WhatsAppセキュリティチェックリスト

ACTIVIST CHECKLIST

最終更新日： **2026年10月22日**　所要時間の目安： **15分**

このコピーは 2026年11月6日 に作成。 脅威が変化するにつれ、また自分の身を守るより良い方法が利用可能になるにつれ、ガイドを頻繁に更新します。最新バージョンはこちらから。 activistchecklist.org/ja/whatsapp/

自動翻訳: このページは自動翻訳されています。現時点で人によるチェックが済んでいるのはページの0%だけで、それ以外の部分には誤りがあるかもしれません。翻訳のチェックに協力する[1]。

WhatsAppのメッセージはエンドツーエンドで暗号化されていますが、Meta（WhatsAppを所有する企業）は今でも大量のメタデータを警察に渡しています。すでにWhatsAppで組織活動をしているなら（特に移民コミュニティで）、このチェックリストでバックアップ、グループ、AI機能、リンク済みデバイス、通知の設定を固めましょう。リスクの高い政治活動では、センシティブな会話はSignalに移しましょう。

多くのアクティビズムはすでにWhatsApp上で行われています。特に移民コミュニティではその傾向が強いです。最も安全でプライバシーに配慮した選択肢ではありませんが、すでに多くの人が使っていたり、WhatsAppの機能（コミュニティなど）が必要だったりするため、コミュニティの組織活動に役立つツールになることもあります。

WhatsAppのメッセージはエンドツーエンド暗号化されているので、会話の内容を守るという点では、通常のSMSよりも安全です。警察があなたの携帯電話会社に召喚状を出して通常のSMSを要求すると、すべてのメッセージの内容を見ることができます。一方、Metaに召喚状を出してWhatsAppのメッセージを要求しても、内容を見ることはできません（チャットのバックアップを有効にしていない限り）。

Think of doing large group organizing WhatsApp the same way you would social media: Assume that bad actors (government, right-wing) could join and monitor any large-unvetted group just like they could join and monitor large groups on social media. Assume they can also see who is in the group in the same way they could see who is following you on social media.

このガイドの対策をすべて行っても、WhatsAppが常に警察に提出できる情報がいくつかあります：

- あなたの連絡先リスト全体（一度でもアプリに連絡先へのアクセスを許可したことがあれば、後で無効にしても、WhatsAppはずっとそのデータを持ち続けます）
- あなたを連絡先リストに登録している他のすべてのWhatsAppユーザー（出典[2]）
- 参加しているすべてのグループの名前
- 参加しているすべてのグループのメンバー
- どの電話番号といつメッセージをやり取りしているか（この情報はリアルタイム[3]でも取得可能で、これは他のほとんどのテック企業が警察に提供していないものです）
- チャットのバックアップを有効にしている場合、GoogleやAppleが提出を強制される可能性があり、そこにはあなたのメッセージがすべて含まれています。バックアップを安全に使う方法は、WhatsAppのチャットを安全にバックアップするを参照してください。

WhatsAppを使うのは初めて？ WhatsAppの使い方[4]についてはこちらのガイドを参照してください。

WhatsAppの基本的な保護対策

すべての人 このセクションは、アクティビズムや権利擁護に関わるすべての人向けです。

10分しか時間がないなら、ここから始めましょう。

重要 WhatsAppのチャットバックアップをオフにする（連絡先の人たちにも同じことを頼もう）

WhatsAppのバックアップはデフォルトでは暗号化されておらず、裁判所の命令で提出させられる可能性があります。

WhatsAppがiCloudやGoogle Driveに作成するデフォルトのバックアップは、エンドツーエンド暗号化されて**いません**。つまり、裁判所がAppleやGoogleに、あなたのチャット履歴をまるごと提出させることができるということです。メッセージ自体は安全に送信されていても、バックアップがあるとチャット履歴全体が簡単にさらされてしまい、その保護が台無しになります。

バックアップをオフにしておけば、フィッシングや使い回しのパスワードを通じてハッカーにiCloudやGoogleアカウントに侵入された場合にも、身を守れます。

バックアップを完全にオフにする方法

IPHONE

WhatsApp → 下部バーの **You** をタップ → **チャット** → **チャットのバックアップ** → **自動バックアップ** を **オフ** に設定

ANDROID

WhatsApp → ⋮ → **チャット** → **チャットのバックアップ** → **自動バックアップ** を **オフ** に設定

友だちにも伝えよう: 自分のバックアップをしっかり守っていても、チャット相手が暗号化なしでバックアップしているかもしれません。相手のバックアップには、あなたのメッセージも含まれています。連絡先の人たちにも、バックアップを守るよう頼みましょう。このガイドを送ってあげるのもいいかもしれません。

どうしてもバックアップが必要な場合は、WhatsAppのチャットを安全にバックアップするで安全な方法を確認してください。

WhatsAppの最終オンライン時刻とオンライン状態「Last seen & online」を非表示にする

知らない人やグループのメンバーに、WhatsAppを使っているタイミングを追跡されるのを防ぎます。

デフォルトでは、一度でもメッセージをやりとりした相手なら誰でも、あなたが最後にWhatsAppを使った時刻を見ることができます。アクティビストにとって、これは誰かがあなたの活動パターンを簡単に把握できてしまう手段になります。

最終オンライン時刻とオンライン状態を非表示にする方法

IPHONE

WhatsApp → 下部バーの **You** をタップ → **Privacy** → **Last seen & online** → **Nobody** を選択

ANDROID

WhatsApp → ⋮ → **Privacy** → **Last seen & online** → **Nobody** を選択

「Strict Account Settings」をオンにするとこの設定がロックされます。独自の設定にしたい場合は、先に「Last seen」を変更しておきましょう。

