ポリシー - Android

- 概要
- アプリ管理
- キオスクモード
- セキュリティ
- マルチメディア
- モバイル通信
- ネットワーク
- システム
- 位置情報とジオフェンス
- ユーザー管理
- 個人利用
- プロファイル間ポリシー
- ステータスレポート
- その他
- コンプライアンス ルール

概要
Android
ポリシーはシステムの中核となるエンティティです。管理対象デバイスに適用および実施されるルールを定
義します。

ダッシュボードの ポリシー セクションから、ポリシーを参照したり新しいポリシーを作成したりできます。
Android ポリシーを開くには、テーブル内のポリシー行をクリックします。システムが ポリシーエディター
ページを開きます。

ポリシーは 登録トークン
に関連付けることができ、プロビジョニングプロセス中にデバイスへ自動的に適用されます。プロビジョニ
ング後にデバイスに割り当てられたポリシーを変更することもできます。

各デバイスは一度に 1 つのポリシーにのみ関連付けることができます。

多くのポリシーオプションは、特定のデバイスタイプ (フルマネージド、専用、仕事用プロファイル)
および Android
バージョンにのみ適用されます。サポートされていない設定は、デバイスによって無視されるか、非
準拠として報告される場合があります。

ポリシーエディターのレイアウト
ポリシーエディターは、一連の展開可能なセクションとして構成されています。ページの上部では、常に次
の項目を編集できます：

名前 (必須)
ID (読み取り専用)
説明 (オプション)

以下のセクションは、ポリシー エディターのパネル (アプリ管理、セキュリティ、ネットワーク、システム、個人利用、プロファイル間ポリシーなど) に対応しています。保存済みのポリシーを開くと、設定が変更されているセクションはすでに開いており、
それ以外は閉じたままです。各パネルの詳細については、このマニュアルの章のページを参照してください
。

保存、削除、および関連付けられたデ

バイス
ポリシーを保存
を使用して変更を適用します。保留中の編集がない場合、またはライセンスが期限切れの場合は、ボタンは
無効になります。

既存のポリシーを開いた場合 (ID がある場合)、ページには ポリシーを削除 アクションと下部に関連付けられたデバイス
リストが表示され、現在そのポリシーを使用しているデバイスの数を確認できます。

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。

キオスクモード
キオスクモードでは、デバイスの機能を単一のアプリまたは複数のアプリに制限できます。単一アプリとマ
ルチアプリのキオスクモードのどちらを選ぶかは、ビジネス目標によって異なります。

単一アプリのキオスクモード
では、デバイスは単一のアプリケーション用に構成され、エンドユーザーはデバイス上の他のアプリにアク
セスできません。またアプリを終了することもできないため、その特定のアプリ専用のデバイスになります

。このモードを有効にするには、 アプリ管理 セクションでアプリを指定し、 インストールタイプ をキオスク に設定します。

マルチアプリのキオスクモード
では、デバイスは複数のアプリケーションへのアクセスを許可されます。エンドユーザーはカスタムランチ
ャーを介して複数のアプリ間を移動できます。このモードを有効にするには、
キオスクカスタムランチャー オプションをオンにします。

キオスクモードが有効な場合、エンドユーザーがシステム設定やステータスバーなどの特定のシステム機能
にアクセスできるかどうかも構成できます。

キオスクカスタムランチャー

キオスクカスタムランチャーが有効かどうか。これにより、ホーム画面が、 アプリ管理設定を介してインストールされたアプリにデバイスをロックダウンするランチャーに置き換わります。アプ
リは 1ページにアルファベット順で表示されます。

電源ボタンの動作

キオスクモードのデバイスで、ユーザーが電源ボタンを押し続けた（長押しした）ときの動作を設定します
。

使用可能（デフォルト）
：キオスクモードのデバイスでユーザーが電源ボタンを長押しすると、電源メニュー（例：電源オフ、
再起動）が表示されます。

ブロック
：キオスクモードのデバイスでユーザーが電源ボタンを長押ししても、電源メニュー（例：電源オフ、再起動）は表示されません。注：これにより、ユーザーがデバイスの電源を切れなくなる可能性があります。

システムエラーの警告

キオスクモードで、クラッシュしたアプリや応答しないアプリのシステムエラーダイアログをブロックする
かどうかを指定します。ブロックすると、ユーザーが UI
で「アプリを閉じる」オプションを選択した場合と同様に、システムはアプリを強制停止します。

ブロック（デフォルト） ：クラッシュやアプリが応答しない（ ANR ）などのすべてのシステムエラーダイアログがブロックされます。ブロックすると、ユーザーが UI
からアプリを閉じた場合と同様に、システムはアプリを強制停止します。

有効 ：クラッシュやアプリが応答しない（ ANR
）などのすべてのシステムエラーダイアログが表示されます。

システムナビゲーション

キオスクモードで有効にするナビゲーション機能（例：ホーム、概要ボタン）を指定します。

無効（デフォルト） ：ホームボタンと概要ボタンにはアクセスできません。

ホームのみ ：ホームボタンのみが有効になります。

有効 ：ホームボタンと概要ボタンが有効になります。

ステータスバー

キオスクモードでシステム情報と通知を無効にするかどうかを指定します。

無効（デフォルト） ：キオスクモードではシステム情報と通知が無効になります。

システムのみ ：ステータスバーにはシステム情報のみが表示されます。

有効
：キオスクモードでは、システム情報と通知がステータスバーに表示されます。注：このポリシーを有
効にするには、 kioskCustomization.systemNavigation を使用してデバイスのホームボタンを有効にする必要があります。

デバイス設定

キオスクモードで設定アプリを許可するかどうかを指定します。

セキュリティ
このセクションでは、セキュリティ関連のポリシーを設定できます。

セキュリティリスクアクション

デバイスがステータスレポートで SecurityRisk を報告したときの動作を選択します。

サポートされている SecurityRisk の種類：

不明な OS： Play Integrity API が、デバイスが不明な OS で実行されていることを検出します
(basicIntegrity チェックは成功しますが、 ctsProfileMatch は失敗します)。

侵害された OS： Play Integrity API が、デバイスが侵害された OS
で実行されていることを検出します (basicIntegrity チェックが失敗します)。

ハードウェアによる評価に失敗 ：デバイスの整合性フィールドに MEETS_STRONG_INTEGRITY
ラベルが表示されない場合、 Play Integrity API
が、デバイスにシステム整合性の強力な保証がないことを検出します。

利用可能なアクション：

企業データをワイプ (デフォルト)：登録を解除して仕事データをワイプします (
フルマネージドの場合はデバイス全体、プロファイル所有の場合は仕事用プロファイルのみ)。

アクションなし ：デバイスを登録したままにし、自動的な操作は行いません。

企業データをワイプ を選択すると、ワイプオプションも設定できます：

工場出荷時リセット保護を保持 ：デバイスをワイプするときに Factory Reset Protection (FRP)
データを保持します。

外部ストレージをワイプ ：ワイプを実行するときに、デバイスの外部ストレージ (SD カードなど)
も追加でワイプします。

eSIM をワイプ ：会社所有デバイスの場合、デバイスがワイプされるときにデバイスからすべての
eSIM が削除されます。個人所有デバイスの場合、デバイス上の管理対象 eSIM (ADD_ESIM
コマンドで追加された eSIM) が削除され、個人所有の eSIM は削除されません。

