書も表示される場合があります。

※画像はPixel4aの画面です。

配布証明書管理

「証明書配布」「EAP Wi-Fi 設定登録」で配布した証明書のインストール状況の確認や、証明書の削除を指示できます。

≪項目一覧≫

文言	説明
全端末から削除	チェックボックスをオンにして「削除」ボタンを押すと、対象の証明書がインストールされた端末全てに削除指示を出します。 ※削除指示は即時適用ではなく次回サーバー通信時に適用されます。 ※EAP Wi-Fi 設定登録で配布した証明書へ削除指示は行えません。
証明書名	アップロードした証明書のファイル名が表示されます。
エイリアス	証明書のエイリアス（端末での表示名）が表示されます。 同じ名前の証明書がアップロードされた場合は「_1」「_2」…のように識別番号が付与されます。
種別	「ユーザー証明書」または「CA 証明書」が表示されます。
配布指定端末	配布指定した端末の台数が表示されます。
Wi-Fi 設定	EAP Wi-Fi 設定登録により配布されている証明書は「○」が表示されます。
利用アプリのパッケージ名	証明書紐づけ先アプリのパッケージ名が表示されます。

※「証明書名」「エイリアス」「配布指定端末」から各証明書の「証明書配布一覧画面」を開けます。

【配布_証明書一覧】

現在配布中の証明書一覧が表示されます。

【全端末から削除指示中_証明書一覧】

「全端末から削除」を選択し、削除指示が出されている証明書一覧が表示されます。

※端末個別に削除指示を出している証明書は表示されません。

※全ての端末から削除が完了すると、一覧の証明書は表示されなくなります。

■証明書配布一覧画面

証明書配布対象としている端末毎のインストール状況を一覧で確認できます。

「選択」のチェックボックスをオンにして「削除」ボタンを押すと、端末個別に削除指示を出せます。

また、端末個別のインストール状況は端末情報画面からも確認可能です。

≪端末情報画面≫

≪インストール状況一覧≫

文言	説明
通信待ち	証明書アップロード後に端末との通信を待機しています。
ダウンロード中	証明書ファイルをダウンロード中です。
ダウンロード完了	証明書ファイルのダウンロードが完了しました。
ダウンロード失敗	証明書ファイルのダウンロードが失敗しました。
インストール完了	証明書ファイルのインストールが完了しました。
インストール失敗	証明書ファイルのインストールが失敗しました。
圧縮ファイル解凍失敗	端末で圧縮ファイルの解凍に失敗しました。
エラー発生	エラーが発生しました。

※ 証明書配布に失敗した場合は、サーバ通信時にリトライ処理が行われます（最大5回）

※「EAP Wi-Fi 設定登録機能」による証明書配布はリトライ処理対象外です。

※「更新日時」にインストール状況が更新された日時が表示されます。

EAP Wi-Fi設定管理

「EAP Wi-Fi 設定登録」で登録した EAP Wi-Fi 設定状況の確認や削除を指示できます。

■検索欄

端末 ID、SSID の何れかを入力して「検索」が可能です。

■全ページ選択

チェックを入れると、全台または検索結果の該当端末全てをページを跨いで削除対象に指定できます。

≪項目一覧≫

文言	説明
選択	チェックをオンにして「削除」ボタンを押すと、削除を指示できます。 ※設定完了している端末に対してのみ指示できます。
SSID	設定した EAP Wi-Fi の SSID が表示されます。
端末 ID	設定登録した端末の端末 ID が表示されます。
電話番号	設定登録した端末の電話番号が表示されます。
機種名	設定登録した端末の機種名が表示されます。
設定適用状況	設定登録した端末の設定適用状況に応じて下記文言が表示されます。 ・設定指示中(通信待ち) ・設定完了 ・設定失敗 ・削除指示中(通信待ち) ・削除失敗
更新日時	設定適用状況を更新した日時が表示されます。