WhatsAppで「Strict Account Settings（厳格なアカウント設定）」を有効にする

2段階認証、セキュリティ通知、知らない送信者からのメディアのブロック、リンクプレビューの無効化、知らない相手からの着信の消音を、まとめて一度にオンにできます。

Strict Account Settingsを有効にすると、いくつもの保護機能が一度にオンになります。アクティビズムに関わるすべての人にとって、基本の設定としておすすめです。

STRICT ACCOUNT SETTINGSを有効にする方法

IPHONE

WhatsApp → 下部のバーで **You** をタップ → **Privacy** → **Advanced** → **Strict account settings** → **Next** → **Turn on**

ANDROID

WhatsApp → ⋮ → **Privacy** → **Advanced** → **Strict account settings** → **Next** → **Turn on**

Strict Account Settingsを使わずに、各設定を個別に有効にしたい場合の手順はこちら

これが必要なのは、上で紹介したワンタップのStrict Account Settingsを使わずに、設定を一つずつ選びたい場合だけです。すでにStrict Account Settingsを有効にしているなら、ここは飛ばしてOKです。

- **2段階認証。** WhatsApp → **Privacy** → **Advanced** → **Two-step verification** → PINを設定
- **セキュリティ通知。** WhatsApp → **Privacy** → **Advanced** → **Security notifications** → オンにする
- **知らない送信者からのメディアをブロック。** WhatsApp → **Privacy** → **Advanced** → **Block media from unknown contacts** → オンにする
- **リンクプレビューを無効化。** WhatsApp → **Privacy** → **Advanced** → **Disable link previews** → オンにする
- **知らない相手からの着信を消音。** WhatsApp → **Privacy** → **Calls** → **Silence unknown callers** → オンにする
- **プロフィールの公開範囲を連絡先のみに制限**（最終オンライン、自己紹介、プロフィール写真、ステータス）。 WhatsApp → **Privacy** → それぞれを **My Contacts** または **Nobody** に設定

2段階認証のPINは、パスワードマネージャー[5]など安全な場所に忘れずに保存しておきましょう。PINをなくすと、自分のアカウントにログインできなくなる可能性があります。

WhatsAppで消えるメッセージをデフォルトでオンにする

誰かのスマホが押収されたり侵入されたりしたときに、あなたと連絡相手を守ります。

消えるメッセージをデフォルトでオンにしておけば、万が一スマホが押収されたり侵入されたりしても、あなたと連絡相手の安全を守りやすくなります。誰のスマホが警察に押収されるかはわかりません。まったく合法なことを話しているつもりでも、政府はあなたの言葉をねじ曲げる方法を見つけてきます。

WhatsAppで選べる期間は24時間、7日間、90日間です。デフォルトには7日間がおすすめ。そのうえで、よりセンシティブな会話では手動で短い期間に設定しましょう。

消えるメッセージをデフォルトでオンにする方法

IPHONE

WhatsApp → 下部のバーで **あなた** をタップ → **プライバシー** → **デフォルトのメッセージタイマー** → 期間を選ぶ

ANDROID

WhatsApp → ⋮ → **プライバシー** → **デフォルトのメッセージタイマー** → 期間を選ぶ

デフォルトのタイマーが適用されるのは、**自分から始めた新しいチャット**だけです。相手からスレッドを始めた場合、タイマーは適用されません。既存のスレッドで設定するには、チャットを開く > 上部の名前をタップ > **消えるメッセージ** を選びます。

WhatsAppで継続的に行うセキュリティ習慣

すべての人　このセクションは、アクティビズムや権利擁護に関わるすべての人向けです。

ソーシャルメディアに投稿できないようなことは、WhatsAppでも共有しない

WhatsAppは大人数を動員するのには向いているけれど、リスクの高い計画には向いていません

DO: WhatsAppは大規模な動員に使う（ソーシャルメディアと同じような使い方で）

DO NOT: ICE監視のシフト、選挙防衛、直接行動の計画をWhatsAppで立てる

政治的・戦略的な話題についてのやりとりは、極右勢力に監視されているかもしれないことを忘れずに。特に、大規模な連絡や動員に使うグループやチャンネルでは、誰が参加するかを完全にはコントロールできないので要注意です。

ソーシャルメディアで公開できないようなことは、WhatsAppでも言わないようにしましょう。

信頼できる仲間とセンシティブな行動を計画するなら、Signal[6]を使いましょう。

WhatsAppでMeta AIと「チャット」しない

組織活動や連絡先、計画についてMeta AIに尋ねた内容はすべて保存され、警察の手に渡るおそれがあります。

アクティビストにとって、Meta AIは便利なアシスタントを装ったデータ収集機能です。組織活動や連絡先、居場所、計画について尋ねた内容はすべて保存され、プロファイリングに使われ、警察の手に渡る可能性もあります。

グループチャットで@MetaAIをタグ付けすると、前後のメッセージがMetaのシステムに取り込まれます。ちょっとした質問をするつもりだっただけでも、です。 Meta AIが会話に加わった時点で、そのやり取りの履歴はもうチャット参加者だけのものではなくなります。

WhatsAppでMeta AIを完全に無効にすることはできません。いちばんの対策は、絶対に使わないこと、そしてグループチャットで **@MetaAI** を絶対にタグ付けしないことです。

特定のチャットやグループからMeta AIを締め出すには、それらのチャットでRestricted chatもオンにしましょう。

「リンク済みデバイス」でペアリングコードを入力したり、QRコードをスキャンしたりしない

攻撃者はあなたをだまして、自分のブラウザをあなたのアカウントにペアリングさせます。そうなると、チャットに完全にアクセスされてしまいます。

DO: WhatsAppのQRコードをスキャンするのは、WhatsApp Webまたはデスクトップ版を「自分で」開いたときだけにする

DO NOT: ウェブサイトや誰かに頼まれて、ペアリングコードを入力したりQRコードをスキャンしたりする

「リンク済みデバイス」とは？ WhatsAppでは、QRコードやペアリングコードでリンクすることで、ほかのデバイス（パソコン、タブレット、別のスマホなど）でも自分のアカウントを使えます。ほとんどの人はこの機能を一度も使いません。詳しく知りたい場合は、WhatsAppの公式解説[7]を見てください。