1. ロックまでの最大時間

デバイスがロックされるまでのユーザーアクティビティの最大時間 (秒) です。値が 0
の場合は制限がないことを意味します。

2. 充電中はオンのまま

デバイスがオンのままになるバッテリー接続モードです。この設定を使用する場合、デバイスがオンのまま
ロックされないように、 ロックまでの最大時間 をクリアすることをお勧めします。

AC 充電器 ：電源は AC 充電器です。

USB ポート ：電源は USB ポートです。

ワイヤレス充電器 ：電源はワイヤレスです。

3. キーガード無効

true の場合、プライマリおよび /
またはセカンダリディスプレイのロック画面を無効にします。このポリシーは専用デバイス管理モードでの
みサポートされます。

4. パスワード要件

パスワード要件ポリシー。

パスワード要件を設定 を使用して、 1 つ以上のパスワード要件ブロックを追加します。 すべてクリアを使用して、設定済みのすべてのパスワード要件を削除します。

パスワード要件では、 自動 スコープ (単一の要件) または個別の デバイス /仕事用プロファイルスコープを使用できます。複雑さベースの要件は、同じスコープの品質ベースの要件と組み合わせる必要が
あります。

4.1. スコープ

パスワード要件を適用するスコープです。

自動
：スコープは指定されていません。パスワード要件は、仕事用プロファイルデバイスでは仕事用プロフ
ァイルに、フルマネージドデバイスまたは専用デバイスではデバイス全体に適用されます。

デバイス ：パスワード要件はデバイスにのみ適用されます。

仕事用プロファイル ：パスワード要件は仕事用プロファイルにのみ適用されます。

4.2. パスワード履歴の長さ

パスワード履歴の長さです。このフィールドを設定すると、ユーザーは履歴内のいずれかのパスワードと同
じ新しいパスワードを入力できなくなります。値が 0 の場合は制限がないことを意味します。

4.3. ワイプまでの最大パスワード失敗回数

デバイスがワイプされるまでに入力できる、誤ったデバイスロック解除パスワードの回数です。値が 0 の場合は制限がないことを意味します。

4.4. パスワード有効期限 (日)

この設定では、指定した日数が経過すると、ユーザーは定期的にパスワードを更新する必要があります。

4.5. パスワードによるロック解除を要求

デバイスまたは仕事用プロファイルを強力な認証方法 (パスワード、 PIN、パターン)
でロック解除した後、他の認証方法 (指紋、信頼エージェント、顔など)
でロック解除できる時間の長さです。指定した期間が経過すると、デバイスまたは仕事用プロファイルのロ
ックを解除できるのは強力な認証方法のみになります。

デバイスのデフォルト ：タイムアウト期間はデバイスのデフォルトに設定されます。

毎日 ：タイムアウト期間は 24 時間に設定されます。

4.6. パスワード品質

必要なパスワード品質です。

複雑さ: 高 ：高パスワード複雑さバンドを次のように定義します。 Android 12 以降: 繰り返し (4444)
や順序 (1234、4321、2468) のシーケンスがない PIN、長さ 8 以上、英字は長さ 6
以上、英数字は長さ 6 以上。

複雑さ: 中 ：中パスワード複雑さバンドを次のように定義します。繰り返し (4444) や順序 (1234、 4321、2468) のシーケンスがない PIN、長さ 4 以上、英字は長さ 4 以上、英数字は長さ 4 以上。

複雑さ: 低 ：低パスワード複雑さバンドを次のように定義します。パターン、繰り返し (4444) や順序 (1234、4321、2468) のシーケンスがある PIN。

なし ：パスワード要件はありません。

弱
：デバイスは少なくとも低セキュリティの生体認証技術で保護されている必要があります。これには、
3 桁の PIN とほぼ同等の個人の身元を認識できる技術が含まれます (誤検出は 1,000 分の 1 未満)。

任意 ：パスワードは必須ですが、パスワードの内容に制限はありません。

数値 ：パスワードには数値文字を含める必要があります。

数値 (複雑)：パスワードには、繰り返し (4444) や順序 (1234、4321、2468)
のシーケンスがない数値文字を含める必要があります。

英字 ：パスワードには英字 (または記号) 文字を含める必要があります。

英数字 ：パスワードには数値文字と英字 (または記号) 文字の両方を含める必要があります。

複雑 ：パスワードは、 passwordMinimumLength、passwordMinimumLetters、
passwordMinimumSymbols などで指定された最小要件を満たす必要があります。たとえば、 passwordMinimumSymbols が 2 の場合、パスワードには少なくとも 2
つの記号を含める必要があります。

4.7. 最小長

許可される最小のパスワード長です。値が 0 の場合は制限がないことを意味します。

4.8. 最小英字数

パスワードに必要な最小英字数です。

4.9. 最小小文字数

パスワードに必要な最小小文字数です。

4.10. 最小大文字数

パスワードに必要な最小大文字数です。

4.11. 最小非英字文字数

パスワードに必要な最小非英字文字数 (数値または記号) です。

4.12. 最小数値桁数

パスワードに必要な最小数値桁数です。

4.13. 最小記号数

パスワードに必要な最小記号数です。

4.14. 統合ロック

仕事用プロファイルを備えた Android 9
以降のデバイスで、デバイスと仕事用プロファイルに統合ロックを許可するかどうかを制御します。他のデ
バイスには影響しません。

統合ロックを許可 ：デバイスと仕事用プロファイルに共通のロックが許可されます。

個別の仕事用ロックを要求 ：仕事用プロファイルに個別のロックが必要です。

5. 工場出荷時リセット無効

設定からの工場出荷時リセットが無効かどうか。フルマネージドデバイスにのみ適用されます。

6. 工場出荷時リセット保護

工場出荷時リセット保護のためのデバイス管理者のメールアドレスです。デバイスが不正な工場出荷時リセ
ットを受けた場合、これらの管理者の 1 人が Google アカウントのメールアドレスとパスワードでログインしてデバイスのロックを解除する必要があります。管理者が指定されていない場合、デバイスは工場出荷時リセット保護を提供しません。フルマネージドデバイ
スにのみ適用されます。

管理者のメールアドレス ： 工場出荷時リセット保護を有効にする
を使用して管理者の設定を開始します。次に 管理者のメールアドレスを追加を使用してアドレスを追加し、削除アクションで削除します。

7. キーガード機能

無効にできるキーガード (ロック画面) 機能。

7.1. すべて無効化

現在および将来のすべてのキーガードカスタマイズを無効にします。

7.2. カメラを無効化

セキュアなキーガード画面 (PIN など) でカメラを無効にします。

7.3. 通知を無効化

セキュアなキーガード画面でのすべての通知の表示を無効にします。

7.4. 未編集の通知を無効化

セキュアなキーガード画面で未編集の通知を無効にします。

7.5. 信頼エージェントの状態を無視

セキュアなキーガード画面で信頼エージェントの状態を無視します。

7.6. 指紋を無効化

セキュアなキーガード画面で指紋センサーを無効にします。

7.7. 通知へのテキスト入力を無効化

セキュアなキーガード画面で通知へのテキスト入力を無効にします。

7.8. 顔認証を無効化

セキュアなキーガード画面で顔認証を無効にします。

7.9. 虹彩認証を無効化

セキュアなキーガード画面で虹彩認証を無効にします。

7.10. すべての生体認証を無効化

セキュアなキーガード画面ですべての生体認証を無効にします。

7.11. すべてのショートカットを無効化
Android 14 以降のセキュアなキーガード画面ですべてのショートカットを無効にします。

マルチメディア
このセクションでは、カメラ /マイクの動作、 USB
データアクセス、印刷、ディスプレイ関連の制限を構成できます。

1. カメラアクセス

カメラの使用と、ユーザーがカメラアクセスの切り替えにアクセスできるかどうか（ Android 12
以降）を制御します。一般に、カメラを無効にすると、完全管理デバイスではデバイス全体に適用され、仕
事用プロファイルデバイスでは仕事用プロファイル内にのみ適用されます。