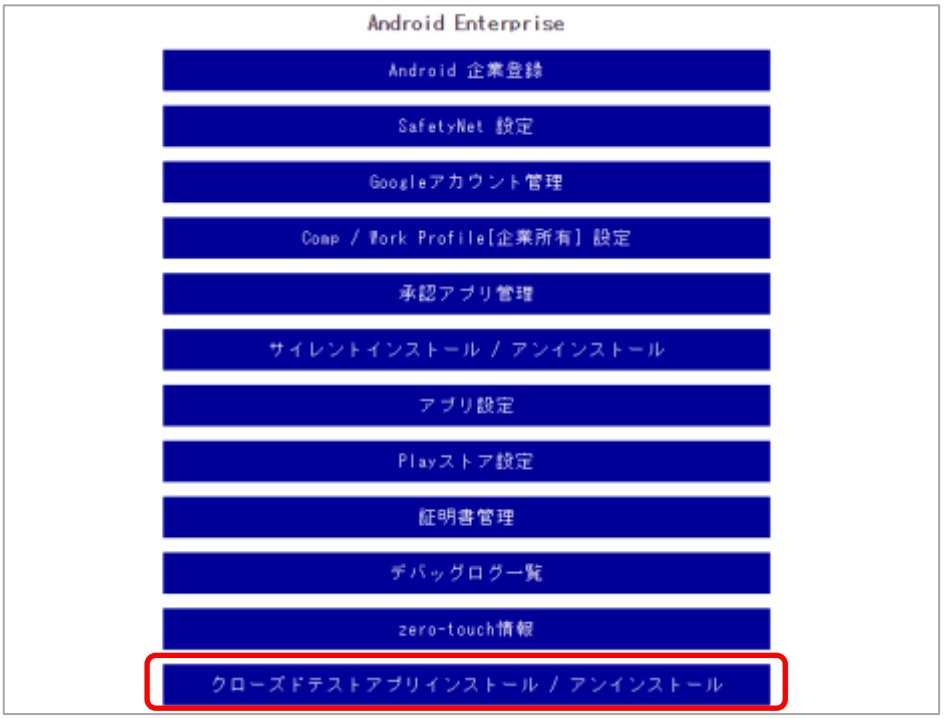
※EAP Wi-Fi 設定に対して削除指示を行い削除が完了すると、端末からは EAP Wi-Fi に使用されていた証明書も合わせて削除されます。

※本画面では EAP Wi-Fi 設定登録による証明書の配布状況は確認できません。

Android12 の場合、削除指示を実施すると管理画面に「削除失敗」と表示されます。
※実際に削除されたかの確認は「端末設定＞セキュリティ＞詳細設定＞暗号化と認証情報＞ユーザー認証情報」をご確認ください。
※SPPM Agent v3.63 以降で回避可能です。

クローズドテストアプリインストール / アンインストール

GooglePlayConsole で設定したクローズドテストアプリのインストール/アンインストールを行えます。



【クローズドテストアプリ　インストール/アンインストール手順】

任意のアプリパッケージ名を「パッケージ名」の欄に入力し、「検索」をクリックします。

検索結果から該当のアプリを選択し「端末選択画面へ」ボタンをクリックします。

端末一覧が表示されます。端末を選択し「インストール」ボタンを押下すると端末に
該当アプリがインストールされます。

※アプリをアンインストールする場合は、端末を選択し「アンインストール」ボタンを押下してください。

10. 連携アプリ設定

AndroidEnterprise の機能を利用することで他アプリとの連携が実現できます。

LINE WORKS 連携設定

ワークスモバイルジャパン株式会社のビジネスチャットアプリ「LINE WORKS」と連携を行えます。
「LINE WORKS」の管理者画面から発行したコードを承認アプリのLINE WORKSのアプリ設定項目で入力し登録を行うとSTAR-MDMの管理アプリとして端末へ配布した「LINE WORKS」アプリでのみログインが可能となります。
※承認アプリで承認されたLINE WORKSでのみログインが可能です。
関連情報☞「アプリ設定」