攻撃者は、あなたをだまして**自分たちの**デバイスをあなたのアカウントにリンクさせられることに気づいています。ウェブサイトや知らない人が、WhatsAppにコードを入力させる「認証」の手順を案内してきたら、それは認証ではありません。それは、あなた自身が相手にチャットへの完全なアクセスを渡してしまうということです。 QRコードでも同じ手口が使われます。

だからこそ、**ウェブサイトや誰かに頼まれて、ペアリングコードを入力したりWhatsAppのQRコードをスキャンしたりは絶対にしないこと。** WhatsAppのQRコードをスキャンするのは、**自分自身で**WhatsApp Webまたはデスクトップ版を開いた直後だけにしましょう。

自分のアカウントはいつでもチェックできます。リンク済みデバイスを定期的に確認するを参照してください。

WhatsAppのPINや6桁の認証コードは絶対に誰にも送らない

「WhatsAppサポート」を名乗る相手であっても同じです。アカウントの乗っ取りはこうして起こります。

WhatsAppのPINと、WhatsAppからSMSで届く6桁の認証コードは、あなたのアカウントの鍵です。これを手に入れた人は、誰でもアカウントを乗っ取れてしまいます。

どんな理由があっても、これらのコードは誰にも教えないでください。相手が「WhatsAppサポート」や「WhatsAppセキュリティ」を名乗っていても同じです。 WhatsAppがDMや電話、SMSでPINや認証コードを聞いてくることは絶対にありません。もし誰かに聞かれたら、それはフィッシングです。

「WhatsAppサポート」を名乗り、この手口でアカウントを乗っ取ろうとする偽メッセージが増えています。メッセージが本物かどうかわからないときは、返信せず、リンクもタップせず、コードも入力しないでください。代わりに、アプリ内の**ヘルプ**からWhatsAppに問い合わせましょう。

WhatsAppの強化された保護対策

中程度の脅威 このセクションは、リーダー的な役割を担っている人や、国家や対立勢力から標的にされやすい運動分野に関わっている人向けです。

WhatsAppの重要なチャットやグループでは「Restricted chat」（制限付きチャット）をオンにする

そのチャットでのMeta AI、チャットのエクスポート、カメラロールへのメディアの自動保存、WhatsApp Webなどのリンク済みデバイスからのアクセスをブロックします。

Restricted chatは、チャットごとに設定するものです。オンにすると、そのチャットのメンバーは誰も次のことができなくなります：

- チャットをエクスポートする
- チャット内の写真や動画を自分のカメラロールに自動保存する
- チャット内でMeta AIの機能を使う
- WhatsApp Web、WhatsApp Desktop、タブレットなどのリンク済みデバイスでチャットを開く

> **Restricted chatにしたチャットは、パソコンには表示されません。**オンにすると、あなたもチャットの他のメンバーも、そのチャットのメッセージはメインのスマホでしか読んだり送ったりできなくなります。チャットのメンバー全員にとって、そのチャットはWhatsApp Desktop、WhatsApp Web、タブレットでは使えなくなります。

これは、AIエージェントや非公式のWhatsAppアプリをチャットから締め出すための機能です。こうしたツールは、リンク済みデバイスとして誰かのWhatsAppアカウントに接続します。グループの誰か一人でもこうしたツールを接続していれば、そのツールはその人のアカウントにあるすべてのチャットを読めてしまいます。あなたのグループのチャットも含めてです。 Restricted chatをオンにすれば、そのチャットはこうしたツールから読めなくなります。攻撃者がチャットのメンバーをだまして、攻撃者のデバイスをその人のアカウントにリンクさせた場合にも役立ちます（WhatsAppのリンク済みデバイス一覧を定期的に確認するを参照）。

重要なチャットごとに、それぞれオンにする必要があります。すべてのチャットに自動で設定することはできず、変更できるのはメインのスマホからだけです。

RESTRICTED CHATをオンにする方法

1対1のチャットの場合（どちらの人でもオンにできます）：

IPHONE

チャットを開く → 上部の連絡先の名前をタップ → **Restricted chat** → オンに切り替える

ANDROID

チャットを開く → ⋮ → **連絡先を表示** → **Restricted chat** → オンに切り替える

グループの場合（オンにできるのはグループ管理者だけです）：

グループを開く → 上部のグループ名をタップ → **Restricted chat** → オンに切り替える

管理者でない場合は、グループの管理者にオンにしてもらうよう頼みましょう。

すでに「高度なチャットプライバシー」（ADVANCED CHAT PRIVACY）をオンにしている場合

制限付きチャットは、以前の「高度なチャットプライバシー」という設定に代わる機能です。「高度なチャットプライバシー」をオンにしていたチャットは、**自動的には制限付きチャットに切り替わりません。**アップグレードするまでは、リンク済みデバイスでも引き続き開けてしまいます。

チャットを開く → 上部のチャット名をタップ → **高度なチャットプライバシー** → **アップグレード** → **続行**

> 制限付きチャットが完全に機能するのは、チャットの参加者全員がWhatsAppの最新バージョンを使っている場合だけです。古いバージョンを使っている人がいると、リンク済みデバイスや非公式アプリ、AIエージェントでチャットが読めてしまう可能性があり、しかもWhatsAppはそれを知らせてくれません。センシティブな内容を扱うグループでは、参加者全員にWhatsAppを最新の状態に保つよう呼びかけましょう。また、スクリーンショットを撮られたり、個別のメッセージを転送されたりするのを防ぐことはできません。

