デモや行動に参加する前の準備

ACTIVIST CHECKLIST

最終更新日： **2026年3月18日**　所要時間の目安： **30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/protest/

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]。

抗議活動で警察が誰か一人のスマホにアクセスすると、連絡先、Signalのスレッド、位置情報の履歴など、ネットワーク全体を把握できてしまいます。このガイドは、あなた自身と、一緒に活動する仲間を守るためのものです。出かける前に：できれば電源を切る、強力なパスコードを設定する、生体認証によるロック解除をオフにする、Signalの消えるメッセージをオンにする、通知のプレビューを非表示にする。オーガナイザーや標的にされやすい人は、さらに対策を進めましょう。

警察が一人のスマホにアクセスすると、アクティビストのネットワーク全体（連絡先、Signalのチャット、位置情報の履歴など）を把握できてしまいます。ここで紹介するステップは、あなた自身だけでなく、あなたとつながっているネットワークも守るためのものです。

このチェックリストの対象： 抗議活動、リスクの高い抗議活動、デモ、または警察の出動が予想されるイベントに参加するすべての人。 ICE監視行動のデジタルセキュリティ[2] のための別個のガイドがあります。

逮捕のリスクをとる予定？ 逮捕の危険があるアクション（座り込みや封鎖など）に参加する場合は、 逮捕の危険があるアクションのためのデジタルセキュリティガイド[3] に従ってください。仲間とのスマホに関する合意事項、行動参加前に救援担当者にスマホを預けることなどについてカバーしています。

なぜこれが重要なのか？

社会運動は何十年もの間、政府のエージェント（地元の警察、FBI、CIA、NSAなど）によって監視され、潜入され、信用を落とされ、妨害されてきました。テクノロジーの発達によって、私たちは誰もが追跡され、プロファイリングされています（たとえ一度も逮捕されたことがなくても）。

でも、私たちの運動を守るためにできることはあります！ このガイドでは、抗議行動やアクションの前と最中に誰でもできる簡単なことを紹介します。自分自身と、運動の中でも特にリスクの高い仲間たちをより安全に守るためのものです。

考えておきたい脅威

- **スマホの押収と捜索** - 逮捕された場合、警察はあなたのスマホに侵入して、メッセージや写真などの個人情報にアクセスし、証拠として使おうとすることがあります
- **通信の監視** - 警察は通常のSMSや通話を傍受して、デモの計画や参加者についての情報を集めることができます
- **位置情報の追跡** - スマホは常に信号を発信していて、そこからあなたの居場所がわかったり、デモに参加していた証拠にされたりすることがあります
- **アクティビストのネットワークの把握** - 一人のスマホからデータを手に入れることで、警察はその人とつながっているアクティビストやオーガナイザーのコミュニティ全体を特定できてしまいます

ほかにもたくさんありますが、ここでは主なものをいくつか挙げました。

そもそもスマホは必要？

いちばん安全なスマホは、スマホを持たないこと。

> 可能なら、**スマホはいっそ持っていかない**のがおすすめです。データとプライバシーを守るうえで、これが最も安全な選択肢です。

とはいえ、行動中に連絡を取り合う必要があることも多いもの。時間とお金をかけられるなら、サブのスマホ[4]が最もバランスのいい選択肢です。入っているデータが最小限で済むからです。

サブのスマホを用意するのが、誰にとっても現実的なわけではないことはわかっています。普段使いのスマホを持っていく必要がある場合は、以下のリストを参考にスマホの安全性を高めましょう。

スマホの基本的な保護

すべての人　このセクションは、リスクの低いデモ（No Kingsなど）に参加するすべての人向けです。イベントのコーディネーターやリスクの高い参加者は、以下のセクションにも取り組んでください。

- [ ] 重要 **逮捕されるリスクが高まってきたら、スマホの電源を完全に切る**
  データが一番守られるのは、スマホの電源が切れているとき（ロックしただけではダメ）

