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。

Revision #59
Created 2025-12-17 10:39:33 UTC by Admin Updated 2026-11-12 09:55:55 UTC by Admin