ネットワーク

Apple ポリシーエディタの ネットワーク セクションでは、デバイスの Wi-Fi ネットワークと VPN を構成し、証明書をインストールし、AirDrop や Bluetooth などの接続機能を制限します。各 Wi-Fi ネットワーク、VPN、証明書はそれぞれ独自の構成プロファイルとしてインストールされ、デバイスの 設定 > 一般 > **VPN** とデバイス管理（Mac: システム設定 > 一般 > デバイス管理、または macOS 13 および 14 では プライバシーとセキュリティ > プロファイル）と、デバイスページの プロファイル、証明書、セキュリティ パネルで確認できます。

> 証明書は 証明書 ページから取得します。先にそこでインポートしてください。ポリシーは証明書を参照するだけなので、証明書がポリシーにコピーされることはありません。

制限

- **AirDrop**を許可
- **AirPlay**の受信リクエストを許可
- **Bluetooth**の変更を許可
- **Bluetooth**共有の変更を許可
- ファイルのネットワークドライブアクセスを許可
- インターネット共有の変更を許可
- コンテンツ キャッシュを許可
- **iTunes** ファイル共有を許可

Wi-Fi ネットワーク

Wi-Fi ネットワークを追加 をクリックし、次を入力します :

- ネットワーク名 **(SSID)**: ネットワークの名前で、最大 32 文字です。
- セキュリティ : なし（オープンネットワーク）、WEP、WPA または WPA2、WPA2 または WPA3、WPA3 のみ、または任意。
- パスワード : パーソナルネットワークのパスワード。
- 自動的に接続 と 非表示ネットワーク（名前をブロードキャストしないネットワーク用）。
- プロキシ : なし、手動（サーバーとポート）、または自動（PAC ファイルの URL。空にすると WPAD でネットワーク上の設定を検索します）。
- プロファイル名 （任意）と 適用先 で、ネットワークを一部のデバイスの種類に限定します。

エンタープライズネットワーク (802.1X)
ユーザーが共有パスワードではなく、自身の認証情報または証明書で認証する場合は、 エンタープライズ (802.1X)をオンにします。

認証: PEAP、TTLS(内部認証あり。たとえば MSCHAPv2)、または TLS(証明書のみ)。
デバイスユーザーの認証情報 : 各デバイスは、ユーザーページで設定されたそのユーザーの EAP
ID、匿名 ID
、パスワードを使用します。ユーザーのないデバイスには、このネットワークは適用されません。
ID、匿名 ID、パスワード : すべてのデバイスで共通です。 ID には変数 $EMAIL$、$USERNAME$
、 $FULLNAME$、$SERIAL$、$UDID$
を含めることができます。パスワードを空にすると、ユーザーがデバイスで入力します。
ID 証明書: デバイスが提示するクライアント証明書です (TLS では必須)
。以下の証明書オプションを参照してください。
信頼された証明書 : RADIUS サーバーの証明書を発行した CA
証明書です。ネットワークとともにインストールされます。
信頼されたサーバー名 : デバイスが受け入れる RADIUS サーバー証明書の名前です (たとえば
radius.example.com や *.example.com)。

VPN

VPN を追加 をクリックして、 iOS、iPadOS、 macOS に組み込まれている IKEv2 または Cisco IPSec VPN
を構成します (VPN アプリは不要です)。

種類 とサーバー 。 IKEv2 の場合はさらに リモート ID(サーバーの ID
。空の場合はサーバーアドレス)とローカル IDも指定します。ローカル ID には変数 $EMAIL$、
$USERNAME$、$FULLNAME$、$SERIAL$、$UDID$ を含めることができます。
デバイスの 認証: 証明書 (証明書ページのもの、デバイスユーザーの証明書、または SCEP
サーバーから要求したもの)、共有シークレット (IPSec の場合は任意のグループ名付き)
、またはユーザー名とパスワードのみを確認する IKEv2 サーバーの場合はなし。
信頼された証明書 : VPN サーバーの CA 証明書で、 VPN とともにインストールされます。 IKEv2 では、期待されるサーバー証明書の発行者と名前も設定できます。
ユーザー名とパスワード : ユーザーはユーザー名 (変数使用可)とパスワード (IKEv2 では EAP、
IPSec では XAuth)
でも認証します。パスワードを空にすると、ユーザーがデバイスで入力します。
VPN 名 (設定に表示されます)と適用先 。