スマホの電源が完全に切れていると、警察によるデータ抽出に対してより安全になります。電源を入れた後、最初にパスコードを入力するまで、データは暗号化されたままです。

だからこそ、データを守るために一番できることは、逮捕されるリスクが高まってきたと思ったらすぐにスマホの電源を切ることです。

スマホの電源の切り方

1. IPHONE
   側面のサイドボタンを**5回**押すと、すぐに**電源オフ**のオプションが表示されます

   ANDROID
   電源メニューが表示されるまで電源ボタンを長押し → **電源を切る**をタップ
2. 素早くできるように、何度か**練習**しておきましょう。
3. リスクの高い状況では、**近くにいる人にも**スマホの電源を切るよう声をかけましょう。

トレードオフ： スマホの電源を切ることにはトレードオフがあることも、わかっています。警察を撮影したり、仲間と連携を取ったりすることの方が大事な場面もあります。自分にとって何を優先すべきか、よく考えてみてください。撮影が必要なら、サブのスマホ[4]を持っていくことも検討してください。そうすれば、端末に入っている機密データを減らせます。

リスクの高い活動の前に、システム全体で位置情報サービスをオフにする

抗議行動やICEウォッチなど、リスクの高い活動では特に重要です。

DO: リスクの高い活動をするときは、スマホ全体で位置情報サービスをオフにする

スマホのアプリはあなたの正確な位置情報を収集し、データブローカーに売っています。警察は令状なしでこのデータを購入し、Webloc[5]のようなツールを使って、抗議行動の現場も含め、ある地域にどのスマホがあったかを調べています。 GoogleやAppleに保存された位置情報の履歴も、召喚状によって提出を求められることがあります。

スマホ全体で位置情報サービスをオフにすると、アプリがGPSの位置情報を収集できなくなります。そのため、データブローカーに売られたり、Google/Appleにアクセスされたりすることもありません。

位置情報サービスをオフにしても、携帯電話会社から位置を隠すことはできません。 スマホの電源が入っていて電波が届いている限り、携帯電話会社は接続している基地局からあなたのおおよその居場所を把握でき、警察はそのデータを入手できます。保護効果が高い順に：

1. スマホを家に置いていく。
2. スマホの電源を切る。ファラデーバッグを使えば、さらに保護を強化できます。
3. 機内モードをオンにし、**さらに**位置情報サービスもオフにする。
4. 位置情報サービスだけをオフにする。

機内モードだけではGPSはオフになりません。アプリは引き続き位置情報を記録でき、再接続したときにそれをアップロードできてしまいます。

位置情報サービスをオフにする方法

IPHONE

設定 → プライバシーとセキュリティ → 位置情報サービスをオフ

（より簡単な方法：Siriに「位置情報サービスをオフにして」と話しかける）

ANDROID

設定 → 位置情報 → 「位置情報を使用」をオフ

その他のヒント：

- 移動のために**地図を印刷する**か、**オフラインマップを保存しておく**と便利です。
- スマートウォッチや、Bluetoothの「鍵・財布の紛失防止」トラッカーを持っている場合は、家に置いていくか、そちらでも追跡をオフにしておきましょう。

位置情報を必要としないアプリ（ほとんどのアプリがそう）からは、位置情報の許可を取り消す

位置情報にアクセスできるアプリが、あなたの行動の詳細な記録を政府やデータブローカーに渡してしまうのを防ぐ

DO: ほとんどのアプリで位置情報の追跡をオフにする

DO NOT: すべてのアプリに居場所を知らせる

IPHONEで位置情報の許可を見直す方法

1. **設定** → **プライバシーとセキュリティ** → **位置情報サービス**に移動
2. アプリを一つずつ確認して、次のいずれかに設定します：
   - **しない：ほとんどのアプリにはこれがベスト**
   - 次回確認またはApp共有時：位置情報をめったに使わないアプリ向け
   - このAppの使用中：どうしても必要なナビアプリだけ
   - 常に：この許可が必要なアプリはほぼありません
3. **カメラ**アプリは必ず「**しない**」に設定しましょう。写真を共有したりアップロードしたりするときに、居場所がバレるリスクを避けられます。
4. **システムサービス** → **利用頻度の高い場所**という項目に移動してオフにする

ANDROIDで位置情報の許可を見直す方法

1. **設定** → **プライバシー** → **権限マネージャー** → **位置情報**に移動
2. アプリをひとつずつ確認して、次のいずれかに設定しましょう：
   - **許可しない：ほとんどのアプリにはこれがベスト**
   - 毎回確認する：位置情報をめったに使わないアプリ向け
   - アプリの使用中のみ許可：どうしても必要なナビアプリだけ
   - 常に許可：この許可が必要なアプリはほぼありません