WhatsAppで写真や動画がカメラロールに自動保存されないようにする

センシティブな画像が、召喚状（subpoena）で提出を求められうるiCloudやGoogleフォトのバックアップに入らないようにします。

WhatsAppで受け取った写真や動画は、思っている以上にいろいろな場所に残ってしまうことがあります。初期設定のままだと、WhatsAppがそれらをそのままカメラロールに保存し、さらにiCloudやGoogleフォトが自動でクラウドにバックアップしてしまう場合があります。

つまり、センシティブな画像（抗議行動の映像、オーガナイザーの写真など、コミュニティを危険にさらしうるもの）やそのメタデータ（撮影場所や撮影時刻など）が、GoogleやAppleのアカウントに残り、警察が召喚状（subpoena）で提出を求めることができる状態になってしまうということです。そうなると、後からすべてのコピーを削除するのはずっと難しくなります。

すべてのチャットで自動保存をオフにする方法

IPHONE

WhatsApp → **設定** → **チャット** → **カメラロールに保存**をオフにする

ANDROID

WhatsApp → **設定** → **チャット** → **メディアの表示**をオフにする

特定のチャットやグループで自動保存をオフにする方法

IPHONE

チャットを開く → 上部のチャット名をタップ → **カメラロールに保存** → **デフォルト**、**常に**、**しない**のいずれかを選ぶ

ANDROID

チャットを開く → 上部のチャット名をタップ → **メディアの表示** → **デフォルト**、**はい**、**いいえ**のいずれかを選ぶ

WhatsAppのプロフィールに本名や自分の写真を使わない

あなたの匿名性を暴こうとする警察や攻撃者から身を守るのに役立ちます。メンバーの身元が確認されていないWhatsAppグループに参加している場合は特に有効です。

コミュニティの組織活動の多くは、WhatsAppの身元確認がされていないグループで行われています。そうしたグループでは、メンバー全員をどこまで信頼できるのかわかりません。こうしたグループには、右派の敵対者[8]や警察[9]が潜入してくることがあります。

偽名やファーストネームだけを使えば、Google検索であなたの本当の身元を突き止められるのを防げます。自分の顔以外の写真を使えば、画像検索や顔認識であなたのSNSアカウントを見つけられるのを防げます。どちらのステップも、ドクシング[10]やネット上の嫌がらせから身を守るのに役立ちます。

WhatsAppで完全に匿名でいるのはとても難しいです。メッセージを送った相手や同じグループのメンバー全員に、あなたの電話番号が見えてしまうからです。グループに悪意のある人がいれば、あなたの電話番号を使って簡単に身元を特定[10]できてしまいます。WhatsAppのユーザー名を設定すれば、まだあなたの番号を知らない人には番号が表示されなくなります。

プロフィールの表示名を変更する方法

IPHONE

WhatsApp → 下部バーの **You** をタップ → 自分の名前をタップ → もう一度名前をタップ → 偽名またはファーストネームだけに変更 → **保存** をタップ

ANDROID

WhatsApp → ⋮ → **設定** → 上部の自分の名前をタップ → もう一度名前をタップ → 偽名またはファーストネームだけに変更 → **保存** をタップ

プロフィール写真を変更する方法

IPHONE

WhatsApp → 下部バーの **You** をタップ → プロフィール写真をタップ → プロフィール写真の下の **編集** をタップ → ネットで見つけた、あなたの身元・好み・趣味・居場所と関係のない一般的な写真をアップロード

ANDROID

WhatsApp → ⋮ → **設定** → プロフィール写真をタップ → プロフィール写真の下の **編集** をタップ → ネットで見つけた、あなたの身元・好み・趣味・居場所と関係のない一般的な写真をアップロード

グループの仲間にも、同じ対策をするよう声をかけましょう。セキュリティはチーム戦です。

- [ ] **WhatsAppのどのチャットでもライブ位置情報を共有していないか確認する**
  ライブ位置情報の共有は、うっかりオンのままになっていることがあります。自分の動きをチャットに流し続けてしまわないよう、ときどきチェックしましょう。

WhatsAppでは、リアルタイムの位置情報を特定の人やグループと一定時間共有できます。簡単にオンにできる分、そのまま忘れてしまいがちです。特に何時間も前に共有を始めた場合はなおさら。

アクティビストにとって、ライブ位置情報の共有をオンにしたままにするのは、チャットにいる誰もが見られる「自分の行動マップ」を差し出しているのと同じです。

ライブ位置情報の共有を確認・停止する方法

IPHONE

WhatsApp → **設定** → **プライバシー** → **ライブ位置情報** → 一覧を確認し、不要になったものはすべて **共有を停止** をタップ

ANDROID

WhatsApp → ⋮ → **設定** → **プライバシー** → **ライブ位置情報** → 一覧を確認し、不要になったものはすべて **共有を停止** をタップ

- [ ] **WhatsAppのチャットを安全にバックアップする（どうしてもバックアップが必要な場合のみ）**
  どうしてもバックアップが必要なら、WhatsAppのエンドツーエンド暗号化バックアップをオンにしましょう。そうすればGoogleやAppleがデータを引き渡すことはできません。

いちばん安全なのは、バックアップを完全にオフにしておくこと（WhatsAppのチャットバックアップを無効にするを参照）。バックアップをオンにするのは、本当に必要なときだけにしましょう。たとえば、機種変更をするときや、国境を越えるために一時的にWhatsAppを削除する必要があるときなどです。

バックアップが必要な場合は、WhatsAppに組み込まれているエンドツーエンド暗号化バックアップをオンにしてください。これをしないと、GoogleやAppleが警察にチャット履歴をまるごと引き渡すよう強制されるおそれがあります。

