??????

[illegible]

???????????????

[illegible]

[illegible] :

- [illegible] **OS**: Play Integrity API [illegible] OS [illegible] basicIntegrity [illegible] ctsProfileMatch [illegible]
- [illegible] **OS** [illegible] Play Integrity API [illegible] OS [illegible] basicIntegrity [illegible]
- [illegible] Play Integrity API [illegible] MEETS_STRONG_INTEGRITY [illegible]

[illegible]

- [illegible] **(** [illegible] **)**: [illegible] ([illegible]) [illegible]
- [illegible]

[illegible]

- [illegible] : [illegible] Factory Reset Protection (FRP) [illegible]
- [illegible] : [illegible] SD [illegible]

eSIM :
eSIM
eSIM ADD_ESIM eSIM
eSIM

1. ??????????

0

2. ?????????

AC : AC

USB : USB

:

3. ???????????????

true /

4. ????????

/

4.1. ??

パスワード要件が適用される範囲。

自動
：適用範囲は未定です。パスワード要件は、デバイスのワークプロファイルに対して適用され、完全に
管理された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　：パスワードの要件は、デバイスのワークプロファイルに対してのみ適用されます。

職場用プロファイル　：パスワードの要件は、職場用プロファイルにのみ適用されます。

4.2. ??????????????

パスワードの保存履歴の長さ。この値を設定すると、ユーザーは保存履歴にあるパスワードと同一の新しい
パスワードを設定できなくなります。値を　0にすると、制限はなくなります。

4.3. ????????????????????????????

デバイスをワイプする前に許容される、誤ったデバイスのロック解除パスワードの入力回数。　0
を指定すると、制限はなくなります。

4.4. ????????????????????

この設定により、ユーザーは指定された日数ごとにパスワードを定期的に更新する必要があります。

4.5. ????????????????????

強力な認証方法（パスワード、　PIN
、パターンなど）を使用してデバイスまたはワークプロファイルをロック解除した後、一定期間は、指紋認
証や信頼エージェントなど、他の認証方法でもロック解除が可能になります。指定された期間が経過すると
、デバイスまたはワークプロファイルのロック解除には、強力な認証方法のみが使用できます。

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設定に設定されています。

毎日：タイムアウト期間は　24時間に設定されています。

4.6. ????????

必要なパスワードの強度。

複雑さのレベルが高い　：Android 12 以降では、繰り返しのない　(4444) または順序のある　(1234,
4321, 2468) シーケンスを含む　PIN、または長さが　8 文字以上の英字、または長さが　6
文字以上の英数字のパスワードを、高強度パスワードとして定義します。

中程度の強度　：中程度のパスワード強度として、以下のものを定義します。繰り返しのない（　4444
）または順序のある（　1234、4321、2468）数列を含む　PIN、または英字のみで構成され、長さが　4
文字以上、または英数字で構成され、長さが　4文字以上のパスワード。

パスワードの強度（低）

：低強度のパスワードとして、以下のものを定義します。パターン、または、繰り返しのない（ 4444 ）または順序のある（ 1234、4321、2468）数列を含む PIN。

なし：パスワードに関する要件はありません。

脆弱

：デバイスは、最低でも、セキュリティレベルの低い生体認証技術で保護する必要があります。これには、個人を特定できる技術が含まれ、おおよそ 3桁の PINコードと同程度の精度が必要です（誤検出は 1,000回に 1回未満）。

任意の ：パスワードは必須ですが、パスワードの内容に関する制限はありません。

数字：パスワードには、数字を含める必要があります。

数値の組み合わせ ：パスワードには、繰り返しのない（例: 4444）および順序がついていない（例: 1234、4321、2468）数字の組み合わせ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）の文字を含める必要があります。

英数字

：パスワードには、数字とアルファベット（または記号）の両方の文字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。例えば、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. ?????

許可される最小パスワードの桁数。 0を指定すると、桁数制限はなくなります。

4.8. ??????

パスワードに必要な最小文字数。

4.9. ??????????????????

パスワードに必要な小文字の最小文字数。

4.10. ??????????????????

パスワードに必要な大文字の最小文字数。

4.11. ???????????????????????

パスワードに必要な英数字以外の文字（数字または記号）の最小数。

4.12. ???????????

パスワードに必要な最小の数字の桁数。

4.13. ??????????

パスワードに必要な最小限の文字数。

4.14. ?????

Android 9

以降の、ワークプロファイルが設定されたデバイスにおいて、デバイスとワークプロファイルに対して、統合ロックを許可するかどうかを設定します。その他のデバイスには影響しません。

統合ロックの許可　　：デバイスとワークプロファイルに対して、共通のロックを使用できます。

個別のロックを必須とする
：ワークプロファイルに対して、個別のロックを設定する必要があります。

5. ??????????????????????

設定からの工場出荷状態へのリセットが無効になっています。これは、完全に管理対象のデバイスでのみ適用されます。

6. ???????????????

工場出荷状態への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。デバイスが許可されていない工場出荷状態のリセットを受けた場合、デバイスのロックを解除するには、これらの管理者の一人が、

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する必要があります。管理者が指定されていない場合、工場出荷状態へのリセット保護は機能しません。完全に管理対象のデバイスでのみ有効です。

管理者メールアドレス　　：工場出荷時設定保護を有効にする
を使用して、管理者設定を開始します。その後、　　管理者メールアドレスの追加
を使用してアドレスを追加し、削除アクションを使用して削除します。

7. ???????????

無効にできるキーガード（ロック画面）の機能。

7.1. ?????????

現在のおよび将来の、すべてのキーガードのカスタマイズを無効にします。

7.2. ??????????

セキュアなロック画面（例: PIN）でのカメラ利用を無効にする。

7.3. ?????????

セキュアなロック画面で、すべての通知を表示しないように設定します。

7.4. ??????????????????????????

セキュリティキーガード画面での、内容を隠さない通知を無効にします。

7.5. ???????????????????

セキュアなキーガード画面での信頼エージェントの状態を無視します。

7.6. ???????????

セキュアなキーガード画面での指紋認証を無効にする。

7.7. ???????????????????

セキュアなキーガード画面での通知へのテキスト入力機能を無効にする。

7.8. ????????????

セキュアなロック画面での顔認証機能を無効にします。

7.9. ???????????????

セキュアなロック画面での虹彩認証機能を無効にします。

7.10. ????????????????

セキュアなロック画面でのすべての生体認証を無効にします。

7.11. ???????????????????

Android 14 以降の、セキュアなキーガード画面上のすべてのショートカットを無効にします。

Revision #38
Created 2025-12-17 10:39:33 UTC by Admin
Updated 2026-04-22 15:51:33 UTC by Admin