カメラや写真アプリの位置情報の追跡をオフにすることは特に重要です

使用中に位置情報が本当に必要かもしれないアプリ：

- ナビ（Apple Maps、Magic Earth、CoMaps）
- 配車アプリ（ただし実際に使っている間だけ）

一時的な許可が必要かもしれないアプリ：

- フードデリバリーアプリが位置情報を必要とするのは、実際に注文するときだけ

位置情報へのアクセスが絶対に必要ないアプリ：

- 写真アプリ
- SNSアプリ
- ゲーム
- ほとんどのショッピングアプリ
- 銀行アプリ
- ニュースアプリ
- ほとんどの仕事効率化アプリ

忘れないで：位置情報にアクセスできるアプリはどれも、プライバシーが漏れる原因になりえます。迷ったら位置情報をオフにして、本当に必要だとわかったときだけオンに戻しましょう。

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[6]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（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[7]
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[7]
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[7]
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[7]
3. **Microsoft Store アプリ：** 自動更新[8]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。

抗議行動やアクションの連絡（メッセージ・通話）にはSignalを使おう

エンドツーエンド暗号化されたメッセージなら、監視からプライバシーを守れる。一方、通常のSMSは傍受されて読まれるおそれがある。

DO: アクティビズムや政治的な活動には**Signal**[9]（無料）をインストールして使う

DO NOT: （アクティビズムにおいて）WhatsApp、Telegram、iMessage、通常のSMSなどを使う

SIGNALのインストールと使い方

1. スマホにSignalをインストール[10]する
2. 既存の連絡先に電話番号からメッセージや通話をするか、相手にSignalのユーザーネームを聞こう。相手もSignalをインストールしている必要あり。

Signalをできるだけ安全に設定するための詳しい手順については、Signalチェックリスト[11]を参照。

Signalの通知でメッセージのプレビューをオフにする

スマホが押収された場合（電源が入ったままなら）、警察はロックを解除しなくてもホーム画面に表示されたメッセージを読むことができます。

SIGNALの通知プレビューをオフにする方法

Signalを開く → プロフィール画像をタップ → **設定** → **通知** → **表示** → **名前もメッセージも非表示**を選択

抗議行動中は、できるだけスマホを機内モードにしておこう

ワイヤレス接続をオフにして、位置情報を守ろう。そうすることで、抗議行動での活動をプライベートかつ安全に保てます。

機内モードにしても、GPSによる位置情報の追跡は止まりません。位置情報サービスを必ずオフにしてください。

スマホを持っていく場合、連絡を取るために使う必要があるかもしれません。携帯の電波がつながっている間は、接続している基地局からおおよその位置が割り出される可能性があることを覚えておこう。

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[12]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[12]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[12]のリンクを参照してください。

スマホの保護をさらに強化する

中程度の脅威 **このセクションは、次に当てはまる人向けです：**

→ 社会運動の場で**オーガナイザーやリーダーをしている**。

→ 自分のアイデンティティ（人種、セクシュアリティ、在留資格など）を理由に、**警察に狙われやすい**。

→ 危険にさらされやすい人たちと**多くの密接なつながりがある**。

リスクが高い場合は、できればデモや活動用にサブのスマホ[4]を用意することをおすすめします。そうすることで、普段使いのスマホを使う場合よりも、あなた自身とあなたのネットワークをずっと強く守れます。

抗議行動・アクション中は、進行中のすべてのスレッドでSignalの消えるメッセージを5〜15分に設定する

スマホが押収されても、消えるメッセージは時間が来れば消えます（ただし、既読のものに限ります）。

消えるメッセージを有効にする方法

Signalを開く → 各スレッドを開く（ひとつずつ） → 連絡先またはグループの名前をタップ → **消えるメッセージ** を選択 → タイマーを **5〜15分** に設定。

アクションが終わったら、もっと長い時間に戻しても大丈夫です。

重要： メッセージが消えるのは「既読」になってからです。つまり、未読の新着メッセージは押収されたスマホに残り、警察に読まれてしまう可能性があります。逮捕された人がわかっている場合は、その人をグループから外しましょう。

