KDDI Smart Mobile Safety Manager
Android Enterprise連携方式の選択と注意点について

KDDI株式会社

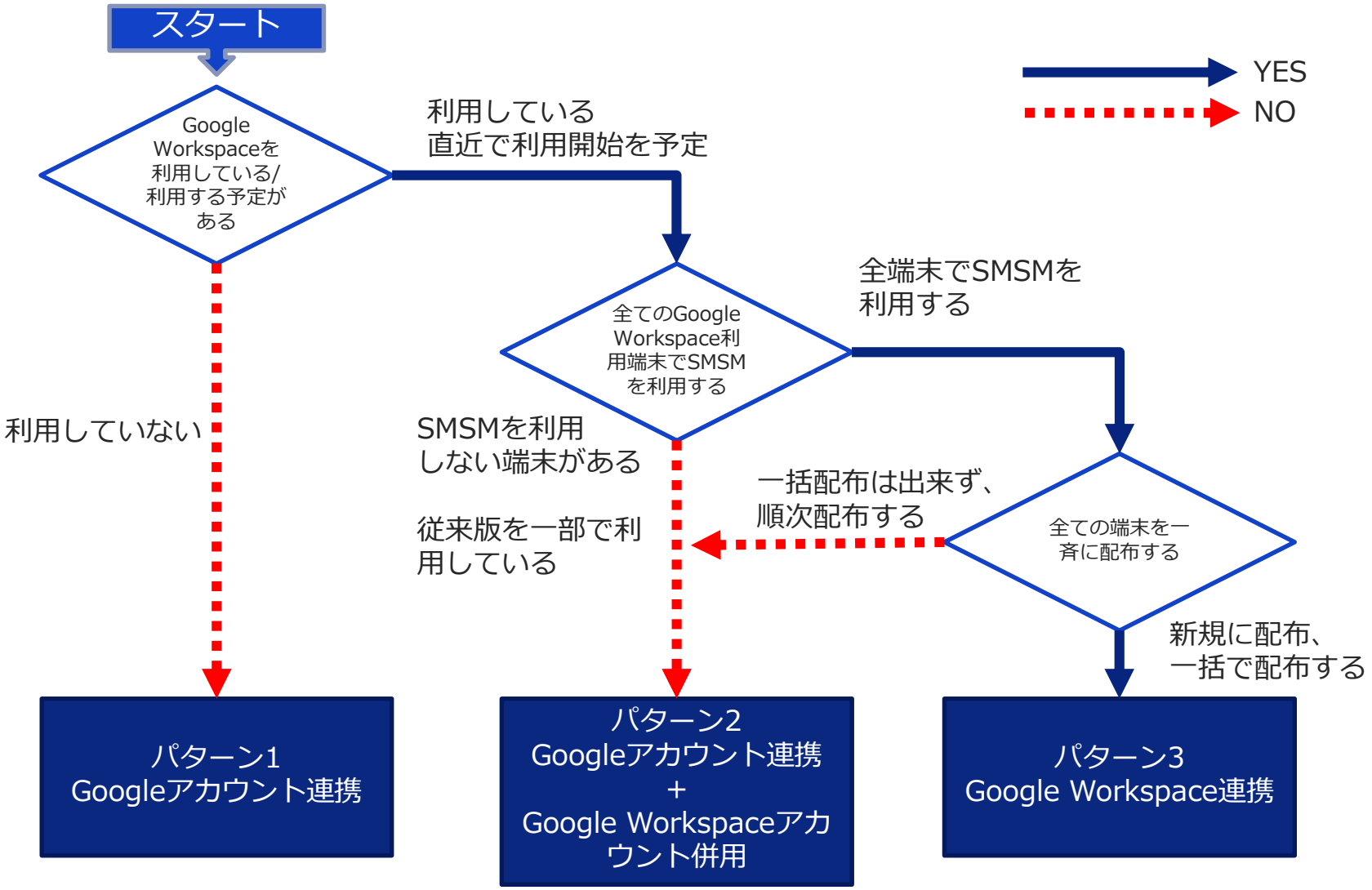
2022年 9 月 29 日

Tomorrow, Together
KDDI

本資料について

本資料は、KDDI Smart Mobile Safety Managerを利用し、Android端末の管理に必要なAndroid Enterpriseの連携方式について、複数ある連携パターンの中で、お客さまの利用状況から最適なパターンとその連携パターンでの注意事項を記載します。

連携方式選択フローチャート



連携パターン1：Googleアカウント連携

Android Enterprise連携設定は、**管理者用のGoogleアカウント**を用意してGoogleアカウント連携を実施してください。

Android Enterprise事前設定マニュアル：
https://www.optim.co.jp/promotion/smsm/pdf/AndroidEnterprise_Preconfiguration.pdf

- Managed Google Playの設定は、各端末にSMSMが配布するManaged Google Playアカウント(管理アカウント)に適用されます。

(注意事項)

