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。

Revision #59
Created 2025-12-17 10:39:32 UTC by Admin
Updated 2026-11-12 09:55:53 UTC by Admin