Signalを開く → プロフィール写真をタップ → **設定** → **消えるメッセージ** → **1週間** から、新しいスレッドすべてに消えるメッセージを設定しておくこともおすすめします。

Signalの通知でメッセージのプレビューと送信者名を非表示にする

スマホが押収されると、警察に通知履歴を見られてしまう可能性があります。

スマホが押収された場合、警察が通知履歴にアクセスする方法は二つあります：

1. スマホのロックを解除しなくても、ホーム画面に表示された通知を見ることができます。
2. ハッキングツールを使えば、スマホが受信した通知のログにアクセスできます。 （Prairieland事件での実例[13]）

これは受信したメッセージだけが対象です。そして、（消えるメッセージを有効にしている場合）Signalからメッセージが消えた後でも、このリスクは残ります。

SIGNALの通知をオフにする方法

IPHONEの場合

Signalを開く → プロフィール画像をタップ → 設定 → 通知 → 通知内容 → **「No Name or Content」を選択**

ANDROIDの場合

Signalを開く → プロフィール画像をタップして設定を開く → 通知 → 表示 → **「No name or message」を選択**

スマホのOS側でSignalの通知をオフにすると、Signalの着信も通知されなくなります。

Signal Desktopを使っている場合は、そちらでも通知をオフにしておきましょう。

参考： iOSにすでに保存されている通知ログを消去したい場合、唯一の方法はスマホを工場出荷状態にリセットし、新しいデバイスとして設定し直すことです。バックアップには通知履歴も含まれているので、バックアップからは復元しないでください。

Signalのセキュリティチェックリストを実践しよう

SIGNALを安全に使うための設定方法

Signalチェックリスト[11]のすべてのステップを完了して、Signalのセキュリティとプライバシーを強化しましょう。

Signalセキュリティチェックリスト →

広告ID（警察に位置情報を追跡されるおそれあり）を無効にする

警察は広告IDを利用したツールで人々を追跡している

ICEをはじめとする警察機関が位置追跡ツールを使っている[5]ことがわかっています。これらのツールは、スマホが発信する「広告ID」に部分的に依存しています。こうしたツールは、社会運動の弾圧によく使われています。

広告IDは、広告経由で送り込まれるスパイウェアの標的選びにも使われてきました[14]。

iPhoneでは、この機能はデフォルトで無効になっています。 Androidではデフォルトで有効になっているので、無効にする必要があります。

広告IDを無効にする方法

IPHONE

設定 → **プライバシーとセキュリティ** → **トラッキング** → **Appからのトラッキング要求を許可**をオフにする

iPhoneでは、この設定はデフォルトで無効になっています。でも、念のため確認しておきましょう。

ANDROID

設定 → 検索アイコンをタップして「広告」で検索 → **広告 ID を削除**をタップ

この設定の場所は機種によって違うので、検索するのがいちばん簡単です。

スマホのロック中は音声アシスタント（Siri や Google アシスタント）をオフにする

ロックされた状態でも、警察があなたのスマホに基本的な操作をさせるのを防ぎましょう。

音声アシスタントをオフにする方法

IPHONE

設定 → **Siri** → **ロック中にSiriを許可** をオフにする

ANDROID

設定 → **Google** → **Google アプリの設定** → **検索、アシスタント、音声** → **Google アシスタント** → **ロック画面** をオフにする

顔やタトゥーなど、個人を特定できるものが写った写真や動画はシェアしない

人の顔が写った写真をシェアするときは気をつけましょう。その人が逮捕されたとき、写真が不利な証拠として使われることがあります。

写真を撮ることにはリスクがあり、同時に大切なことでもあります。アクションの記録は、私たちのストーリーを伝え、共感を広げるために欠かせないことが多いからです。一方で、国家がアクティビストを追跡し、起訴するために使える証拠をつくってしまうことは避けたいところです。

身元を守りながら写真を撮る方法

- できれば、そもそも顔を写さないようにしましょう。
- Google フォト、iCloud 写真などのクラウドへの自動アップロードをオフにしておきましょう。そうすれば、写真を確認してぼかしを入れる前に勝手にアップロードされることを防げます。
- 顔が写った写真を撮ってしまい、それをどこかに送る場合は、Signal のぼかしツール[15]を使いましょう。タトゥーや目立つ服装など、特徴的な部分にもぼかしを入れましょう。
- SNS に投稿する写真には十分注意しましょう。警察はアクティビストを追跡するために、SNS を常に監視し、調べています。
- 顔見知りのグループで活動しているなら、記録や共有についてのルールを事前に話し合っておきましょう。