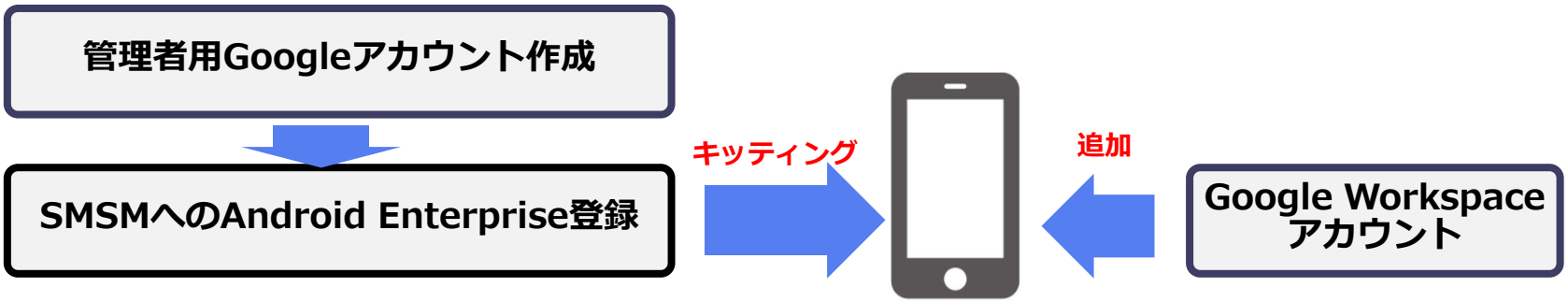
－SMSMの設定にて「アカウント制限」を「制限しない」とした場合、端末へ私的なGoogleアカウント追加が可能となり、業務に不要なGoogle Play上のアプリをインストールすることが可能となります。

【推奨設定】

－SMSMの設定にて、「アカウント制限」を「制限する」に設定した運用を推奨します。

連携パターン2：Googleアカウント連携＋Google Workspaceアカウント併用

Android Enterprise連携設定は、**管理者用のGoogleアカウント**を用意してGoogleアカウント連携を実施してください。
その後、ご利用中の**Google Workspaceアカウントを端末に追加**してください。



（注意事項）

1）Google Workspace管理コンソールでの「端末管理機能」の使用禁止

Google Workspaceの端末管理機能を有効化すると、端末からGoogle Workspaceが使用できなくなったり、場合によっては　端末の初期化が必要となるケースがあります。

2）Google Workspaceアカウントの端末への追加が必要

Google Workspaceの利用を可能とするために、端末に手動でGoogle Workspaceアカウントの追加設定が必要です。この設定には、SMSMにて「アカウント制限」を「制限しない」と設定するため、端末へ私的なGoogleアカウントの追加が可能となり、業務に不要なGoogle Play上のアプリをインストールすることが可能になります。

3）追加したGoogle WorkspaceアカウントにてGoogle Play利用可能

2）にて追加したGoogle Workspaceアカウントは、SMSMが制限するManaged Google Play以外に切り替えて利用できるため、業務に不要なGoogle Play上のアプリをインストールすることが可能になります。

連携パターン2：Googleアカウント連携＋Google Workspaceアカウント併用

【推奨設定】

以下の（１）から（３）について、対応した上でご利用いただくことを推奨します。

（１）Google Workspace管理コンソールでの「端末管理機能」の無効化

SMSMからデバイス管理を可能とするために、 Google Workspaceコンソールにて「サードパーティのAndroidモバイル管理を有効にする」を「無効」に設定することを推奨します。
（参考）設定方法は下記マニュアルのP50ページをご確認ください。

Androidキッティングマニュアル：
https://www.optim.co.jp/promotion/smsm/pdf/Android_Kitting.pdf

（２）Google Workspace管理コンソールでの「ユーザ切り替え」の無効化

Google WorkspaceアカウントによるGoogle Play利用を制限するため、 Google Workspace管理コンソールにて以下の設定を行うことを推奨します。

①管理コンソールの左カラムよりデバイス → モバイルとエンドポイント → 設定 → 一般設定
を選択し、遷移先の画面で[全般]を選択。モバイル管理の設定項目が表示されるので、
そちらから「モバイル管理をオフにする（管理しない）」を選択し保存。