ユーザーの選択（デフォルト） ：デフォルトのデバイス動作です。カメラは利用可能で、（ Android 12以降）ユーザーはカメラアクセスを切り替えられます。

無効
：すべてのカメラが無効になります（完全管理：デバイス全体、仕事用プロファイル：仕事用プロファ
イルのアプリのみ）。管理対象スコープでは、カメラアクセスの切り替えは効果がありません。

強制 ：カメラは利用可能です。 Android 12
以降を実行する完全管理デバイスでは、ユーザーはカメラアクセスを切り替えられません。その他のデ
バイス /バージョンでは、ユーザーの選択と同様に動作します。

2. マイクアクセス

完全管理デバイスでは、マイクの使用と、ユーザーがマイクアクセスの切り替えにアクセスできるかどうか
（Android 12以降）を制御します。この設定は、完全管理されていないデバイスには効果がありません。

ユーザーの選択（デフォルト） ：デフォルトの動作です。マイクは利用可能で、（ Android 12 以降）ユーザーはマイクアクセスを切り替えられます。

無効 ：マイクが無効になります（デバイス全体）。マイクアクセスの切り替えは効果がありません。

強制 ：マイクは利用可能です。 Android 12
以降では、ユーザーはマイクアクセスを切り替えられません。 Android 11
以前では、ユーザーの選択と同様に動作します。

3. USBデータアクセス

USB経由で転送できるファイルやデータを制御します。会社所有デバイスでのみサポートされます。

ファイル転送を許可しない（デフォルト） ：ファイル転送は許可されませんが、他の USB
データ接続（例：マウス /キーボード）は許可されます。

データ転送を許可しない ：すべての種類の USBデータ転送が禁止されます（ USB HAL 1.3
以降を備えた Android 12
以降）。サポートされていない場合、デバイスは「ファイル転送を許可しない」にフォールバックしま
す。

データ転送を許可 ：すべての種類の USBデータ転送が許可されます。

4. 印刷

印刷を許可するかどうかを制御します（ Android 9以降）。

許可（デフォルト） ：印刷が許可されます。

許可しない ：印刷は許可されません（ Android 9以降）。

5. 画面の明るさ設定

画面の明るさモードと（オプションで）明るさの値を制御します。

画面の明るさモード：

ユーザーの選択（デフォルト） ：ユーザーは画面の明るさを構成できます。

自動
：明るさは自動になり、ユーザーは変更できません。明るさの値は設定できますが、自動調整の一部と
して使用されます（完全管理の Android 9以降、会社所有の Android 15以降の仕事用プロファイル）。

固定
：明るさは構成した値に設定され、ユーザーは変更できません。明るさの値は必須です（完全管理の
Android 9以降、会社所有の Android 15以降の仕事用プロファイル）。

画面の明るさ：

1～255の値（ 1 = 最低、 255 = 最高）。値が 0
の場合は、明るさの値が設定されていないことを意味します。

6. 画面のタイムアウト設定

ユーザーが画面のタイムアウトを構成できるかどうか、また強制する場合はタイムアウト値を制御します。
画面のタイムアウトモード フィールドでは、ユーザー制御と強制の動作を切り替えます。
ユーザーの選択（デフォルト） ：ユーザーは画面のタイムアウトを構成できます。
強制 ：画面のタイムアウトは構成した値に設定され、ユーザーは変更できません（完全管理の Android
9以降、会社所有の Android 15以降の仕事用プロファイル）。
画面のタイムアウト：
タイムアウト時間（秒）。値は 0より大きい必要があります。 ロックまでの最大時間
より大きい場合、システムが値を制限し、非準拠として報告する可能性があります。

7. 画面キャプチャの無効化

画面キャプチャが無効かどうか。

8. 音量調整の無効化

マスター音量の調整が無効かどうか。

9. 物理メディアのマウントの無効化

物理的な外部メディアのマウントが無効かどうか。

モバイル通信
このセクションでは、モバイル通信に関連するポリシーを構成できます。

1. 機内モード

機内モードをユーザーが切り替えられるかどうかを制御します。

ユーザーの選択（デフォルト）
：ユーザーは機内モードをオンまたはオフに切り替えることができます。

無効 ：機内モードは無効です。ユーザーは機内モードをオンに切り替えることはできません。 Android
9以降でサポートされています。

2. モバイル通信 2G

モバイル通信 2G設定をユーザーが切り替えられるかどうかを制御します。

ユーザーの選択（デフォルト） ：ユーザーはモバイル通信 2G
をオンまたはオフに切り替えることができます。

無効 ：モバイル通信 2Gは無効です。ユーザーは設定からモバイル通信 2G
をオンに切り替えることはできません。 Android 14以降でサポートされています。

3. APNsの上書き

APNsの上書きを有効にするか無効にするかを制御します。有効にすると、構成された上書き APNs
のみが使用され、デバイス上の他のすべての APNsは無視されます。

無効（デフォルト） ：設定済みのすべての APN
設定はデバイスに保存されますが、無効になっており効果はありません。デバイス上の他の APN
はすべて引き続き使用されます。

有効 ：上書き用 APNのみが使用され、他の APNはすべて無視されます。この設定は、 Android 10
以上の完全管理デバイスでのみ構成できます。

4. APN設定

1つ以上の APNエントリを構成します。 APNを追加 でエントリを作成し、 APNを削除 で削除します。

各APNには必須フィールドがあります：

APNタイプ ：この APNのトラフィックタイプを 1つ以上選択します（利用可能かどうかは管理モードと
Androidのバージョンによって異なります）。

APN名 ：通信事業者が提供する APN識別子です。

表示名 ： UIに表示されるわかりやすい名前です。

任意の APNフィールド：

認証タイプ 、ユーザー名 、パスワード ：通信事業者の認証を構成します（必要な場合）。

プロトコル とローミングプロトコル ： IPプロトコルの構成です。

ネットワークタイプ ：APNが使用できるセルラー技術を制限します（例： LTE/5G NR）。

プロキシアドレス とプロキシポート ：データトラフィック用の HTTP
プロキシです（該当する場合）。

MMSプロキシアドレス 、 MMSプロキシポート 、 MMSC（ MMSセンター URI） ： MMS 関連の設定です。

数値オペレーター ID（ MCC+MNC） とキャリア ID：通信事業者を識別するフィールドです。

Always On設定 ：この APNによってアクティブ化される PDUセッションを常時オンにするかどうか。
Android 15以上でサポートされます。

MVNOタイプ ：モバイル仮想ネットワーク事業者の識別子タイプです。

MTU IPv4と MTU IPv6： IPv4/IPv6ルートの最大転送単位です。 Android 13
以上でサポートされます。

5. セルブロードキャスト設定の無効化

セルブロードキャストの構成が無効かどうか。

6. モバイルネットワーク設定の無効化

モバイルネットワークの構成が無効かどうか。

7. ローミングデータの無効化

ローミングデータサービスが無効かどうか。

8. 発信の無効化

発信が無効かどうか。

9. SMSの無効化

SMSメッセージの送受信が無効かどうか。

10. 5Gネットワークスライシングの構成

エンタープライズ 5G
ネットワークスライシングを有効にするには、優先ネットワークサービスの設定を構成します。最大 5 つのエンタープライズスライスを設定し、アプリケーションを特定のネットワークに割り当てて、トラフィ
ックルーティングを最適化できます。

