アプリ管理

このセクションでは、アプリの可用性、インストール、アップデート、権限管理に関連するポリシーを設定
できます。

Managed Google Playアカウントは、デバイスのプロビジョニング時に自動的に作成されます。

1. Playストアモード

このモードは、 Play
ストアでユーザーが利用できるアプリと、ポリシーからアプリを削除したときのデバイス上の動作を制御し
ます。

ホワイトリスト（デフォルト）
：ポリシーにあるアプリのみが利用可能で、ポリシーにないアプリはデバイスから自動的にアンインス
トールされます。 Playストアには利用可能なアプリのみが表示されます。

ブラックリスト
：すべてのアプリが利用可能で、デバイスに置くべきでないアプリはアプリケーションポリシーで明示
的に ブロック としてマークする必要があります。 Play
ストアには、ブロックされたアプリを除くすべてのアプリが表示されます。

2. 信頼できないアプリのポリシー

デバイスで適用される、信頼できないアプリ（不明なソースのアプリ）のポリシー。このオプションは、ユ
ーザーが Playストア外からアプリをインストールできるかどうか（サイドローディング）を決定する Android のシステム設定を制御します。

禁止（デフォルト） ：デバイス全体で信頼できないアプリのインストールを禁止します。

個人プロファイルのみ
：ワークプロファイルがあるデバイスでは、デバイスの個人プロファイル内でのみ信頼できないアプリ
のインストールを許可します。

許可 ：デバイス全体で信頼できないアプリのインストールを許可します。

3. Google Play Protect

Google Play Protect

4.

5.

Android 16

6.

7.

8.

すべてのアプリに対する明示的な権限またはグループの付与、拒否。これらの値は
デフォルトの権限ポリシー 設定を上書きします。

権限ポリシーを追加 を使用してエントリを作成し、削除アクションで削除します。

各エントリには次が含まれます：

Androidの権限 /グループ ：Androidの権限またはグループ（必須）。例：
android.permission.READ_CALENDARまたは android.permission_group.CALENDAR。

ポリシー ：付与 / 拒否 / プロンプト（ デフォルトの権限ポリシー
と同じポリシーオプションを使用します）。

9. アプリケーション

ポリシーに含める必要があるアプリケーションの一覧。一覧の内容の動作は、 Playストアモード
に設定された値によって異なります。

Playストアモード がホワイトリスト
に設定されている場合、ポリシーにあるアプリのみが利用可能で、ポリシーにないアプリはデバイスから自
動的にアンインストールされます。

Playストアモード がブラックリスト
に設定されている場合、すべてのアプリが利用可能で、デバイスに置くべきでないアプリはアプリケーショ
ンポリシーで明示的に ブロック としてマークする必要があります。

新しいアプリを追加するには、 アプリケーションを追加 ボタン（または アプリケーションを追加
アイコン）をクリックし、 Managed Google Playから を選択して、 Play ストアからアプリを選び、アプリカードの 選択 ボタンをクリックします。

Google Play
で公開されていないがデバイスにすでに存在するアプリ（システムアプリやメーカー製アプリなど）を追加
するには、 アプリケーションを追加 をクリックし、
パッケージ名で追加（プリインストール済みアプリ） を選択し、アプリのパッケージ名（例：
com.example.app）を入力して 追加 をクリックします。アプリは 強制インストールのインストールタイプで追加されます。キオスクのカスタムランチャーにアプリを表示するには、
インストールタイプ をプリインストール または 強制インストール にする必要があります。 利用可能
の場合、アプリは表示されません。

Managed Google Playで利用できないアプリは、アプリケーション一覧で Android
アイコンが付きます。 Google Play
からインストールできないため、デバイスにすでに存在している必要があります。アプリがないデバ
イスにはインストールできません。

お住まいの国で Play
ストアに公開されているすべてのアプリがデフォルトで選択可能です。独自のプライベートアプリま
たは Web
アプリを選択するには、まずシステムにアップロードする必要があります。詳細については、