【LINE WORKS連携手順】

【LINE WORKS管理者画面】

管理者画面>セキュリティ>モバイルセキュリティ>デバイス管理(MDM)

外部MDM連携を「有効にする」にチェックを付け「Key Value」の値をコピーし「保存」してください。

【STAR-MDM 管理画面】

管理者画面>その他>アプリ設定でLINE WORKSのアプリ設定画面を開きます。

「Key Value」の値をSTAR-MDM管理画面のアプリ設定でLINE WORKSの設定項目に入力し「登録」してください。

登録が完了するとLINE WORKSにログインが可能です。

※端末一覧画面の「LINE WORKS」欄には連携状態は表示されません。

（iOS の LINE　WORKS 連携状況が表示されます。）

※登録の前にLINEWORKSが端末にインストールされている必要があります。

ChromeアプリのURLアクセス制限

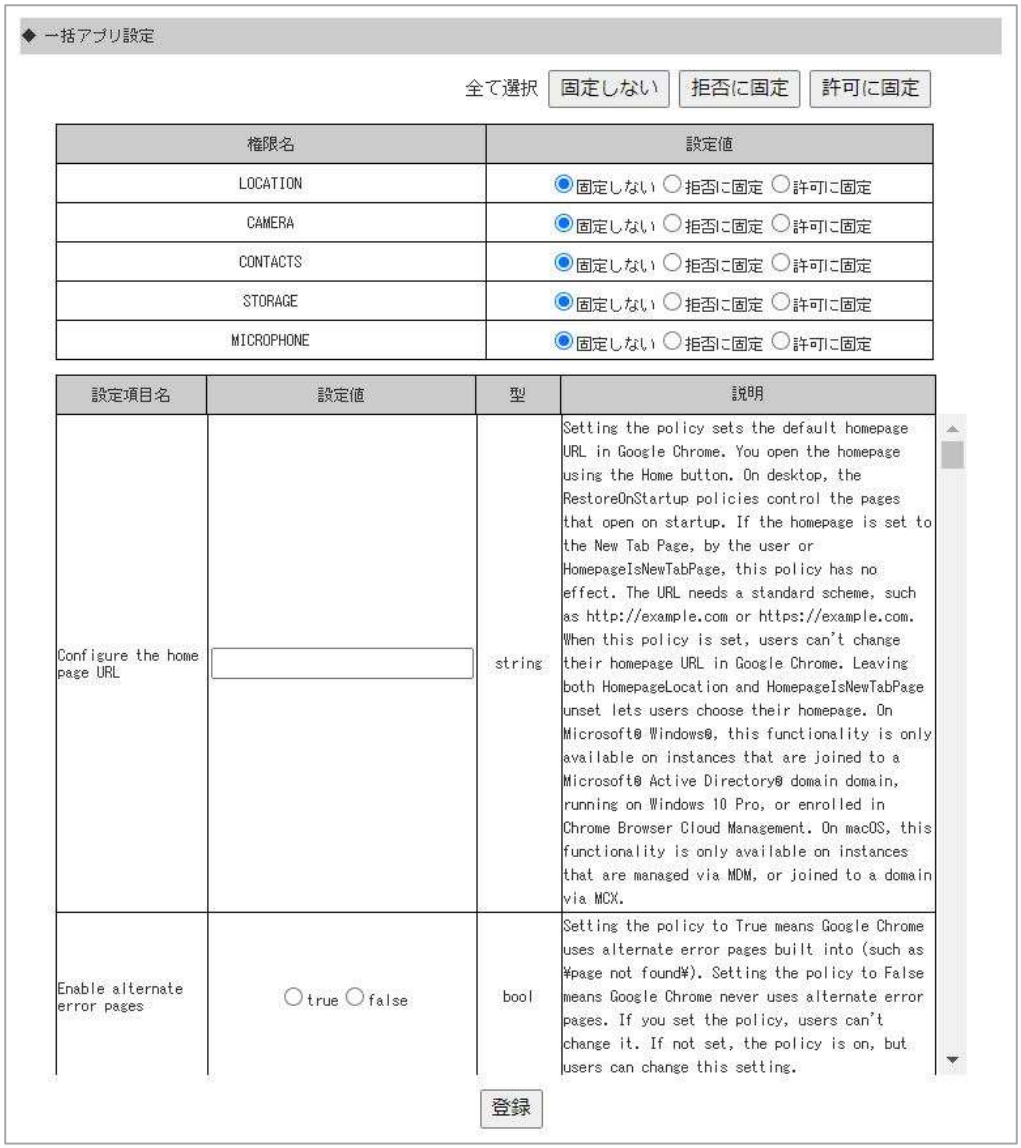
アプリ設定機能を利用し、Chromeアプリのアクセス先をブラックリスト形式・ホワイトリスト形式で
制限することができます。
※Chromeでアプリ設定機能を利用するためには、承認アプリ管理でChromeを承認する必要があります。
関連情報☞「アプリ設定」**※承認アプリ**

