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。

Revision #18
Created 2026-06-24 08:08:36 UTC by Admin
Updated 2026-11-12 09:55:57 UTC by Admin