道順を印刷するか、オフラインマップを使う

Google マップの履歴には、あなたが行ったすべての場所が記録されています。警察は令状があればこのデータを手に入れられます。

DO: 印刷した道順か、Magic Earth[16] または Apple マップのオフラインマップを使う

DO NOT: Google マップを使う

特定のエリアにいた人を誰でも追跡するために警察が使う「ジオフェンス令状」から身を守ることができます。

プライバシーを守ったナビゲーションの使い方

- アクションや抗議行動に出かける前に、**位置情報サービスをオフ**にしましょう。
- 携帯キャリアにも居場所を知られないように、できるだけスマホを**機内モード**にしておきましょう。
- できれば昔ながらの**印刷した道順**を使いましょう。検索のプライバシーを守るため、Open Street Map[17] から印刷しましょう。（さらにプライバシーを高めたいなら、Tor Browser[18] で Open Street Map にアクセスしましょう。）
- プライバシーを守りながらオフラインで地図や道順を使えるアプリを使いましょう。いちばんおすすめなのは Magic Earth マップ[16]（Android と iPhone に対応）ですが、Apple マップもオフラインマップをダウンロードでき、十分に使えます。アプリ内でエリアを事前にダウンロードする機能を探し、その後はずっとスマホを機内モードにしておきましょう。自動ナビ機能は使えないので、道順を自分で一つずつ確認しながら進む必要があります。

BluetoothとWi-Fiをオフにする

警察は追跡ツール[19]を使って、スマホが発しているBluetoothやWi-Fiの信号から、その場所に誰がいるかを特定できます。

スマホを持っていくなら、連絡を取るためにモバイル通信が必要で、機内モードにするのは現実的ではないはず。そのため、追跡されるリスクを減らすには**BluetoothとWi-Fiをオフにする**のがベストです。

iPhoneの注意点： 画面を下にスワイプして「**コントロールセンター**」からBluetooth/Wi-Fiをオフにしても、実際には完全にはオフになりません。今つながっているネットワークから切断されるだけで、追跡可能な信号は出し続けています。完全にオフにするには、以下の手順に従ってください。

BLUETOOTHとWI-FIをオフにする方法

IPHONE

設定 → **Bluetooth** → **Bluetoothをオフにする**

IPHONE

設定 → **Wi-Fi** → **Wi-Fiをオフにする**

ANDROID

設定 → **Bluetooth** → **詳細設定**（または三点メニュー） → **Bluetoothをオフにする**、さらに**Bluetoothスキャンをオフにする**

ANDROID

設定 → **Wi-Fi** → **詳細設定**（または三点メニュー） → **Wi-Fiをオフにする**、さらに**スキャン**または**Wi-Fiスキャン**をオフにする

仲間を危険にさらすおそれのあるSignalグループから退出する

スマホが押収されたときに、あなたのネットワークを守ることにつながります。

警察にスマホを押収された場合、最大のリスクのひとつは、あなたのネットワーク全体がさらされてしまうことです。 Signalアカウントで本名を使っていなくても、Signalのユーザー名の裏にはそれぞれ固有のIDがあります。警察はこのIDを使って、押収した複数のデバイスをまたいで同一人物を特定できてしまいます。

グループからの退出と削除、両方が必要です：

- 退出するだけだと、過去のメッセージやグループのメンバー履歴がスマホに残ったままになります。
- 削除するだけだと、新しいメッセージが届き続け、スレッドがまた表示されてしまいます。

SIGNALグループから退出し、さらに削除する方法

1. **後で再参加する計画を立てておく：** 逮捕の可能性がある場面に向かう前に、自宅など安全な場所で、すべてのグループと、アクションや国境通過が終わった後に再追加してくれる人のリストを紙に書いておきましょう。
2. **グループから退出するには：** Signal → [グループ] → 上部のグループアイコンをタップ → **グループから退出**
   - 自分が唯一の管理者の場合は、メンバー全員を削除するか、別の人を管理者に指定する必要があります。
3. **スマホからグループを削除するには：** Signal → メイン画面 → スレッドを左にスワイプ → **削除**
   - 他の人の端末からは削除されません。