暗号化バックアップをオンにする方法

IPHONE

WhatsApp → 下部のバーで **You** をタップ → **Chats** → **Chat Backup** → **End-to-end encrypted backup** → パスキーまたはパスワードを設定

ANDROID

WhatsApp → ⋮ → **Chats** → **Chat Backup** → **End-to-end encrypted backup** → パスキーまたはパスワードを設定

パスワードはパスワードマネージャー[5]に保存しましょう。 WhatsAppはパスワードを復元してくれません。

iPhoneのみ: WhatsAppの暗号化バックアップに加えてさらに保護を強化したい場合は、Appleの **iCloudの高度なデータ保護** をオンにすることもできます。これはiCloud全体に適用される別の設定で、iCloudアカウント内のほとんどのデータをエンドツーエンドで暗号化します。

グループのオーガナイザー・管理者向け

中程度の脅威 このセクションは、リーダー的な役割を担っている人や、国家や対立勢力から標的にされやすい運動分野に関わっている人向けです。

組織活動のグループを運営しているなら、個人の設定と同じくらい、グループ自体の設定も重要です。

☐ WhatsAppの組織活動グループの守りを固めよう

グループのプライバシーは、いちばんセキュリティの弱いメンバーと同じ強さにしかならない。

組織活動のグループを運営しているなら、個人の設定と同じくらい、グループ自体の設定も重要です。

グループチャットのプライバシーは、いちばんセキュリティの弱いメンバーと同じ強さにしかなりません。誰か一人が潜入者だったり、デバイスが乗っ取られていたりすれば、チャットの内容がすべて漏れてしまう可能性があります。グループ全体でルールを守れるよう、お互いにサポートし合いましょう。

グループ設定の守りを固める方法

おすすめのグループ設定:

- [ ] **グループ作成時から消えるメッセージをオンにする。** グループが許容できる範囲で、いちばん短い期間を選びましょう。
- [ ] グループで**制限付きチャットをオンにする**（管理者のみ設定できます）。これにより、チャットのエクスポートが無効になり、メディアがメンバー全員のカメラロールに自動ダウンロードされなくなり、Meta AIがチャットに入れなくなります。さらに、リンク済みデバイスをブロックすることで、AIエージェントや非公式アプリも締め出せます。このグループはスマホでしか使えず、WhatsAppのデスクトップ版やWeb版では使えないことをメンバーに伝えておきましょう。以前に旧設定の「チャットの高度なプライバシー」をオンにしていた場合は、自動では切り替わらないので、制限付きチャットにアップグレードしましょう。
- [ ] **グループを招待制にする。** グループのスレッドを開く → グループ名をタップ → **グループの権限** → グループ情報の編集、メンバーの追加、メッセージの送信ができる人を制限する。
- [ ] **グループのルールを最初に決めておく:** クラウドバックアップはしない、リスクの高いアクションについてはWhatsAppで話さない、承認なしに新しい人を追加しない、など。新しく入るメンバー全員にこのルールに同意してもらい、既存のメンバーにも定期的にリマインドしましょう。
- [ ] **グループのニーズとリスク許容度に合った審査の方法を決める。** グループが大きいほど、潜入されやすくなります。

- [ ] **WhatsAppのコミュニティ機能を使って、グループメンバーの電話番号を非公開にする**
  コミュニティではメンバー同士の電話番号が非表示になるので、大規模なグループや、全員の身元を確認しきれていないグループで組織活動をするときに役立ちます。

WhatsAppには**コミュニティ**という比較的新しい機能があり、複数のサブグループをまとめる親グループを作ることができます。

オーガナイザーにとってのメリットは、コミュニティに「電話番号のプライバシー」機能があること。これにより、メンバー同士がお互いの電話番号を見られなくなります。

> コミュニティの電話番号のプライバシー機能には限界があります。グループの管理者には引き続きあなたの電話番号が見えますし、すでに連絡先にあなたの番号を保存している人にも見えてしまいます。

WhatsAppで大規模な組織活動のグループを運営しているなら、コミュニティへの移行を検討してみてください。他のメンバーや潜入者によってメンバーがドクシング[10]されるリスクを減らせます。

リスクの高いアクティビストのための保護対策

高い脅威 このセクションは、知名度が高い人や、深刻な結果や報復につながりかねないハイリスクな活動に関わっている人向けです。

このセクションのチェックリスト項目は、デバイスが警察に押収された場合にあなたのデータを守るのに役立ちます。

ロックダウンモード（iPhone）または高度な保護機能（Google・Android）を有効にする

スパイウェアは高度な攻撃の一種で、私たちのデバイスにある巧妙な脆弱性を悪用します。これに対抗するため、AppleとGoogleはスパイウェアへの防御を強化する高度なセキュリティモードを導入しています。

iPhoneでは**ロックダウンモード**[11]、Androidでは**高度な保護機能プログラム**[12]と呼ばれています。（Androidスマホを持っていなくても、Googleアカウントだけで高度な保護機能プログラムを有効にすることもできます。）

Appleのロックダウンモードをオンにしていたのにスパイウェアに感染した、という報告は**まったくありません**。Androidの高度な保護機能は比較的新しく、その効果はまだ実証されていません。

使い勝手とのトレードオフ：どちらの機能も、一部の機能が使えなくなるなどの犠牲をともないます。トレードオフの一覧はこちら[13]。使っていて不便な問題が出てきたら、あとからいつでも機能をオフにできます。