接続

ユーザーが設定で接続 : VPN がインストールされ、ユーザーが必要に応じてオンにします。
オンデマンド : デバイスが自動的に VPN に接続します。 信頼された Wi-Fi を除く
を指定すると、リストした Wi-Fi ネットワーク (たとえばオフィスのネットワーク)では VPN

が使用されません。
常時接続 (IKEv2、監視対象の iPhone と iPad のみ): 携帯回線と Wi-Fi のすべてのトラフィックが
VPN を経由し、ユーザーはオフにできません。他のデバイスにはこの VPN は適用されません。
VPN でユーザー名を使用する場合、パスワードをポリシーで設定する必要があります。
アプリごとの VPN: 一部のアプリのみが VPN を使用します。 アプリ管理
セクションでアプリごとに VPN を選択し (アプリの VPNフィールド、 Mac では使用できません)
、必要に応じて VPN を使用する Safari ドメインをリストします。

常時接続またはオンデマンド VPN
は、先にテスト用デバイスでテストしてください。サーバーに到達できない場合、デバイスが接続で
きなくなる可能性があります。

グローバルプロキシ、暗号化 DNS、 Web コンテンツフィルタ
これらの設定はデバイスのすべてのトラフィックに適用されます。各切り替えでオンにします。

グローバル HTTP プロキシ (監視対象の iPhone と iPad、 Mac): すべての HTTP
トラフィックが、すべてのネットワークでプロキシを経由します。サーバーとポート (
任意のユーザー名とパスワード付き)、または自動構成 (PAC ファイルの URL
。空にするとネットワーク上で検索)を設定します。 Wi-Fi ログインページを許可
をオンにすると、ユーザーはプロキシを使わずに公共 Wi-Fi ネットワークにサインインできます。
暗号化 DNS: デバイスは DNS over HTTPS(サーバー URL)または DNS over TLS(サーバー名)
で、お使いの DNS
サーバーを使用して名前を解決します。必要に応じて一部のドメインのみに限定できます。監視対
象デバイスでは、ユーザーがオフにできないようにできます。
Web コンテンツフィルタ (監視対象の iPhone と iPad): iOS
に組み込まれたフィルタで、常に許可または常にブロックする Web
サイトのリストを使用してアダルトサイトを制限するか、 Web
サイトのリストのみを許可します。許可したサイトは Safari にブックマークとして表示されます。

プロキシまたは DNS
サーバーが誤っていると、デバイスが接続できなくなる可能性があります。先にテスト用デバイスで
設定を試してください。

証明書

証明書を追加 をクリックして証明書を単独でインストールします。 Safari
とアプリが信頼する必要がある認証局、またはアプリが使用する ID です。 Wi-Fi ネットワークや VPN の証明書は、ここで追加する必要はありません。

証明書のオプション

証明書ページの証明書 : すべてのデバイスで同じ証明書です。 証明書を選択
をクリックして選択します。
デバイスユーザーの証明書 :
各デバイスは、そのユーザーにリンクされたクライアント証明書を受け取ります。ユーザーに証明
書がないデバイスには適用されません。ユーザーに別の証明書をリンクすると、デバイスが更新さ
れます。
SCEP サーバーから要求 : 各デバイスが SCEP サーバー (たとえば Microsoft NDES) から独自の証明書を要求するため、秘密鍵がデバイスから出ることはありません。サーバー URL 、サーバーが必要とする場合はチャレンジ、サブジェクト (たとえば CN=$EMAIL$)
、代替名、キーサイズ、キー用途を設定します。

古い RC2 暗号化で保護されたクライアント証明書 (.p12)は、 Apple
デバイスにインストールできません。インポートする前に、 3DES または AES
暗号化で再度書き出してください。

セキュリティ
パスワードや秘密鍵を含むプロファイルは、作成対象のデバイスにのみ送信されます。デバイスは管理証明
書で要求に署名する必要があります。パスワードと証明書はログに記録されません。

Revision #6
Created 2026-11-10 15:16:16 UTC by Admin
Updated 2026-11-12 09:55:46 UTC by Admin