【ChromeのURLアクセス制限方法】

アプリ設定の以下の設定項目でURLを指定することによりアクセス制限が可能です。

≪Chromeアプリ設定項目≫

「Block access to a list of URLs」⇒禁止するURLを指定します。
「Allow access to a list of URLs」⇒禁止されたURLの中で例外として許可するURLを指定します。
「Managed Bookmarks」⇒ブックマークを設定することができます。
「Configure the home page URL」⇒ホームページURLを設定することができます。



≪代表的なご利用例≫

■ブラックリスト制限(一部のサイトのみ禁止する場合)

https://www.yahoo.co.jp と https://www.google.com を制限する場合

設定項目名	設定値
Block access to a list of URLs	["https://www.yahoo.co.jp"," https://www.google.com "]

■ホワイトリスト制限(一部のサイトのみ許可する場合)

https://www.yahoo.co.jp と https://www.google.com のみ許可し、それ以外のサイトを禁止する場合

設定項目名	設定値
Block access to a list of URLs	["*"]
Allow access to a list of URLs	["https://www.yahoo.co.jp"," https://www.google.com"]

■その他　設定例

・HTTPSのアクセスのみ許可する

設定項目名	設定値
Block access to a list of URLs	["*"]
Allow access to a list of URLs	["https://*"]

・特定サイト内の一部コンテンツのみ許可する場合(例:YouTubeの場合)

設定項目名	設定値
Block access to a list of URLs	["youtube.com"]
Allow access to a list of URLs	["youtube.com/URL名①","youtube.com/URL名②"]