10.1. デフォルトの優先ネットワーク

アプリケーションリストにないアプリケーション、またはアプリの 優先ネットワークが設定されていない場合に使用する、デフォルトの優先ネットワーク IDです。指定したネットワーク ID の構成が必要です（ 優先ネットワークなし に設定されている場合を除く）。

注： com.google.android.apps.work.clouddpcやcom.google.android.gms
などの重要なアプリは、このデフォルト設定から除外されます。

10.2. ネットワークサービス構成

ネットワーク構成を追加 を使用してスライス構成を作成します。最大 5
つの構成を追加できます。各構成には次のものがあります：

優先ネットワーク ID（自動割り当て） ：ネットワーク ID は自動的に割り当てられ、変更できません。

デフォルト接続へのフォールバック
：デバイス全体のデフォルトネットワークへのフォールバックを許可するかどうか。許可しない場合、 5Gスライスが利用できないときアプリはインターネットにアクセスできません。

一致しないネットワーク
：この構成の対象となるアプリが、優先サービス以外のネットワークを使用できるかどうか。
許可しない に設定する場合、 デフォルト接続へのフォールバック も許可しないにする必要があります。 Android 14以上が必要です。

ネットワーク
このセクションでは、ネットワーク関連のポリシーを構成できます。

WiFi構成 を介して、システムが Wi‑Fi構成をプロビジョニングおよび管理できます。 Wi‑Fiの構成に設定された値に応じて、ユーザーはネットワークの追加 /
変更を制限されたり、まったく制御できなかったりする場合があります。

デバイスの無線状態

1. Wi‑Fiの状態

Wi‑Fiの現在の状態と、ユーザーがその状態を変更できるかどうかを制御します。

ユーザーの選択（デフォルト） ：ユーザーは Wi‑Fiを有効 /無効にできます。

有効 ：Wi‑Fiはオンで、ユーザーはオフにできません（ Android 13以降）。

無効 ：Wi‑Fiはオフで、ユーザーはオンにできません（ Android 13以降）。

2. 最小 Wi‑Fiセキュリティレベル

デバイスが接続できる Wi‑Fiネットワークの最小要件セキュリティレベルです。 Android 13 以降の完全管理デバイスと会社所有デバイスの仕事用プロファイルでサポートされます。

オープンネットワーク（デフォルト） ：デバイスはすべての種類の Wi‑Fi
ネットワークに接続できます。

パーソナルネットワーク ：オープンな Wi‑Fi
ネットワークを許可せず、少なくともパーソナルセキュリティ（例： WPA2‑PSK）を要求します。

エンタープライズネットワーク ：エンタープライズ EAP
ネットワークを要求し、このセキュリティレベル未満の Wi‑Fiネットワークを許可しません。

192ビットエンタープライズネットワーク ： 192
ビットのエンタープライズネットワークを要求します。最も厳しいオプションです。

3. 超広帯域（ UWB）の状態

超広帯域設定の状態と、ユーザーがオン /オフを切り替えられるかどうかを制御します。

ユーザーの選択（デフォルト） ：ユーザーは UWBのオン /オフを切り替えられます。

無効 ： UWBは無効で、ユーザーは設定から切り替えられません（ Android 14以降）。

デバイス接続管理

4. Bluetooth共有

Bluetooth共有を許可するかどうかを制御します。

許可 ： Bluetooth共有が許可されます（完全管理デバイスのデフォルト、 Android 8以降）。

許可しない ： Bluetooth共有は許可されません（仕事用プロファイルのデフォルト、 Android 8
以降）。

5. Wi‑Fiの構成

Wi‑Fi構成の権限を制御します。選択したオプションに応じて、ユーザーは Wi‑Fi
ネットワークの構成を完全に制御できるか、制限付きで制御できるか、まったく制御できません。

Wi‑Fiの構成を許可（デフォルト） ：ユーザーは Wi‑Fiを構成できます。

Wi‑Fi構成の追加を許可しない ：新しい Wi‑Fi
構成の追加は許可されません。ユーザーは構成済みのネットワークを切り替えられます（ Android 13
以降、完全管理および会社所有の仕事用プロファイル）。

Wi‑Fiの構成を許可しない ：Wi‑Fi
ネットワークの構成を許可しません。完全管理デバイスでは、ユーザーが構成したネットワークが削除
され、 WiFi構成
を介して構成されたネットワークのみが保持されます。会社所有の仕事用プロファイルでは、既存のネ
ットワークは影響を受けませんが、ユーザーは Wi‑Fiネットワークを追加 /削除 /変更できません。

> Wi-Fiの構成が無効になっていて、デバイスが起動時に接続できない場合、システムは
> ネットワークエスケープハッチ
> を表示して、ユーザーが一時的に接続してポリシーを更新できるようにすることがあります。

6. Wi-Fi Direct設定

Wi-Fi Direct設定の構成と使用を制御します。 Android 13
以降を実行する会社所有デバイスでサポートされます。

許可（デフォルト） ：ユーザーは Wi-Fi Directを使用できます。

許可しない ：ユーザーは Wi-Fi Directを使用できません。

7. テザリング設定

テザリング設定を制御します。設定された値に応じて、ユーザーはさまざまな形式のテザリングを部分的ま
たは完全に使用できなくなります。

すべてのテザリングを許可（デフォルト）
：すべての形式のテザリングの構成と使用を許可します。

Wi-Fiテザリングを許可しない ：ユーザーが Wi-Fi
テザリングを使用することを許可しません（会社所有の Android 13以降）。

すべてのテザリングを許可しない
：すべての形式のテザリングを許可しません（完全管理および会社所有の仕事用プロファイル）。

8. Wi-Fi SSIDポリシー

デバイスが接続できる Wi-Fi SSIDの制限です（デバイスで構成できるネットワークには影響しません）。
Android 13以降を実行する会社所有デバイスでサポートされます。

SSID拒否リスト（デフォルト） ： SSIDがリストに含まれている Wi-Fi
ネットワークには接続できませんが、他のネットワークには接続できます。

SSID許可リスト ：デバイスはリストに含まれる SSIDにのみ接続できます。 SSID
リストを空にすることはできません。

SSIDを追加
を使用してエントリを追加します。選択したポリシーの種類に応じて、リストは許可または拒否する SSID

として解釈されます。
ポリシーエディターの UIでは、 SSIDリストは許可リストの場合は 許可された Wi‑Fi SSID
、拒否リストの場合は 拒否された Wi‑Fi SSIDというラベルになります。

9. Wi‑Fiローミング設定

SSIDごとに Wi‑Fiローミングモードを構成します。エントリを作成するには、 Wi‑Fiローミング設定を追加
を使用します。
各エントリには次が含まれます：
SSID：ローミング設定を適用する SSIDです（必須）。
Wi‑Fiローミングモード ：デフォルト / 無効 / アグレッシブ。無効とアグレッシブには Android 15 以降が必要で、完全管理デバイスと会社所有デバイスの仕事用プロファイルでのみサポートされます。