セキュリティ習慣のヒント：

- 3か月ごとにSignalのスレッドを整理するよう、定期的なリマインダーを設定しましょう。
- どのグループから退出したか、アクションの後に誰に再追加を頼めるかを、必ずメモしておきましょう。

注： この作業がすごく面倒で手間がかかると感じたら（実際そうです！）、それもアクション用にサブのスマホ[4]を使うべき理由のひとつです。そのスマホは、その日のアクションを実行するのに必要な一つか二つのグループにだけ参加させておけばいいのです。

- [ ] **スマホをバックアップする**
  スマホが押収されて、新しいスマホが必要になったときのために。

より安全にするために、スマホのバックアップはクラウドではなくパソコンに取るのがおすすめです。警察は令状を取って、iCloudやGoogleのバックアップ、オンライン上の写真やドキュメントなどを手に入れることができます。

> **スマホをパソコンにバックアップする方法**
>
> iPhoneの場合：USBケーブルでパソコンに接続し、iTunes/Finderを開いてデバイスを選択します。手動でバックアップする項目の「今すぐバックアップ」をクリックし、データを守るために「ローカルのバックアップを暗号化」が選択されていることを確認してください。（パスワードは忘れずに保存しておくこと）
>
> Androidの場合：USBケーブルでスマホをパソコンに接続し、表示されたら「ファイル転送」モードを選んで、必要なフォルダ（DCIM、Downloadなど）を手動でコピーします。コピー先はパソコンのハードドライブです。

- [ ] **ファラデーバッグを使って、スマホから出る追跡可能な信号をすべて遮断する**

ファラデーバッグは、スマホに出入りするすべての信号（GPS、携帯電話の電波、Wi-Fi、Bluetoothなど）を遮断します。

理論上は、スマホの電源を切れば同じ効果があるはずです。よくあることではありませんが、スマホをハッキングして電源が切れていてもネットワークに接続できる[20]ようにする方法が存在します[20]。ファラデーバッグを使えば、さらに安心です。

ファラデーバッグの購入先の例：

- Mic Lockのファラデーバッグ[21]（13ドル）- 最も安いけれど、信号が少し漏れることがある
- MOS Equipmentのファラデーバッグ[22]（23ドル）
- SLNTのファラデーバッグ[23]（30ドル）

デモで身を守るためのその他のヒント

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。

- [ ] **逮捕されたときに電話する番号を決めておく。油性ペンで体に書いておく。**

逮捕されたときに電話をかけて、外側からサポートしてもらうための番号です。リスクの高い状況で特に重要です。

逮捕されたときに電話する番号の選び方

1. **逮捕されたときに誰に電話するか決めておく：**
   - 地域で留置サポートのホットラインが活動しているかわからない場合は、誰かを緊急連絡先に決めて、その人の電話番号を使いましょう。法的サポートにつないでくれる友人や、信頼できる仲間でもOKです。必ず事前に本人の同意をもらっておきましょう。
   - リスクの高いアクションに参加する場合は、オーガナイザーがすでに専用の法律ホットライン番号を用意していることもあります。
   - 大都市なら、アクティビストをサポートするスタッフがいる National Lawyers Guild（全米法律家ギルド）の留置サポート用ホットラインがあるかもしれません。 NLG の留置サポート用ホットライン番号の一覧はこちら[24]。ホットラインを使うのは、事前に留置サポートのフォームを提出してある場合だけにするのがおすすめです。そうすれば、あなたへのサポートを進めながら、あなたの連絡先にも代わりに電話してもらえます。
2. **法律ホットラインの番号を油性ペンで体に書いておく。**簡単にこすれて消えない場所（上腕、脚、胴体）に書きましょう。逮捕されて電話をかけられるときは、その番号にかけてください。

☐ 目立たない服装で周りに溶け込もう。プライバシーをより守りたいなら顔を隠すことも検討しよう

警察は顔認識技術[25]を使って、防犯カメラの映像からあなたを特定することができます。敵対する人たちは、「逆画像検索」ツールを使ってあなたを見つけ出し、ネット上で嫌がらせをしてくることがよくあります。