▼制限方法の詳細についてはこちらをご確認ください。

https://www.chromium.org/administrators/url-blacklist-filter-format

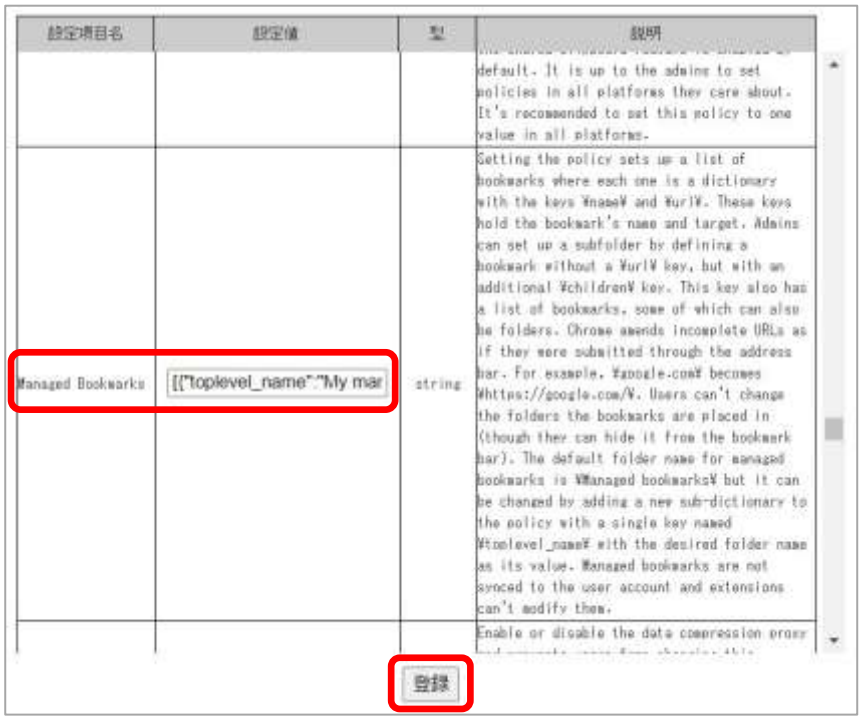
【ブックマーク設定方法（Managed Bookmarks）】

アプリ設定の以下の設定項目でChromeのブックマークの設定が可能です。

「Managed Bookmarks」の設定値に、下記を参考に入力して登録してください。

例

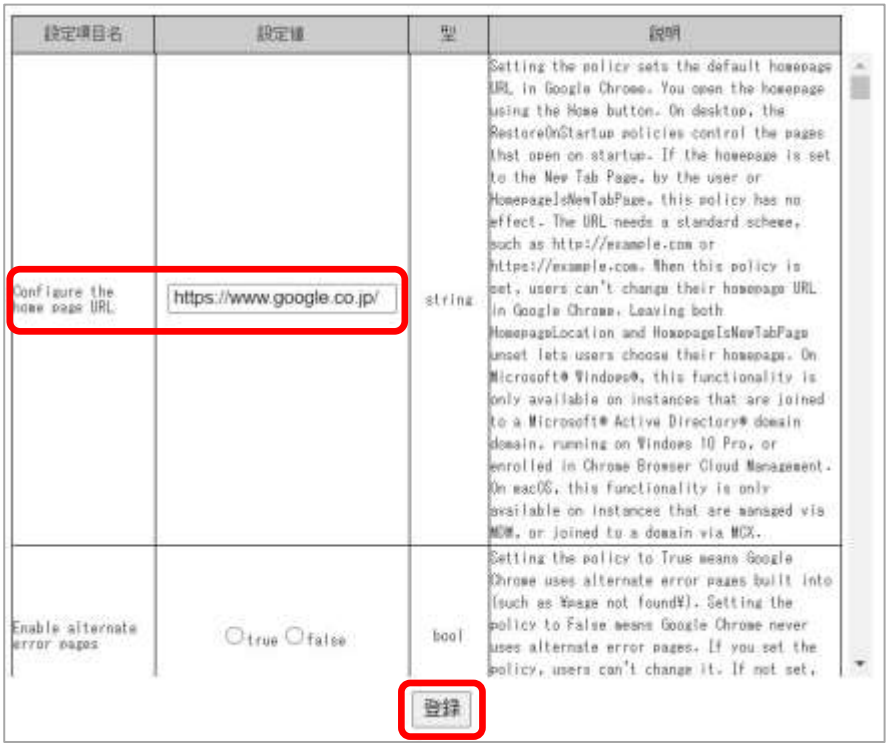
[{"toplevel_name":"任意のフォルダ名"},{"url":"https://www.starnet.co.jp/（URL）","name":"スターネット株式会社（表示名）"},{"url":"https://www.yahoo.co.jp/（URL）","name":"YHOO! JAPAN（表示名）"}]