ネットワークの制限

10. Bluetoothの無効化

Bluetoothが無効かどうか。 Bluetooth
設定の無効化はユーザーが回避できるため、この設定を優先してください。

11. Bluetooth連絡先共有の無効化

Bluetooth連絡先共有が無効かどうか。

12. Bluetooth設定の無効化

Bluetoothの構成が無効かどうか。

13. ネットワークリセットの無効化

ネットワーク設定のリセットが無効かどうか。

14. 送信ビームの無効化

NFCを使用してアプリからデータをビーム送信することが無効かどうか。

VPN

15. Always On VPNアプリ

Always On VPNのパッケージ名を指定して、指定した管理対象アプリのデータが常に構成済みの VPN を経由するようにします。

注：この機能を使用するには、 Always Onとアプリ別 VPNの両方の機能をサポートする VPN
クライアントを展開する必要があります。

16. VPNロックダウン

VPNが接続されていないときのネットワーク接続を許可しません。

17. VPN設定の無効化

VPNの構成が無効かどうか。

プロキシとネットワークサービス

18. 優先ネットワークサービス

仕事用プロファイルで優先ネットワークサービスを有効にするかどうかを制御します。たとえば、組織が通
信事業者と契約して、仕事用データがエンタープライズ専用の通信事業者ネットワークサービス（例： 5G

ネットワーク上のエンタープライズスライス）を介して送信されるようにすることがあります。これは完全管理デバイスには影響しません。

無効：仕事用プロファイルで優先ネットワークサービスが無効になります。

有効：仕事用プロファイルで優先ネットワークサービスが有効になります。

エンタープライズネットワークスライシングを使用する場合は、**5G** ネットワークスライシングの構成 を セルラー ポリシーパネルでも構成し、アプリを 優先ネットワーク 設定でスライスに割り当てます。

19. 推奨グローバルプロキシ

ネットワークに依存しないグローバル HTTPプロキシです。通常、プロキシは WiFi 構成でネットワークごとに構成する必要があります。グローバルプロキシは、一般的な内部フィルタリングなどの特殊な構成に役立つ場合があります。グローバルプロキシはあくまで推奨であり、一部のアプリは無視する場合があります。

無効

直接プロキシ

プロキシ自動設定 **(PAC)**

19.1. ホスト

直接プロキシのホストです。

19.2. ポート

直接プロキシのポートです。

19.3. PAC URI

プロキシの設定に使用する PAC スクリプトの URI です。

19.4. 除外ホスト

直接プロキシの場合、プロキシをバイパスするホストです。ホスト名には ***.example.com** などのワイルドカードを含めることができます。

除外ホストを追加 を使用してエントリを追加します（直接プロキシでのみ使用可能です）。

Wi-Fi 設定

デバイスにシステムが適用する Wi-Fi ネットワーク設定を定義します。 **Wi-Fi** 設定を追加
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。

20. Wi-Fi 設定フィールド

各設定には以下が含まれます:

設定名 ：必須。

SSID: 必須。

自動接続 ：ネットワークが範囲内にあるときに自動的に接続するかどうか。

Fast Transition: クライアントがネットワークで Fast Transition (IEEE 802.11r-2008)
を使用しようとするかどうか。

非表示 **SSID**: SSID がブロードキャストされるかどうか。

MAC ランダム化モード ：ハードウェアまたは自動 (Android 13+)。

20.1. セキュリティ

Wi-Fi セキュリティオプション:

WEP-PSK: WEP (事前共有キー)。

WPA-PSK: WPA/WPA2/WPA3-Personal (事前共有キー)。

WPA-EAP: WPA/WPA2/WPA3-Enterprise (拡張認証プロトコル)。

WPA3 192-bit モード : WPA3 192-bit モードのみを許可する WPA-EAP ネットワーク。

20.2. パスフレーズ (事前共有キー)

セキュリティが **WEP-PSK** または **WPA-PSK** の場合に表示されます。パスフレーズは必須です。

20.3. EAP メソッド (エンタープライズ)

セキュリティが WPA‑EAPまたは WPA3 192-bit モード の場合に表示されます。 EAP の外部メソッドを 1 つ選択してください：

EAP‑TLS

EAP‑TTLS

PEAP

EAP‑SIM

EAP‑AKA

20.4. フェーズ 2 認証

トンネリング外部メソッド（ EAP‑TTLSおよび PEAP）の場合に表示されます。

MSCHAPv2

PAP

20.5. ユーザーからの EAP 認証情報

有効にすると、システムはユーザーごとにデバイスへ EAP 認証情報を自動的に適用します。 ユーザー セクションでユーザー認証情報を設定できます。

20.6. クライアント証明書

Wi‑Fi 認証に使用するクライアント証明書を EAP‑TLSに割り当てることができます。詳細については、

証明書管理 ページをお読みください。

証明書がすでに割り当てられている場合は、 証明書を開く で表示するか、 証明書を変更
で別の証明書を選択できます。

または、 Android キーチェーンに保存され、 Wi‑Fi 認証に許可されているクライアント証明書を参照するクライアント証明書キーペアのエイリアス を指定できます。

クライアント証明書 とクライアント証明書キーペアのエイリアス
の両方が設定されている場合、キーペアのエイリアスは無視されます。

20.7. ID

ユーザーの ID。トンネリング外部プロトコル（ PEAP、 EAP‑TTLS
）では、トンネル内の認証に使用され、トンネル外の EAP ID には 匿名 ID が使用されます。非トンネリング外部プロトコルでは、 EAP ID に使用されます。

20.8. 匿名 ID
トンネリングプロトコルのみで、外部プロトコルに提示されるユーザーの ID を示します。

20.9. パスワード

ユーザーのパスワード。指定しない場合、デフォルトでユーザーにプロンプトが表示されます。

20.10. サーバー CA 証明書
ホストの証明書チェーンの検証に使用する CA 証明書のリストです。少なくとも 1 つの CA
証明書が一致する必要があります。詳細については、 証明書管理 ページをお読みください。
サーバー CA 証明書を追加 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。

20.11. ドメインサフィックスの一致
サーバードメイン名の制約のリストです。エントリは、認証サーバー証明書の代替サブジェクト名の DNS 名に対するサフィックス一致要件として使用されます。

システム
このセクションでは、システム関連のポリシーを設定できます。

1. 最小 API レベル

許可される最小の Android API レベルです。

2. 暗号化ポリシー

暗号化が有効かどうか。
デフォルト ：この値は無視されます。つまり、暗号化は不要です。
パスワードなしで有効 ：暗号化は必須ですが、起動時のパスワードは不要です。パスワードありで有効 ：暗号化が必須で、起動時にパスワードが必要です。

3. 日付と時刻の自動設定

会社所有デバイスで日付、時刻、タイムゾーンの自動設定が有効かどうか。
ユーザーの選択 (デフォルト)
：日付、時刻、タイムゾーンの自動設定はユーザーの選択に委ねられます。
強制 ：デバイスで日付、時刻、タイムゾーンの自動設定を強制します。

4. 開発者設定

開発者設定 (開発者オプションとセーフブート) へのアクセスを制御します。
無効 (デフォルト): すべての開発者設定を無効にし、ユーザーがアクセスできないようにします。許可: すべての開発者設定を許可します。ユーザーは設定にアクセスし、必要に応じて構成できます。