IPHONEでロックダウンモードを有効にする方法

iPhone： 設定 → プライバシーとセキュリティ → ロックダウンモード → ロックダウンモードをオンにする

この機能はiOS 16以降で利用できます。

ANDROIDで高度な保護機能を有効にする方法

Android： 設定 → セキュリティとプライバシー → その他の設定 の下にある **高度な保護機能** をタップ

注：この設定の場所はAndroid端末によって異なる場合があるので、設定の検索バーで「高度な保護機能」と検索するのがおすすめです。

この機能はAndroid 16以降で利用できます。

スマホ（とパソコン）のOSを常に最新バージョンにしておく

ハッカーやスパイウェア、警察が使うスマホのハッキングツールから身を守れます。

DO: 通知が来たらすぐにアップデートをインストールする

DO NOT: 「後でアップデート」ボタンを押し続ける

OSのアップデートが出るたびに、セキュリティホールが修正されています。インストールしていないアップデートが増えるほど、警察があなたのデバイスをハッキングできる手段も増えていきます。鍵のかかっていないドアがどんどん増えていく、大きな建物を想像してみてください。

OSが最新の状態でなければ、このガイドで紹介している他の対策の多くも、あなたのデータを守れません。

まずはスマホから始めましょう。リスクの高い活動をする場合は、すべてのデバイスをアップデートしておきましょう。

アップデートのやり方

セキュリティアップデートはとても大切なので、**手順を一つずつ案内するツールを作りました。**

スマホとパソコンのアップデートを確認する →

手動でアップデートする方法

手動でアップデートしたい場合は、デバイスごとに次の手順で行えます：

クリックして手動の手順を表示

iPhone

1. **デバイスがまだサポート対象か確認する：** お使いのiPhoneがまだサポートされているか確認する[14]
2. **オペレーティングシステム： 設定** → **一般** → **ソフトウェアアップデート**
3. **アプリ** は、デフォルトで自動アップデートされる設定になっています。確認するには、**設定** → **アプリ** → App Store を開き、**Appのアップデート** がオンになっていることを確かめましょう。

Mac

1. **デバイスがまだサポート対象か確認する：** お使いのMacがまだサポートされているか確認する[14]
2. **オペレーティングシステム： Appleメニュー** → **システム設定** → **一般** → **ソフトウェアアップデート**
3. **Mac App Storeからインストールしたアプリ：** これらのアプリは、デフォルトで自動アップデートされる設定になっています。確認するには、**App Store** を開いて App Store → **設定** に進み、**自動アップデート** がオンになっていることを確かめましょう。
4. **その他のアプリ：** 画面上部のメニューバー → アプリ名をクリック → **アップデートを確認** または **[アプリ名]について** をクリック でアップデートを確認するか、**設定...** の中を探してみてください。アップデートのオプションが見当たらない場合は、バックグラウンドで自動的にアップデートされる設定になっている可能性があります。

Android

1. **デバイスがまだサポート対象か確認する：** お使いのAndroidがまだサポートされているか確認する[14]
2. **オペレーティングシステム： 設定** → **システム** → **システム アップデート**（メーカーによって異なる場合があります）
3. Google Playストアの **アプリ** は、デフォルトで自動アップデートされる設定になっています。確認するには、**Playストア** を開いてプロフィールアイコンをタップし、**設定** → **ネットワーク設定** → **アプリの自動更新** に進みます。

Windows

1. **システムをアップデートする： スタート** → **設定** → **更新とセキュリティ** → **Windows Update**
2. **デバイスがまだサポート対象か確認する：** お使いのWindowsパソコンがまだサポートされているか確認する[14]
3. **Microsoft Store アプリ：** 自動更新[15]が有効になっていることを確認しましょう（デフォルトでオン）。
4. **その他のアプリ：** メニューバー → **ヘルプ** → **更新の確認** でアップデートを確認するか、アプリの設定で **アップデート** や **バージョン情報** を探してみてください。

顔認証・指紋認証によるロック解除（生体認証）をオフにする

生体認証よりもパスコードのほうが、法的に強い立場[16]をとれます。警察は、生体認証でロックを解除するよう強要してくることがあります。

顔認証・指紋認証によるロック解除をオフにする方法

iPhone： 設定 → **Face IDとパスコード** → **iPhoneのロックを解除**をオフにする

（ほかの項目はオンのままで大丈夫です。）

Android： 設定 → **ロック画面**（または**セキュリティ**）> **生体認証とセキュリティ** → スマホのロック解除に使う**顔認証と指紋認証の両方をオフにする**

注意点：顔認証や指紋認証があれば、毎回入力しなくても済むので、より強力なパスワードを使えます。どちらかを選ばなければならないなら、顔認証・指紋認証をオフにするよりも、長いパスコードにするほうが大切です。生体認証をオンのままにするなら、リスクの高い状況に向かうときにすぐオフにする方法を知っておきましょう（下のコツを参照）。

- **一時的に生体認証を無効にするいちばん確実な方法は、スマホの電源を完全に切ること。** そうするとデータも暗号化されます。次のロック解除ではパスコードが必要になります。
- **iPhoneのロックのコツ：** 顔認証・指紋認証をオンのままにしている場合でも、**サイドボタンを5回押す**と、次のロック解除でパスコードの入力を必須にできます。
- **iPhoneのカメラのコツ：** ロック画面で**左にスワイプ**すれば、ロックを解除せずに写真を撮れます。（撮影中に逮捕された場合に備えて。）
- **Androidのカメラのコツ：** 多くのAndroidスマホでは、**サイドボタン／電源ボタンを二度押す**と、ロックを解除せずにカメラを起動できます。