プライベートアプリ ページをお読みください。

各アプリは、カード内に視覚的にまとめられた独自の設定で構成できます：

9.1. インストールタイプ

アプリに対して実行するインストールの種類。

利用可能 ：アプリをインストールできます。

プリインストール ：アプリは自動的にインストールされ、ユーザーが削除できます。

強制インストール ：アプリは自動的にインストールされ、ユーザーは削除できません。

ブロック
：アプリはブロックされ、インストールできません。以前のポリシーでインストールされていた場合、アンインストールされます。

セットアップに必要
：アプリは自動的にインストールされ、ユーザーは削除できません。インストールが完了するまでセットアップは完了しません。

キオスク
：アプリはキオスクモードで自動的にインストールされます。優先ホームインテントとして設定され、ロックタスクモードのホワイトリストに登録されます。アプリがインストールされるまでデバイスのセットアップは完了しません。インストール後、ユーザーはアプリを削除できません。この
インストールタイプ は、ポリシーごとに 1 つのアプリにのみ設定できます。これがポリシーに存在する場合、ステータスバーは自動的に無効にな

ります。詳細については、専用の キオスクモード ページをお読みください。

9.2. インストールの制約

アプリのインストールに対する一連の制約を定義します。複数の制約が選択されている場合、アプリをイン
ストールするにはすべての制約を満たす必要があります。

このオプションは、 インストールタイプ がプリインストール または 強制インストール
の場合にのみ表示されます。

従量制でないネットワーク ：デバイスが従量制でないネットワーク（例： Wi‑Fi ）に接続されている場合にのみ、アプリをインストールします。

充電中 ：デバイスが充電中の場合にのみ、アプリをインストールします。

アイドル ：デバイスがアイドル状態の場合にのみ、アプリをインストールします。

9.3. 自動更新モード

アプリの自動更新モードを制御します。

デフォルト
：アプリは、ユーザーへの影響を最小限に抑えるために低い優先度で自動的に更新されます。アプリは
、次のすべての制約が満たされたときに更新されます。（ 1
）デバイスがアクティブに使用されていない、（ 2
）デバイスが従量制でないネットワークに接続されている、（ 3
）デバイスが充電中である。デバイスは、開発者による公開後 24
時間以内に新しい更新の通知を受け、その後、上記の制約が次に満たされたときにアプリが更新されま
す。

延期 ：アプリは、古くなってから最大 90日間は自動更新されません。アプリが古くなってから 90 日後、利用可能な最新バージョンが低い優先度で自動的にインストールされます（ デフォルトの自動更新モードを参照）。アプリが更新された後は、再び古くなってから 90 日が経過するまで自動更新されません。ユーザーはいつでも Play
ストアから手動でアプリを更新できます。

高優先度
：アプリはできるだけ早く更新されます。制約は適用されません。デバイスは、新しい更新が利用可能
になるとすぐに通知されます。

9.4. 最小バージョンコード

デバイスで実行されるアプリの最小バージョン。設定すると、デバイスはアプリを少なくともこのバージョ
ン コードに更新しようとします。アプリが最新でない場合、デバイスには 非準拠の詳細 が含まれ、
非準拠の理由 は APP_NOT_UPDATEDに設定されます。アプリは、この値以上のバージョン コードで Google Play に公開されている必要があります。ポリシーごとに最大 20 個のアプリで最小バージョン
コードを指定できます。

9.5. 委任されたスコープ

Android Device Policyからアプリに委任されるスコープ。他のアプリに特別な Android
権限の選択を付与できます：

証明書のインストール ：証明書のインストールと管理へのアクセスを許可します。

管理対象構成 ：管理対象構成の管理へのアクセスを許可します。

アンインストールのブロック ：アンインストールのブロックへのアクセスを許可します。

権限 ：権限ポリシーと権限の付与状態へのアクセスを許可します。

パッケージアクセス ：パッケージアクセス状態へのアクセスを許可します。

システムアプリ ：システムアプリを有効にするためのアクセスを許可します。

9.6. 優先ネットワーク

このアプリに使用する優先ネットワークサービス。設定すると、アプリは利用可能なときに指定されたエン
タープライズネットワークスライスを接続に使用します。これは、 モバイル通信 パネルの 5G ネットワークスライス構成 セクションで構成されたネットワークスライスと一致する必要があります。