5. Common Criteria モード

Common Criteria モードを制御します。 Common Criteria モードは、情報技術セキュリティ評価の
Common Criteria (CC) で定義されたセキュリティ標準です。 Common Criteria モードを有効にすると、デバイス上の特定のセキュリティコンポーネントが強化されます (例: Bluetooth Long Term Keys の AES-GCM
暗号化、一部のネットワーク証明書に対する追加検証、暗号化ポリシーの整合性チェック)。Common Criteria モードは、 Android 11 以降を実行する会社所有のデバイスでのみサポートされます。警告 : Common Criteria
モードは、通常は高度に機密性の高い組織でのみ必要とされる厳格なセキュリティモデルを適用します。標
準的なデバイスの使用に影響する可能性があります。必要な場合にのみ有効にしてください。

無効 (デフォルト): Common Criteria モードを無効にします。

有効: Common Criteria モードを有効にします。

6. Memory Tagging Extension (MTE)

デバイス上の Memory Tagging Extension (MTE) を制御します。

ユーザーの選択 (デフォルト): ユーザーはデバイスで MTE を有効または無効にできます (
デバイスがサポートしている場合)。

強制: MTE が有効になり、ユーザーは変更できません (Android 14 以降。完全管理デバイスおよび会社所有デバイス上の仕事用プロファイルでサポートされます)。

無効: MTE が無効になり、ユーザーは変更できません (Android 14
以降。完全管理デバイスでのみサポートされます)。

7. コンテンツ保護

欺瞞的なアプリをスキャンするコンテンツ保護を有効にするかどうかを制御します。これは Android 15 以降でサポートされます。

無効 (デフォルト): コンテンツ保護は無効になり、ユーザーはこれを変更できません。

強制: コンテンツ保護が有効になり、ユーザーはこれを変更できません (Android 15 以降)。

ユーザーの選択 : コンテンツ保護はポリシーで制御されません。ユーザーが選択できます (Android
15 以降)。

8. アシストコンテンツ

AssistContent をアシスタントアプリなどの特権アプリに送信できるかどうかを制御します (例: Circle to Search)。AssistContent にはスクリーンショットやアプリの情報 (パッケージ名など)
が含まれます。これは Android 15 以降でサポートされます。

許可 (デフォルト): アシストコンテンツを特権アプリに送信できます (Android 15 以降)。

不許可: アシストコンテンツを特権アプリに送信できません (Android 15 以降)。

9. ウィンドウ作成の無効化

アプリのウィンドウ以外のウィンドウの作成を無効にするかどうか。このオプションは、次のシステム UI が表示されないようにします : トーストとスナックバー、電話アクティビティ (着信など)
と優先電話アクティビティ (通話中など)、システムアラート、システムエラー、システムオーバーレイ。

10. ネットワークエスケープハッチ

ネットワークエスケープハッチを有効にするかどうか。起動時にネットワーク接続を確立できない場合、エ
スケープハッチはデバイスポリシーを更新するために一時的にネットワークに接続するようユーザーに促し
ます。ポリシーを適用した後、一時的なネットワークは忘れられ、デバイスの起動が続行されます。これにより、最後のポリシーに適切なネットワークがなく、デバイスがロックタスクモードのアプリで起動した場合や、ユーザーがデバイス設定にアクセスできない場合に、ネットワークに接続できなくなることを防ぎます。

11. デフォルトアクティビティ

特定のインテントフィルターに一致するインテントを処理するためのデフォルトアクティビティのリスト。
たとえば、この機能により、 IT 管理者は、 Web リンクを自動的に開くブラウザアプリや、ホームボタンをタップしたときに使用するランチャーアプリを選
択できます。

デフォルトアクティビティを追加 を使用してエントリを作成します。エントリ内では、アクションを追加 と カテゴリを追加 を使用してインテントフィルターを構築します。

11.1. 受信アクティビティ

デフォルトのインテントハンドラーとなるアクティビティ。これは Android のコンポーネント名 (例: com.android.enterprise.app/.MainActivity)
である必要があります。または、値はアプリのパッケージ名でもかまいません。その場合、 Android Device Policy がアプリから適切なアクティビティを選択してインテントを処理します。

11.2. アクション

フィルターで一致させるインテントアクション。フィルターにアクションが含まれている場合、インテント
が一致するには、そのアクションがそれらの値のいずれかである必要があります。アクションが含まれてい
ない場合、インテントアクションは無視されます。

11.3. カテゴリ

フィルターで一致させるインテントカテゴリ。インテントには必要なカテゴリが含まれており、一致するにはそれらすべてがフィルターに含まれている必要があります。つまり、フィルターにカテゴリを追加しても、そのカテゴリがインテントで指定されていない限り、一致には影響しません。

12. 許可する入力方法

許可する入力方法を指定します。

すべて許可 : 制限は適用されません。すべての入力方法が許可されます。

システムのみ : システムに組み込まれた入力方法のみが許可されます。

システムと提供されたもののみ :
提供された入力方法とシステムに組み込まれた入力方法のみが許可されます。

12.1. 許可する入力方法

許可する入力方法のパッケージ名。 許可する入力方法 が システムと提供されたもののみに設定されている場合にのみ適用されます。

入力方法を追加 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。

13. 許可するアクセシビリティサービス

許可するアクセシビリティサービスを指定します。

すべて許可 : 任意のアクセシビリティサービスを使用できます。

システムのみ : システムに組み込まれたアクセシビリティサービスのみを使用できます。

システムと提供されたもののみ : 提供されたアクセシビリティサービスとシステムに組み込まれたアクセシビリティサービスのみを使用
できます。

13.1. 許可するアクセシビリティサービス

許可するアクセシビリティサービス。 許可するアクセシビリティサービス が
システムと提供されたもののみ に設定されている場合にのみ適用されます。

アクセシビリティサービスを追加 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。

14. システム更新ポリシー

システム更新を管理するための構成。

デフォルト :
デバイスのデフォルトの更新動作に従います。通常、ユーザーがシステム更新を承認する必要がありま
す。

自動: 更新が利用可能になり次第、自動的にインストールします。

ウィンドウ指定 : 毎日のメンテナンスウィンドウ内で自動的にインストールします。これにより、
Play
アプリもウィンドウ内で更新されるように構成されます。これはキオスクデバイスに強く推奨されます
。なぜなら、これが Play
によって前景に固定されたアプリを継続的に更新できる唯一の方法だからです。

延期: 自動インストールを最大 30 日間延期します。

14.1. メンテナンスウィンドウ (ウィンドウ指定の場合のみ)

システム更新ポリシー が ウィンドウ指定 に設定されている場合、 fromと to フィールドを使用して毎日のメンテナンスウィンドウを定義できます。

14.2. システム更新の凍結期間

デバイスで実行されている OS バージョンを凍結するために、無線 (OTA)
システム更新が延期される毎年繰り返される期間。デバイスを無期限に凍結しないようにするには、各凍結
期間を少なくとも 60 日空ける必要があります。各凍結期間は 90 日を超えてはなりません。

システム更新の凍結期間を追加 を使用してエントリを作成します。

15. 認証情報プロバイダーのデフォルト

Android 14 以降で、どのアプリを認証情報プロバイダーとして使用できるかを制御します。

不許可 (デフォルト): credentialProviderPolicy
が指定されていないアプリは、認証情報プロバイダーとして機能できません。

システムを除き不許可 : credentialProviderPolicy が指定されていないアプリは、 OEM のデフォルト認証情報プロバイダーを除き、認証情報プロバイダーとして機能できません。