スマホのパスコードを8〜10桁のランダムな数字にする

8桁のランダムなパスコードを警察が解読するには何年もかかります。今のパスコードなら、自動化ツールを使えばおそらく5分もかからずに突破されてしまいます。

DO: ランダムパスコード生成ツール[17]を使って8〜10桁のコードを作る

DO NOT: 自分で考えたパスコード（日付、キーボード上のパターンなど）を使う。できれば6桁のパスコードは使わない。

パスコードの変更方法

1. このランダムパスコード生成ツール[17]を使って、8〜10桁のランダムなパスコードを作りましょう。（自分で考えるのはNG。人間はランダムに選ぶのが苦手です！）
2. パスコードを変更する：

   iPhone： 設定 → **Face IDとパスコード** → **パスコードを変更** → **パスコードオプション** → **カスタムの数字コード**

   Android： 設定 → **セキュリティ** → **画面ロック** → 現在のロックを入力 → **PIN／パスワード** → パスコードを入力
3. 覚えやすくするために、今すぐ**新しいパスコードを**少なくとも10回続けて**入力する練習をしましょう**。（生体認証をオフにすると、スマホをロックするたびにパスコードの入力が求められるようになります。）
4. 覚えるまでは、新しいパスコードを紙に書いて自宅の安全な場所に保管しておきましょう。そして2〜3週間たったら、その紙は処分してください。スマホでリマインダーを設定しておくと便利です。

パスコードの解読にはどのくらい時間がかかる？

種類	解読にかかる時間（平均）	例
6桁の推測しやすいパターン	**24時間以内**に解読される	**333666（よくあるパターン）または110585（Nov 5, 1982を表す日付のパターン）**
6桁のランダムなコード	解読に**200日**	**238253**
8桁のランダムなコード	解読に**40年以上**	**34780026**

注意：これらの時間はスマホにのみ当てはまります。パソコンはずっと短時間で解読されてしまうので、はるかに強力なパスワードが必要です。

出典： 上の表の推定値は、警察が使うフォレンジック用ハッキングツールで実際に観測された毎秒の試行回数を前提にしています。もっと強いセキュリティが必要なら、10桁のパスコードを使いましょう。考えうる最も強力な解読手段に対しても身を守れます。出典はパスコードに関するFAQ[17]のリンクを参照してください。

WhatsAppには写真ライブラリの特定の写真へのアクセスだけを許可する

WhatsAppがライブラリ内のすべての画像を見られないようにします。会社がいつかデータの使い方を変えた場合に備えるためです。

Metaは最近、Facebookアプリにある機能[18]を導入しました。写真ライブラリ内のすべての画像がMetaのサーバーに送られ、処理されるというものです。これは深刻なプライバシーの侵害で、アクティビストにとって法的なリスクにもなりえます。

Meta（WhatsAppも所有している親会社）は、WhatsAppにはこの種の機能は存在しないと主張しています。それでも、同じ会社がFacebookでまさにその機能を導入した以上、WhatsAppの写真への広範なアクセスはオフにしておく価値があります。

WHATSAPPの写真ライブラリへのアクセスを制限する方法

アクセスを制限すると、新しい写真を共有するときに手順が一つか二つ増えますが、操作は簡単です。

IPHONE

設定アプリ → **アプリ** → **WhatsApp** → **写真** → **制限付きアクセス**を選択

ANDROID

設定アプリ → **アプリ** → **WhatsApp** → **権限** → **写真と動画** → **Select photos and videos every time**を選択（端末によっては**Ask every time**）

ロック画面でWhatsAppの通知内容を非表示にする

スマホが押収されたときに、メッセージのプレビューや送信者の名前が表示されないようにします。

スマホが押収されると、メッセージ自体が消えた後でも、通知履歴からメッセージの内容や送信者の名前がわかってしまうことがあります。なぜこれが重要なのかは、Prairielandの事件[19]を見てください。

Appleは、メッセージが無効化された後もSignalの受信通知が保存されてしまう問題を、iOS/iPadOS 26.4.2（および旧バージョン向けの18.7.8メンテナンスアップデート）で修正しました。この問題は修正されたものの、Androidスマホに同じ弱点が残っているかどうかははっきりしていません。どちらのプラットフォームでもプレビューは非表示にしておく価値があります。

WHATSAPPの通知内容を非表示にする方法

IPHONE

設定アプリ → **通知** → **WhatsApp** → **プレビューを表示**を**しない**に設定

ANDROID

設定アプリ → **アプリ** → **WhatsApp** → **通知** → **Show notification content on lock screen**をオフにする

WhatsAppのAI通知要約をオフにする

Apple IntelligenceやAndroidの通知要約機能は、通知内容の一部をクラウドサーバーに送信することがあります。

Apple IntelligenceやAndroidの通知要約機能は、通知内容の一部をクラウドサーバーに送信することがあります。何がどこに送られているのかははっきりしておらず、政府の要請によってそのデータの提出が強制される可能性もあります。

このテーマについて、Signalに関連した記事があります。同じことがWhatsAppにも当てはまります：Apple IntelligenceはSignalのメッセージを読んでいる？[20]

WHATSAPPのAI通知要約をオフにする方法

IPHONE

設定アプリ → **通知** → **通知を要約** → **WhatsApp**をオフにする

ANDROID

設定アプリ → **通知** → **通知の要約**（Notification summaries） → **WhatsApp**を除外リストに追加する

WhatsAppの「リンク済みデバイス」を定期的にチェックする

リンク済みデバイスをときどき見直すことで、アカウントの乗っ取りを防げます。

WhatsAppのマルチデバイス機能は、攻撃者がアカウントを乗っ取るための主な入り口になっています。攻撃者はあなたをだましてQRコードを読み取らせたり、ペアリングコードを入力させたりします。そうすると、攻撃者のコンピューターで、あなたが送受信するすべてのメッセージが見えるようになってしまいます。

このマルチデバイスの仕組みは、ジャーナリストやオーガナイザーを狙う傭兵型スパイウェアにも悪用されてきました。詳しくはスパイウェアのページ[21]を見てください。

リンク済みデバイスの確認方法

IPHONE

WhatsApp → 下部バーの**あなた**をタップ → **リンク済みデバイス**

ANDROID

WhatsApp → ⋮ → **リンク済みデバイス**

見覚えのないものはすべてログアウトしましょう。 WhatsApp Webやデスクトップアプリを使っていないなら、すべてログアウトしてください。

特にセンシティブなチャットやグループでは、制限付きチャットをオンにすると、そのチャットがリンク済みデバイスに一切表示されなくなります。そのため、リンク済みデバイスが乗っ取られても内容を読まれることはありません。