9.7. デフォルトの権限ポリシー

アプリによって要求されるすべての権限に対するデフォルトポリシー。指定した場合、これはすべてのアプ
リに適用されるポリシーレベルの デフォルトの権限ポリシー
を上書きします。すべてのアプリに適用される 権限ポリシー は上書きしません。

プロンプト（デフォルト） ：権限の付与をユーザーに求めます。

付与 ：権限を自動的に付与します。

拒否 ：権限を自動的に拒否します。

9.8. ワークプロファイルと個人用アプリの接続

デバイスのワークプロファイルと個人プロファイル間で、アプリが自身と通信できるかどうかを制御します
（ユーザーの同意が必要、 Android 11以降）。

禁止（デフォルト） ：アプリがプロファイル間で通信するのを防ぎます。

許可 ：ユーザーの同意を得た後、アプリがプロファイル間で通信できるようにします。

9.9. Always On VPNロックダウンの除外

VPNが接続されておらず、 ロックダウンが有効
な場合に、アプリのネットワーク接続を許可するかどうかを指定します。 Android 10 以降を実行しているデバイスでのみサポートされます。

適用（デフォルト） ：アプリは Always On VPNロックダウン設定に従います。

除外 ：アプリは Always On VPNロックダウン設定の対象外です。

9.10. ワークプロファイルのウィジェット

ワークプロファイルにインストールされたアプリがホーム画面にウィジェットを追加できるかどうかを指定
します。

許可 ：アプリケーションはホーム画面にウィジェットを追加できます。

禁止 ：アプリケーションはホーム画面にウィジェットを追加できません。

9.11. ユーザー制御設定

特定のアプリでユーザー制御を許可するかどうかを指定します。ユーザー制御には、強制停止やアプリデー
タの消去などのユーザーアクションが含まれます（ Android 11以降）。アプリで extensionConfig が有効になっている場合、この設定に関係なくユーザー制御は禁止されます。キオスクアプリでは、 許可を使用してユーザー制御を許可できます。

未指定 ：アプリのデフォルト動作を使用して、ユーザー制御を許可するか禁止するかを決定します。

許可 ：アプリでユーザー制御が許可されます。

禁止 ：アプリでユーザー制御が禁止されます。

9.12. 無効

アプリが無効になっているかどうか。無効になっても、アプリデータは保持されます。

9.13. 認証情報プロバイダーを許可

Android 14以降でアプリが認証情報プロバイダーとして動作できるかどうか。

9.14. 管理対象構成

アプリの管理対象設定を構成するには、 管理対象構成を有効にする
ボタンをクリックします。アプリに管理対象構成がすでに設定されている場合は、 管理対象構成ボタンで構成を変更するか、 構成を削除 ボタンで削除できます。

管理対象構成 オプションは、この機能をサポートするアプリでのみ使用できます。

9.15. 権限ポリシー

アプリに対する明示的な権限の付与または拒否。これらの値は、すべてのアプリに適用される
デフォルトの権限ポリシー と権限ポリシー を上書きします。

権限ポリシーを追加 を使用して、アプリカードに 1
つ以上の権限ルールを追加し、削除アクションで削除します。

9.16. トラック ID

デバイスがアクセスできるアプリのクローズドテストトラック IDの一覧。複数のトラック ID が選択されている場合、デバイスはアクセス可能なすべてのトラックの中で最新バージョンを受け取ります
。トラック IDが選択されていない場合、デバイスはアプリの製品版トラックにのみアクセスできます。