位置情報とジオフェンス
このパネルには、デバイスの位置情報レポート、位置情報の適用、ジオフェンス定義を制御する Android ポリシー設定がまとめられています。 Cerberus Enterprise
でデバイスの位置情報を収集する場合や、デバイスが構成済みのエリアに出入りするのを検出する場合に使
用します。

位置情報のレポート

位置情報をレポート

デバイスの位置情報レポートを有効にします。この設定で収集された位置データは、

ダッシュボードの位置情報マップ 、デバイス概要の位置履歴、ジオフェンス処理で使用されます。

位置情報履歴とジオフェンスのイベントは 90日間
保持され、それより古いデータは毎晩自動的に削除されます。登録済みの各デバイスの最新の位置は
常に保持されるため、マップに表示され続けます。

完全には管理されていないデバイスでは、位置データは、 Cerberus Enterprise アプリに必要な位置情報の権限があるかどうか、およびデバイスで位置情報サービスが有効になって
いるかどうかにも依存する場合があります。

個人用 Appleデバイス（ User Enrollment）では、位置情報とジオフェンスはデフォルトでオフです。
Appleポリシーの 個人用デバイスでの位置情報とジオフェンス
がオンになっている場合にのみ利用でき、さらにユーザーが Cerberus Enterprise
アプリの位置情報を許可している必要があります。

位置情報モード

会社所有デバイスのデバイス位置情報設定を制御します。

ユーザーの選択 ：位置情報サービスはポリシーによって制限されません。
強制 ：デバイスで位置情報サービスが有効になります。
無効 ：デバイスで位置情報サービスが無効になります。

位置情報の共有を無効化

仕事用アプリの位置情報共有を無効にします。プロファイル所有者デバイスでは仕事用プロファイルに影響します。完全管理デバイスではデバイス全体の位置情報を無効にし、デバイスの位置情報モードを上書きし
ます。

アクティブなジオフェンスがある場合

の自動動作
アクティブなジオフェンスが機能するには位置情報レポートが必要です。 1
つ以上のジオフェンスがアクティブな場合、 Cerberus Enterprise
は関連する位置情報設定を自動的に整合させます。

アクティブなジオフェンスが存在する間は、 位置情報をレポート が強制的にオンになります。
位置情報モード は強制 に設定されます。
位置情報の共有を無効化 は強制的にオフになります。

1つ以上のジオフェンスがアクティブなときに 位置情報をレポート を無効にしようとすると、 Cerberus Enterprise
は確認ダイアログを表示します。続行すると、ポリシー内のすべてのアクティブなジオフェンスが非アクテ
ィブになります。

ジオフェンスリスト
1つのポリシーには最大 10個のジオフェンス
を含めることができます。ジオフェンス名はポリシー内で一意である必要があります。

新しいエントリを作成するには、 ジオフェンスを追加を使用します。各ジオフェンスには次の主要フィールドがあります：

名前 ：必須で一意である必要があります。
緯度 と経度 ：エリアの中心です。
半径（ m） ：必須で、 200～ 10000メートルの範囲です。
説明 ：管理者向けの任意のメモです。
入場をレポート と退場をレポート ：生成する遷移イベントを選択します。
アクティブ ：ジオフェンスを削除せずに有効または無効にします。

各ジオフェンスでは、 入場をレポート または 退場をレポート の少なくとも 1
つを有効にしておく必要があります。

以前の最小半径は 100メートルでした。 200
メートル未満の既存のジオフェンスは引き続き機能し、ポリシーを保存するときにそのまま維持され
ます（移動または名前変更した場合も同様です）。半径を変更する場合は、 200
メートル以上にする必要があります。

地図編集ツール
各ジオフェンスカードには、エリアの地図プレビューが含まれています。ジオメトリは地図から、または数
値フィールドから編集できます。

エリア編集のロックが解除されているときに、地図をクリックしてジオフェンスの中心を移動しま
す。
現在地 ボタンを使用して、地図を現在のブラウザ位置に合わせます。
地図を再センタリング ボタンを使用して、そのジオフェンスの推奨ビューポートを復元します。
ロックボタンを使用して、ジオフェンスのジオメトリへの偶発的な変更を防ぎます。

ジオフェンスデータが表示される場所

ジオフェンスの遷移は、 Androidのデバイス概要 ページの位置情報パネル内にある ジオフェンスタブで確認できます。このタブでは、専用の地図上に遷移が表示され、フィルタリングツールと遷移リスト
も利用できます。

ユーザー管理

ユーザー追加の無効化
新しいユーザーとプロファイルの追加を無効にするかどうか。 managementMode が DEVICE_OWNER のデバイスでは、このフィールドは無視され、ユーザーはユーザーの追加または削除を許可されません。

アカウント変更の無効化
アカウントの追加または削除を無効にするかどうか。

ユーザー認証情報の構成の無効化
ユーザー認証情報の構成を無効にするかどうか。

ユーザー削除の無効化
他のユーザーの削除を無効にするかどうか。

ユーザーアイコン設定の無効化
ユーザーアイコンの変更を無効にするかどうか。

壁紙設定の無効化
壁紙の変更を無効にするかどうか。

仕事用アカウント設定の認証
仕事用アカウントの設定中にユーザーが認証する方法を制御します。このオプションは、管理対象の Google ドメイン (Google Workspace) に基づく Android エンタープライズでのみ使用できます。

デバイスの設定 /登録時に、このポリシーは仕事用アカウントのサインインが必要かどうかに影響しますが、
Google Admin Console の設定 Google を使用して認証
と登録トークンの種類によっては、引き続き認証が必要になる場合があります。

登録済みのデバイスの場合、このポリシーは、デバイスが管理対象の Google Play
アカウントによって管理されている場合 (つまり、 Google 登録を使用して認証 なしで登録された場合) にのみ適用されます。

詳細とトラブルシューティングについては、 Google 登録を使用して認証 を参照してください。

ブロックされたアカウントの種類

ユーザーが管理できないアカウントの種類。このオプションは、デバイスユーザーが承認されていないアカ
ウントを追加することを防ぎます。

ブロックされたアカウントの種類を追加 を使用して、 1 つ以上のアカウントの種類を追加します。

各エントリには アカウントの種類 フィールド (必須) があります。 com.google
などの文字列を入力します。削除アクションを使用してエントリを削除します。

個人利用

仕事と個人利用のために会社所有デバイスを プロビジョニングする場合、仕事用プロファイル外での個人利用のためにユーザーがデバイスを操作する方法を制限するルールを指定できます。

このセクションは仕事用プロファイルを備えた会社所有デバイスにのみ適用されます。フルマネージ
ドデバイスや個人所有デバイスには影響しません。

1. カメラ無効

カメラが無効かどうか。

2. 画面キャプチャ無効

画面キャプチャが無効かどうか。

3. 仕事オフの最大日数

仕事用プロファイルをオフにできる期間を制御します。

4. Bluetooth 共有

仕事用プロファイルを備えた会社所有デバイスの個人プロファイルで Bluetooth 共有を許可するかどうかを制御します。

5. プライベートスペース

デバイスでプライベートスペースを許可するかどうかを制御します。

6. Play

Play

( )

7.

Play

Play +

7.1.

8.