その他のリソース

- WhatsAppの使い方ガイド[4] — Electronic Frontier Foundation
- WhatsAppのセキュリティを強化する[22] — Freedom of the Press Foundation

よくある質問

各チャットに表示される「暗号化を確認」というオプションは何ですか？

この機能を使うと、特定のチャットの暗号鍵を確認できます。これは、相手と最初につながったときに、攻撃者が通信の間に割り込もうとした可能性があるような、非常にリスクの高い状況で使われるものです。こうした高度な脅威まで考慮しなければならないほどセンシティブなチャットなら、WhatsAppではなくSignalを使うべきです。

WhatsAppがエンドツーエンド暗号化を回避する「バックドア」を作ったと主張する2026年の訴訟については？

2026年に起こされた二つの別々の訴訟で、WhatsAppにはMetaのスタッフがエンドツーエンド暗号化を回避してユーザーのメッセージを読める仕組みがあると主張されています。この主張を検証した暗号の専門家たちは、事実ではないか、誇張されている可能性が高いと考えています。もし主張が事実だと判明すれば、大手テック企業によるこれまでにないプライバシー侵害ということになります。私たちのスタンス：とんでもない主張には、それに見合うだけの確かな証拠が必要です。 Metaが倫理的な企業だとはまったく思っていませんが、訴訟で何が明らかになるかを見守りたいと考えています。いつも通り、心配ならSignalを使いましょう。

WhatsAppは通常のテキストメッセージ（SMS）より安全？

メッセージの内容に関しては、安全です。 WhatsAppのメッセージはエンドツーエンドで暗号化されているので、たとえ召喚状があっても、携帯電話会社がメッセージの内容を警察に渡すことはできません。通常のテキストメッセージ（SMS）は暗号化されておらず、携帯電話会社にはすべての内容が見えています。それでもメタデータについては、WhatsAppはSignalより劣ります。Metaは、あなたが誰にいつメッセージを送ったか、どのグループに入っているかを記録していて、警察から求められればそれを渡します。

警察は私のWhatsAppメッセージを読める？

あなたのデバイスと相手のデバイスの間でやり取りされている途中のメッセージの内容は読めません。ただし、エンドツーエンド暗号化をオンにしないままチャットのバックアップを有効にしていると、メッセージにアクセスされる可能性があります。また、警察はMetaに大量のメタデータ（連絡先リスト、メッセージの相手、参加しているグループ、IPアドレス）の提出を強制できます。さらに、押収したスマホのパスコードが弱ければ、ロックを突破してメッセージを直接読むこともできます。

WhatsAppのユーザー名を使えば、警察から電話番号を隠せる？

いいえ。ユーザー名で電話番号を隠せるのは、まだあなたの番号を知らない他のWhatsAppユーザーに対してだけです。WhatsAppを使うには今でも電話番号が必要で、Metaはその番号を、連絡先リストや参加しているグループ、誰とメッセージをやり取りしているかといった情報と一緒に警察へ提出できてしまいます。

WhatsAppではなくSignalを使うべきなのはどんなとき？

センシティブな政治的組織活動にはSignalを使いましょう。 Signalはメタデータをほとんど収集しておらず、警察からの要請があっても渡せる情報はほぼありません。コミュニティがすでにWhatsAppを使っていて乗り換えそうにないなら、設定を見直す価値はあります。ただし、リスクの高い会話はできるだけSignalに移しましょう。

関連ガイドでさらに学ぼう

Signalのセキュリティ
Signalメッセージアプリの設定を見直して、より安全な通信を。

セキュリティの基本
すべてのアクティビストに実践してほしい、基本のセキュリティ対策。

スパイウェア対策
スパイウェアや監視ソフトウェアから身を守ろう。

ドクシング対策
ドクシングやネット上のハラスメントから身を守ろう。

- アクティビストのためのVPN 16分で読めます 23
- セキュリティアップデート確認ツール 14
- Protonを安全に使う方法 17分で読めます 24
- リンクのトラッキングを削除する 3分で読めます 25
- Signalは安全？ 5分で読めます 26
- Apple IntelligenceはSignalのメッセージを読んでいる？ 6分で読めます 20

リンク

1. activistchecklist.org/ja/contribute/
2. justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/
3. rollingstone.com/politics/politics-features/whatsapp-imessage-facebook-apple-fbi-privacy-1261816/
4. ssd.eff.org/module/how-to-use-whatsapp
5. activistchecklist.org/ja/essentials/
6. activistchecklist.org/ja/signal/
7. faq.whatsapp.com/1324084875126592/?cms_platform=web
8. nitter.net/camhigby/status/2015093531526729789
9. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
10. activistchecklist.org/ja/doxxing/
11. support.apple.com/en-us/105120
12. landing.google.com/intl/en_us/advancedprotection/
13. activistchecklist.org/ja/lockdown/
14. activistchecklist.org/ja/updates/
15. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b

16. ssd.eff.org/module/attending-protest
17. strongphrase.net/passcode
18. redact.dev/blog/meta-camera-roll-ai-sharing-suggestions-2025
19. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
20. activistchecklist.org/ja/signal-ai/
21. activistchecklist.org/ja/spyware/
22. freedom.press/digisec/blog/upgrading-whatsapp-security/
23. activistchecklist.org/ja/vpn/
24. activistchecklist.org/ja/proton/
25. activistchecklist.org/ja/links/
26. activistchecklist.org/ja/signal-secure/