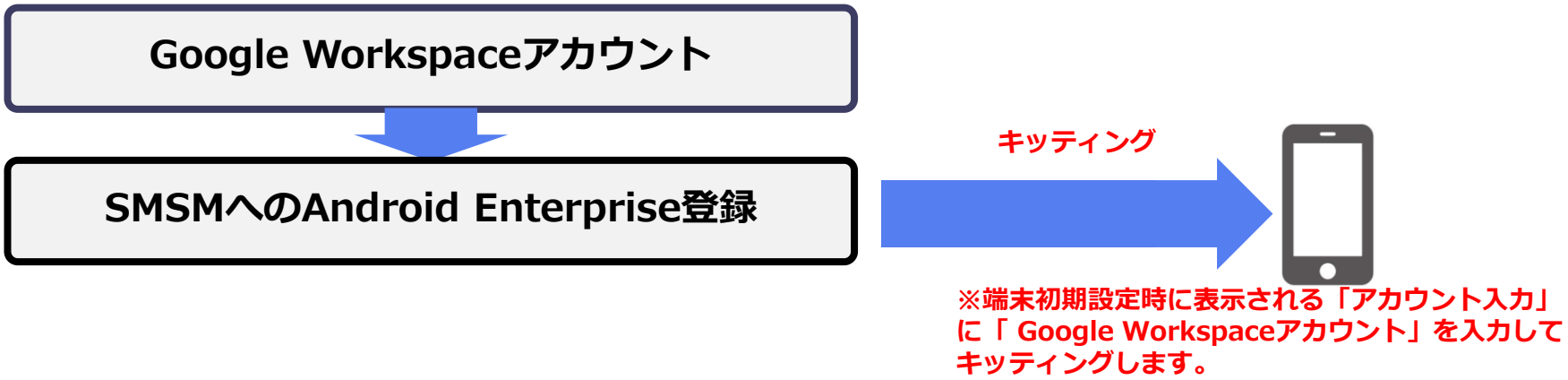
②管理コンソールの左カラムよりアプリ　→その他Googleサービス　→対象の組織を選択
する→　GooglePlayを選択し、「オフ（すべてのユーザー）」に設定する。

（３）SMSMでのアカウント制限の有効化

Google Workspaceアカウントを端末へ追加した後、私的利用のGoogleアカウント追加を制限するため、SMSMの設定にて「アカウント制限」を「制限する」へ設定します。
なお、端末設定を利用者へ任せた場合、私的利用のGoogleアカウントを設定される可能性があるため、対象端末はまとめて一か所で設定することを推奨します。

連携パターン3： Google Workspace連携

Android Enterprise連携設定は、お持ちの**Google Workspaceアカウント**を用意してGoogleアカウント連携を実施してください



Androidキッティングマニュアル　3.2 Google Workspaceアカウントを登録する場合：
https://www.optim.co.jp/promotion/smsm/pdf/Android_Kitting.pdf

（注意事項）

１）すべての利用端末は１つのSMSMにて管理

同じドメインのGoogle Workspaceを利用する端末は、すべて１つのSMSM契約にて管理します。
SMSMに加入しない端末は、SMSM管理外となりGoogle Workspaceが利用できません。
利用端末をSMSMから他のEMMへ変更する場合は、 Google Workspace －EMM間連携設定の解除と、既存端末を初期化し、他のEMMへの再キッティングが必要となります。

連携パターン3： Google Workspace連携

2）すべての利用端末はGoogle Workspace e利用が必要

Google Workspace連携の場合、すべての利用端末にてGoogle Workspaceアカウントを設定する必要があります。SMSMにて「従来版エージェント」と「ストア版エージェント」をご利用の場合、「従来版エージェント」を利用する端末はSMSM管理外となります。

【推奨設定】

（1） Google WorkspaceとSMSM「ストア版エージェント」の利用

すべての利用端末の初期設定時に、 Google Workspaceアカウントを設定し、SMSM「ストア版エージェント」のインストールします。

（2）SMSMでのアカウント制限の有効化

私的利用のGoogleアカウント追加を制限するため、SMSMの設定にて「アカウント制限」を「制限する」へ設定します。

その他注意事項

SMSMにて利用端末を管理する場合、Android Enterprise連携パターンに関わらず、以下の注意が必要です。

（1）SMSMのSecure Shieldによるアカウント削除抑止

Secure Shieldを利用しない場合、SMSMの連携している管理アカウントを削除できます。

- 管理アカウントを削除すると、以降端末でManaged Google Play機能がご利用いただけません
- 端末にインストールされているエージェントバージョンによって対処方法が異なります。
  - ■エージェントバージョンが 9.11.107.0 未満の場合
    端末を初期化後、再度キッティングしてください。
  - ■エージェントバージョンが 9.11.107.0 以上の場合
    同期を実施することで復旧されます。

SecureShield設定にてアカウント削除の制御が可能です。

※対応機種がございますのでご確認ください。

https://www.optim.co.jp/promotion/smsm/pdf/SettingSafetyManager.pdf

（2）端末へのアカウント追加にはSMSM設定変更が必要

SMSMの設定にて「アカウント制限」を「制限する」へ設定している場合、
端末へExchangeやメールなど別のアカウントを追加できません。
端末へ別アカウントを追加する場合は、一時的にSMSMの設定にて「アカウント制限」を「制限しない」へ変更する必要があります。


Tomorrow, Together
KDDI