[redacted]

[redacted]

[redacted] /[redacted]

[redacted]
[redacted]

- [redacted]
  [redacted]
  [redacted]

- [redacted]
  [redacted]

[redacted]

[redacted]
[redacted] /[redacted]
[redacted]
[redacted]

- [redacted]
  [redacted]
  [redacted]

- [redacted]
  [redacted]
  [redacted]

- [redacted] [redacted]

[redacted]

[redacted]
[redacted]

プロファイル間のアプリ機能

個人用プロファイルのアプリが仕事用プロファイルのアプリのアプリ機能を呼び出せるかどうかを制御しま
す。これには Android 16以上が必要です。

この設定は、ポリシーレベルの アプリ機能
オプション（アプリ管理セクション内）に依存します。アプリ機能が 許可しない
に設定されている場合、 APIは許可 に設定されたプロファイル間のアプリ機能を拒否します。

個人用プロファイル内の仕事用連絡先

仕事用プロファイルに保存されている連絡先を、個人用プロファイルの連絡先検索や着信に表示できるかど
うか。

許可（デフォルト）
：仕事用プロファイルの連絡先を個人用プロファイルに表示できるようにします。

許可しない
：個人用アプリが仕事用プロファイルの連絡先にアクセスしたり、仕事用の連絡先を検索したりするこ
とを防ぎます。

システム以外は許可しない ：OEMのデフォルトの電話、メッセージ、連絡先アプリ（ Android 14+
）を除き、ほとんどの個人用アプリが仕事用プロファイルの連絡先にアクセスすることを防ぎます。

個人用プロファイル内の仕事用連絡先が構成されている場合、必要に応じて 除外パッケージ名エントリのリストを定義できます。選択したモードに応じて、これらの除外は個人用アプリの許可リストま
たはブロックリストとして機能します。

ステータスレポート
このセクションでは、デバイスから取得するデータを設定できます。ステータスデータは
デバイスステータス ダッシュボードページで確認できます。

アプリケーションレポート
アプリレポートが有効かどうか。 (インストール済みアプリについて報告される情報です。)

このオプションはシステム (コンパニオンアプリの連携)
で必要であり、常に有効になっています。無効にできません。

削除されたアプリを含める
削除されたアプリをアプリケーションレポートに含めるかどうか。

デバイス設定
デバイス設定のレポートが有効かどうか。 (
デバイス上のセキュリティ関連のデバイス設定に関する情報です。)

ソフトウェア情報
ソフトウェア情報のレポートが有効かどうか。 (デバイスソフトウェアに関する情報です。)

メモリ情報
メモリレポートが有効かどうか。 (メモリとストレージの測定に関するイベントです。)

ネットワーク情報

ネットワーク情報のレポートが有効かどうか。 (デバイスのネットワーク情報です。)

ディスプレイ情報
ディスプレイレポートが有効かどうか。仕事用プロファイルを備えた個人所有デバイスではレポートデータ
を利用できません。 (デバイスのディスプレイ情報です。)

電源管理イベント
電源管理イベントのレポートが有効かどうか。仕事用プロファイルを備えた個人所有デバイスではレポート
データを利用できません。

ハードウェアステータス
ハードウェアステータスのレポートが有効かどうか。仕事用プロファイルを備えた個人所有デバイスではレポートデータを利用できません。

システムプロパティ
システムプロパティのレポートが有効かどうか。

Common Criteria モード
Common Criteria モードのレポートが有効かどうか。

その他

1. イースターエッグゲームの無効化

設定のイースターエッグゲームが無効かどうか。

2. 初回使用時のヒントをスキップ

初回使用時にヒントをスキップするフラグです。エンタープライズ管理者は、アプリが初回起動時にユーザ ーチュートリアルやその他の導入ヒントをスキップするよう、システムの推奨を有効にできます。

3. 短いサポートメッセージ

管理者によって機能が無効にされている設定画面で、ユーザーに表示されるメッセージです。メッセージが 200文字を超える場合、切り捨てられることがあります。

4. 長いサポートメッセージ

デバイス管理者の設定画面でユーザーに表示されるメッセージです。

5. 所有者のロック画面情報

ロック画面に表示するデバイス所有者情報です。

6. セットアップアクション

セットアッププロセス中に実行するアクションです。登録時に、デバイスのセットアップに必要な 1 つ以上のアプリをユーザーに開くよう要求できます。
セットアップアクションを追加 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。

6.1. アプリを起動

起動するアプリのパッケージ名

6.2. タイトル

アプリの起動が必要な理由をユーザーに説明する、ユーザー向けメッセージを提供します。

6.3. 説明

アプリの起動が必要な理由をユーザーに説明する、ユーザー向けメッセージを提供します。

7. エンタープライズ表示名の可視性

デバイスでエンタープライズ表示名を表示するかどうかを制御します（例：会社所有デバイスのロック画面
メッセージとして）。
表示（デフォルト） ：デバイスでエンタープライズ表示名が表示されます（ Android 7 以降の仕事用プロファイルと Android 8以降の完全管理デバイスでサポートされます）。
非表示 ：デバイスでエンタープライズ表示名が非表示になります。

コンプライアンス ルール
デバイスまたは仕事用プロファイルが以下に示すポリシー設定のいずれかに準拠していない場合、 Android Device Policy はデフォルトで直ちにデバイスまたは仕事用プロファイルの使用をブロックします：

パスワード要件
暗号化ポリシー
キーガード無効
許可された入力方式
許可されたアクセシビリティサービス

デバイスまたはワーク プロファイルが 10 日経ってもコンプライアンス違反のままである場合、 Android Device Policy はデバイスを工場出荷時設定にリセットするか、ワーク プロファイルを削除します。

このセクションでは、デフォルトのコンプライアンス適用ルールを上書きしたり、新しいルールを追加した
りできます。

ルール

特定のポリシーをデバイスに適用できない場合の動作を定義するルールのリストです。

ルールを追加 を使用して新しいルールを作成します。各ルールカードは削除アクションで削除できます。

設定名

適用する最上位のポリシーです。たとえば、 アプリケーション やパスワード要件 などです。

必須。
値はサポートされている最上位のポリシー名と一致する必要があります。一致しない場合、フィールドは無
効としてマークされます。

ブロックまでの日数

デバイスまたは仕事用プロファイルがブロックされるまでにポリシーが準拠しない日数です。即座にアクセ
スをブロックするには、 0 に設定します。 ブロックまでの日数 はワイプまでの日数
より短くする必要があります。会社所有のデバイスにのみ適用されます。

許容範囲: 0～300。

ブロックスコープ

ブロックアクションのスコープを指定します。会社所有のデバイスにのみ適用されます。

デフォルト (新しいルール)：仕事用プロファイル 。

仕事用プロファイル
：ブロックアクションは仕事用プロファイルのアプリにのみ適用されます。個人プロファイルのアプリ
は影響を受けません。

デバイス全体
：ブロックアクションは、個人プロファイルのアプリを含むデバイス全体に適用されます。

ワイプまでの日数

デバイスまたは仕事用プロファイルがワイプされるまでにポリシーが準拠しない日数です。
ワイプまでの日数 はブロックまでの日数
より長くする必要があります。会社所有のデバイスにのみ適用されます。

必須。 デフォルト (新しいルール)： 1。

許容範囲: 1～ 300。

工場出荷時リセット保護を保持

デバイスで工場出荷時リセット保護データを保持するかどうか。この設定は仕事用プロファイルには適用されません。

デフォルト (新しいルール)：有効。