【ホームページURL設定方法（Configure the home page URL）】

Chrome アプリ内のホームボタンをタップした際に、表示されるホームページ URL を設定することができます。

「Configure the home page URL」の設定値に、設定したい URL を入力して登録します。



Lookout 連携設定

Lookout 社のモバイルセキュリティサービス「Lookout」と連携を行えます。Lookout 連携機能を利用することで、Lookout が検知した脅威を STAR-MDM 管理画面上やメール通知で確認することができます。

Lookout 連携の動作環境や設定手順の詳細については 弊社までお問い合わせください。

11. ログ管理について

各操作によりログ管理に操作ログが表示されます。

■Android 企業登録
管理者[管理者名]が Android 企業登録を実施しました。
管理者[管理者名]が Android 企業登録を削除しました。

■サイレントインストール/アンインストール（該当端末の電話番号表示）
アプリ[アプリ名]のサイレントインストールを指示しました。[端末 ID:]
アプリ[アプリ名]のサイレントアンインストールを指示しました。[端末 ID:]
アプリ[アプリ名]のサイレントアンインストールに失敗しました。 [端末 ID:]
アプリ[アプリ名]のサイレントインストールに失敗しました。 [端末 ID:]
管理者[<管理者 ID>]がサイレントインストールの指示を[<予約時間>]に予約しました。
管理者[<管理者 ID>]が[<予約時間>]のサイレントインストールの予約をキャンセルしました。

※端末毎にログが表示されます。
※サイレントインストール/アンインストールの成功ログは表示されません。実際にインストールされているかの確認は端末を直接確認していただくか、アプリ一覧ポリシーによる端末アプリ一覧の確認が必要です。
※インストール失敗のログが表示された場合は、配信アプリの再承認が必要である可能性があります。
承認アプリのバージョンアップによる権限追加の有無は 1 日 1 回チェックされますが、チェック前は管理画面に要再承認のメッセージが表示されないため、そのまま配信操作を行え、その結果失敗となります。成功させるには翌日承認アプリ管理画面に表示された再承認ボタンを押すか、「GooglePlay を開く」から直接該当のアプリの承認ボタンを押して、再度配信を試みてください。

■アプリ設定
管理者[管理者名]がアプリ[アプリ名]の設定を一括登録しました。
管理者[管理者名]がアプリ[アプリ名]の設定を個別登録しました。

■Comp(Work Profile)関連
Work Profile が作成されました。
Work Profile がユーザーによって削除されました。
サーバ指示により Work Profile が削除されました。
Work Profile が ON になりました。
Work Profile が OFF になりました。

※その他、Work Profile（仕事領域）の SPPM で作成されたログは最後尾に（WP）と表示されます。

6 ご利用時の注意点

■端末の注意事項

・端末登録時に端末に追加される「Google 管理者アカウント」または「管理アカウント」を削除してしまうと、Android Enterprise のサイレントインストール/アンインストール、アプリ設定、PlayStore レイアウト設定機能が使用できなくなります。一度削除してしまうと再設定には端末初期化し再キッティングが必要となるため、必要なアカウントを登録後はデバイス制御ポリシーで「アカウントの追加・削除」の制限設定を推奨します。

・マルチユーザー機能は常時制限されています。

・開発者向けオプション内「OEM ロック解除を有効にする」は常時制限されています。

・E-SDK / E-API 機能との併用は非対応です。

【Android Enterprise 利用時における E-SDK/E-API 非対応項目一覧】

- 緊急時ポリシー：E-SDK「端末ロック中に機内モード解除」
- デバイス制御ポリシー：E-SDK/E-API 全項目
- 位置情報取得ポリシー：E-SDK「位置情報取得終了後に GPS 機能 OFF 機能」
- アプリ配信ポリシー・Agent 管理ポリシー：E-SDK/E-API 「サイレントインストール」
- 利用アプリ制限：E-SDK/E-API 「apk の展開の許可設定」「制限アプリ無効化」（AndroidEnterprise 仕様のアプリ無効化に切り替わります。）
- 端末暗号義務化ポリシー：E-SDK/E-API 「外部メモリの暗号義務化」