トラック IDオプションは、組織で利用可能なトラック IDが少なくとも 1 つあるアプリでのみ使用できます。特定のアプリのクローズドテストトラックに組織を追加する方法

の詳細については、 こちら をお読みください。

10. デフォルトのアプリケーション設定

サポートされている種類のデフォルトアプリを設定します。少なくとも 1 つの種類にデフォルトアプリが設定されている場合、そのプロファイルでユーザーはデフォルトアプリを変
更できなくなります。

デフォルトのアプリケーションの種類 ごとに許可されるデフォルトアプリケーション設定は 1 つのみです。デフォルトアプリケーションの一覧に重複を含めることはできません。

10.1. デフォルトのアプリケーションの種類

構成するアプリカテゴリを選択します（例：ブラウザー、電話、 SMS
、ウォレット、アシスタント）。可用性は Androidのバージョンと管理モードによって異なります。

10.2. デフォルトアプリケーションのスコープ

デフォルトアプリを適用する場所（完全管理、ワークプロファイル、個人プロファイル）を選択します。選
択した種類でサポートされているスコープのみを選択できます。

選択したスコープのいずれもデバイスの管理モードに該当しない場合、デバイスは非コンプライアン
スの詳細を報告します。

10.3. デフォルトアプリケーション

選択した種類のデフォルトとして設定できるアプリの一覧。最初にインストールされた対象のアプリがデフ
ォルトに設定されます。

スコープに 完全管理 または ワークプロファイル が含まれる場合、各アプリは アプリケーション
一覧にも存在し、 インストールタイプ がブロック に設定されていない必要があります。

11. 秘密キーの選択

秘密キールールを選択
に一致するルールがない場合に、ユーザーがデバイスで秘密キーエイリアスを選択するための UI

を表示できるようにします。

Android P
より前のデバイスでは、これを設定するとエンタープライズキーが脆弱になる可能性があります。

12. 秘密キールールを選択

アプリの秘密キーへのアクセスを制御します。ルールは、 Android Device Policy が指定されたアプリに付与する秘密キー（ある場合）を決定します。アクセスは、アプリが
KeyChain.choosePrivateKeyAlias（またはそのオーバーロード）を呼び出して特定の URL
の秘密キーエイリアスを要求したとき、または URL固有でないルール（つまり、 urlPattern
が設定されていない、空の文字列、または .*に設定されている場合）では Android 11
以降で直接付与され、アプリは最初に KeyChain.choosePrivateKeyAliasを呼び出さずに KeyChain.getPrivateKeyを呼び出すことができます。アプリが KeyChain.choosePrivateKeyAlias を呼び出したときに複数の choosePrivateKeyRules
が一致する場合、最後に一致したルールが返すキーエイリアスを定義します。

秘密キールールを追加 を使用してエントリを作成し、削除アクションで削除します。

12.1. 秘密キーエイリアス

使用する秘密キーのエイリアス。

12.2. URLパターン

リクエストの URLと照合する URLパターン。未設定または空の場合、すべての URLに一致します。これは
java.util.regex.Patternの正規表現構文を使用します。

12.3. パッケージ名

このルールが適用されるパッケージ名。各アプリの署名証明書のハッシュは、 Play
から提供されたハッシュと照合されます。パッケージ名が指定されていない場合、エイリアスは
KeyChain.choosePrivateKeyAlias
またはそのオーバーロードを呼び出すすべてのアプリに提供されます（ただし、 Android 11以降でも KeyChain.choosePrivateKeyAlias
を呼び出さない場合は提供されません）。ここで指定されたパッケージと同じ Android UIDを持つアプリは、
KeyChain.choosePrivateKeyAliasを呼び出すとアクセスできます。

パッケージ名を追加 を使用してエントリを追加し、削除アクションで削除します。

アプリを削除するには、アプリカードの下部にある ゴミ箱 アイコンをクリックします。

Revision #60
Created 2025-12-17 10:39:40 UTC by Admin
Updated 2026-11-12 09:56:00 UTC by Admin