周りに溶け込む方法

- **特定されにくい無難な服を着る**（すごく特徴的な柄や色は避ける）。
- **タトゥーを隠す**など、写真や動画で目立ってしまうような特徴的なものは隠しておきましょう。
- **KN-95マスクを着用する**と、COVID対策にもなり、匿名性も高まります。

☐ 監視を意識して移動の計画を立てよう

自分が負うリスクの大きさを考え、監視を避けるためにどこまで手間をかけたいかを検討しましょう。

気をつけたい追跡の例：

- **ナンバープレート自動読取装置：** あらゆる場所にありますが、特に料金所や橋に多く設置されています。
- **監視カメラ**[26]：ほとんどの店舗や企業などの内外、そして公共交通機関にはカメラが設置されています。スマートドアベルなど、一般家庭のカメラのことも頭に入れておきましょう。
- **交通系ICカード**：交通系ICカードを使って公共交通機関に乗ると、デジタルな記録が残ります。抗議行動に向かうときは、現金で支払うか使い捨ての乗車券を買うことを検討しましょう。（ちなみに、ほとんどの公共交通機関には常にたくさんの監視カメラがあります。）
- **クレジットカード**：クレジットカードやタッチ決済を使うと、特定の時間に特定の場所にいたことを示すデジタルな記録が残ります。プライバシーを守るために、できるだけ現金を使うことを検討しましょう。
- **配車アプリ（Uber/Lyft）：** 配車アプリを使って抗議行動の現場に行くと、あなたの移動経路や居場所がはっきりと記録に残ります。

さらに詳しく

ヒント： 次のアクションの前に、一緒に行く仲間とこのチェックリストをグループセッション[27]でやってみるのもおすすめです。そのほうが楽しいし、全員が最後までちゃんとやり切れます。

- Electronic Frontier Foundation - 抗議活動に参加するためのガイド[6]（2024年更新）
- CLDC - Expect the Unexpected: Secure Your Phone Against Confiscation or Loss / 予期せぬ事態に備えて：押収や紛失からスマホを守る[28]（2021年）
- Freedom of the Press Foundation - What to do if your phone is seized by the police / 警察にスマホを押収されたらどうするか[29]（2016年）
- Freedom of the Press Foundation - Mobile security tips: Nine steps to prepare your phone before an action / モバイルセキュリティのヒント：アクションの前にスマホを準備する九つのステップ[30]（2020年）
- Freedom of the Press Foundation - Your smartphone and you: A handbook to modern mobile maintenance / スマホとあなた：現代のモバイルメンテナンスのハンドブック[31]（2024年）
- The Markup - How Do I Prepare My Phone for a Protest? / 抗議行動に向けてスマホをどう準備する？[32]（2024年）

関連ガイドでさらに学ぼう

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。

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。

旅行・飛行機移動のセキュリティ
移動・旅行するアクティビストのためのデジタルセキュリティ対策。

リンク

1. activistchecklist.org/ja/contribute/
2. activistchecklist.org/ja/ice/
3. activistchecklist.org/ja/action/
4. activistchecklist.org/ja/secondary/
5. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
6. ssd.eff.org/module/attending-protest
7. activistchecklist.org/ja/updates/
8. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
9. signal.org
10. signal.org/download/
11. activistchecklist.org/ja/signal/
12. strongphrase.net/passcode
13. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
14. activistchecklist.org/ja/spyware/
15. signal.org/blog/blur-tools/
16. magicearth.com
17. openstreetmap.org
18. activistchecklist.org/ja/research/
19. unwall.app/www.wired.com/story/dnc-hidden-signal-hunt/
20. theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data
21. mic-lock.com/products/signal-blocking-faraday-bag
22. mosequipment.com/collections/all-products/products/mission-darkness-non-window-faraday-bag-for-phones
23. slnt.com/collections/faraday-phone-sleeves/products/faraday-bags?variant=48508947005734
24. nlg.org/chapters-2/
25. sls.eff.org/technologies/face-recognition
26. sls.eff.org/technologies/surveillance-camera-networks
27. activistchecklist.org/ja/party/
28. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
29. freedom.press/training/mobile-security-for-activists-and-journalists/
30. freedom.press/training/mobile-security-protest-preparation-tips-activists/
31. freedom.press/training/your-smartphone-and-you-handbook-modern-mobile-maintenance/
32. themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024