・利用アプリ制限でアプリ制限/制限解除時にアプリ一覧ポリシーによりアプリ変更が検知されます。

アプリ制限時⇒「削除」

アプリ制限解除時⇒「追加」

※上記の理由から、アプリ一覧ポリシーによるアプリ変更検知のメール送信機能は非対応です。

・端末初期設定の QR コード読み取り時、NFC 通信時に「エラー この端末は出荷時設定へのリセット保護によりロックされています。IT 部門にお問い合わせください。」と表示される場合があります。これは端末初期化前の Google アカウントにより端末がロックされた状態です。

この場合は通常の初期設定手順を進め、Google アカウント入力画面で前回初期化前に登録していた Google アカウントでログインしてください。ログイン後、バックキーで初期設定画面トップに戻り、QR コードと NFC 通信を正常にお使い頂けます。

・機種によっては制御が正しく動作しない場合がございます。STAR-MDM 管理画面から管理者様へのお知らせをご確認頂くか、弊社までお問合せ下さい。

・Android Enterprise 利用中は SPPM Agent をアンインストールできません。

・アンインストールが可能なプリインアプリは初期設定時に削除されます。

・プリインアプリのバージョンアップデートを行うには承認アプリに追加されいてる必要があります。

■管理画面の注意事項

・Android Enterprise 端末では「アンインストール有効化」指示は非対応です。一旦 Android Enterprise として設定した端末を STAR-MDM の管理下から外し通常端末として利用するには、端末の初期化が必要です。

・「ライセンスキーリセット」を実施する際は、端末の初期化を行ってから実施してください。端末初期化せずに「ライセンスキーリセット」を実施した場合は、端末のサーバー通信時に STAR-MDM の監視下から外れます。ただし、Android Enterprise により制御された一部の端末機能は制限されたままになる場合があります。

※ユーザーによる端末初期化の制御は STAR-MDM の監視下から外れた際に解除されます。

・GooglePlay for Work https://play.google.com/work/ で承認/非承認操作を行うと、STAR-MDM の画面と差異

がでるため、GooglePlay for Work での操作は非推奨です。
・承認アプリのバージョンアップによる権限追加の有無は 1 日 1 回チェックされます。
このとき、チェックが実施される前では追加権限承認前アプリの「サイレントインストール」や「アプリ設定」等の操作が可能となります。その場合は、サイレントインストールは失敗となり（失敗ログ表示あり）、アプリ設定は実際のアプリに反映されません（失敗ログ表示なし）。
・企業登録削除後に再登録する場合は、少し時間をおいてから企業再登録を実施してください。
（Google 社側での登録情報の削除処理にタイムラグがある為です。）
・GooglePlay for Work との承認アプリの同期は現在非対応です。元々GooglePlay for Work で承認アプリをご利用中だった場合や、一度削除した企業登録は、再度登録すると以前承認していたアプリは承認アプリとして管理画面に表示されません。一度、管理画面の「GooglePlay を開く」から各アプリの「非承認」⇒「承認」の操作が必要となります。
・デバイス制御ポリシーで「アプリのアンインストール」を制限したままサイレントアンインストールを実施すると、通知覧にアプリ削除に関する通知が表示され続ける場合があります。また、通知に詳細はメールで送信される旨の文章が記載されている場合がありますが、そのような動作は発生しません。
・G Suite アカウント/Google 管理者アカウントでの企業登録では、Google 管理コンソールまたは STAR-MDM 管理画面の Google アカウント管理機能を利用し追加した管理対象アカウントを、各端末の STAR-MDM 登録時に追加してお使い頂く必要があります。
・管理画面に「http://」でアクセスしている場合は Google 関連ページが表示されない場合があります。
「https:// 」でアクセスし直してください。
・「Play ストア」を利用アプリ制限で制限している状態ではサイレントインストール/アンインストールとアプリ設定の機能はご利用いただけません。