逮捕される可能性がある行動のためのデジタルセキュリティ

ACTIVIST CHECKLIST

最終更新日： **2026年10月30日**　所要時間の目安： **20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/action/

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]。

これは、事前に計画された比較的リスクの低い非暴力の市民的不服従行動で、一部の人が逮捕のリスクを負うものの、法的な影響は比較的軽い場合のためのガイドです。ベストな方法: 行動開始前にスマホを自宅に置いていくか、逮捕のリスクをとらない人に預ける。

このガイドでは、一部の人々が逮捕覚悟で行動予定の非暴力市民的不服従行動（またの名を直接行動）にスマホを持参する必要があるときのデジタルセキュリティについて説明します。仲間の安全を守ることの一環です。行動にあたっては身体的な安全についても計画を立て、セーフティチームを設置し、全員が自分の権利について知っていることを確認する必要があります。 Our safety checklist for action organizers[2] can help with all of these.

リスクレベルを見極める：このガイドは、法的リスクが比較的低いアクション（例：座り込みや、自分の体をドアに鎖でつなぐなど）を想定しています。もし匿名性が必須だったり、重大な法的結果をもたらす何かを計画しているのであれば、 このガイドがカバーする内容以上に注意すべき。

このガイドは、次のような状況を想定しています：

- 全員が守るデジタルセキュリティのルールを決められる程度に、中心となる組織がしっかりしている行動であること。
- アクションに参加する人のほとんどに、**スマホを持ってこない**よう呼びかけている
- 現場での連携のために、どうしてもスマホが必要な人がいる（例：戦術リーダー、メディック、ディエスカレーションチームなど）
- 逮捕のリスクが高い、または自分が逮捕の危険を冒すことを計画している。
- 警察が押収したスマホのデータにアクセスするために、スマホのロック解除ツールを使ってくる可能性がある
- 行動の現場への行き帰りでの監視は気にしていないこと。

どれか一つでも当てはまらない場合は、さらに対策が必要かもしれません。抗議行動向けのスマホセキュリティ強化セクション[3]をチェックするか、サブのスマホ[4]（「使い捨てスマホ」と呼ばれることもあります）を持っていくことを検討しましょう。

オーガナイザーへのヒント： 行動に向けた準備期間中に、セキュリティパーティーを開く[5]のもおすすめです。当日までに、仲間と一緒にこれらのステップを進めておけます。

なぜこれが大事なのか？

社会運動は何十年もの間、政府機関（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、私たちは皆追跡され、プロファイリングされています（一度も逮捕されたことがなくても）。

言論と集会の自由についての法的権利を行使しているときであっても、多くの政府勢力は抗議を圧殺しようとし、アクティビストの行動を犯罪化します。(「ミネソタ15」の例を参照[6])

それでも、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、抗議行動の前や最中に誰でもできるシンプルな対策を紹介します。自分自身と、運動の中で特に危険にさらされている仲間をより安全に守るためです。これらの予防措置を取ることは、（自分と自分のデータだけでなく）組織活動で関わる全員を守ることに役立ちます。それは何らかの悪いことをしているという仕草でも、そう認めることでもありません。

考えておくべき脅威

- **スマホの押収と捜索** - 逮捕されると、警察はあなたのスマホに侵入し、メッセージや写真などの個人情報を引き出して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、抗議行動の計画や参加者の情報を集めることができます
- **アカウントデータや携帯キャリアのデータの開示命令** - 警察は裁判所の命令を取って、あなたのオンラインアカウント（GoogleやAppleなど）や、携帯キャリアが持つ通信・位置情報のデータにアクセスできます。
- **情報提供者と潜入捜査官** - ミーティングやグループチャットにいる人々が、見聞きした内容を警察に渡しているかもしれない
- **活動家ネットワークの把握** - 一人のスマホからデータを得るだけで、警察はその人とつながっている活動家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

アクションの参加者全員へ

- [ ] 重要 **Agree as a crew that anyone risking arrest should hand their phone to a support person (or leave it at home)**
  電源が切られ、押収されるリスクの低いスマホは、全員の安全を守ることにつながります。

For lower-risk arrestable actions, it's best to have everyone either A) leave their phone at home or B) **turn off their phones** and leave them with a support person. これは大体の場合、監獄サポートを担当する人です 監獄サポート。この担当者はアクションに参加しないか、アクションの外側の端など、リスクがごく低い位置にいるようにしましょう。

アクションでのスマホに関する取り決めの作り方

1. **本当にスマホが必要な役割はどれかを決める。** たいていは、戦術リーダー、警察との連絡係、救護担当など、ごく数人だけです。それ以外の人は全員、サポート担当者にスマホを預けます。逮捕のリスクが高い役割の人は、スマホを持ってこないようにしましょう。（または、配置についたらすぐに預けるようにします。）
2. **配置につく前に、サポート担当者がほとんどのスマホを回収する。**
3. **釈放された人にスマホを返す方法を計画しておく。**通常は、逮捕された人を支援するジェイルサポート担当者が、釈放された人のところへスマホを届けます。
4. **取り決めは早めに共有し、何度も伝える。** トレーニングやアクション前のブリーフィングでも繰り返しましょう。

ヒント：スマホがたくさんあって、それぞれの人が指したスマホが本当にその人のものか確認する必要がある場合は、目の前でロックを解除してもらうといいでしょう。

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**[7]（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[8]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[9]を参照。

重要 デフォルト設定を変更して、Signalの新しいスレッドすべてで消えるメッセージを有効にする

万が一、誰かのスマホが押収されたり侵入されたりしても、全員の安全を守りやすくなります。

Signalの使い方で、誰でもできる一番効果的な改善は、消えるメッセージ[10]が***デフォルトで***有効になっているか確認することです。私たちが話を聞くアクティビストの多くは、これをデフォルトで有効にしていません。（しかも、新しいスレッドごとに手動で有効にするのは、ほとんどの人が忘れてしまいがち。）

これはあなた自身の安全も、ほかの人の安全も守ります。誰のスマホが警察に押収されるかはわかりません。たとえ完全に合法的なことを話しているつもりでも、政府は私たちの言葉をねじ曲げて、異議を唱えた私たちを罪に問おうとする手を見つけてくることがあります

消えるメッセージについて、気をつけておきたいことが二つあります：

1. **まず、デフォルト設定を変更して**、自分が作るスレッドすべてでこの機能が有効になるようにしましょう。
2. **次に、ほかの人が始めたスレッドでも有効になっているか確認しましょう：**ほかの人がスレッドを始めた場合、消えるメッセージが有効になっていないことがあります。その場合は自分で有効にする必要があるかもしれません。

消えるメッセージを有効にする方法

1. **デフォルトを変更するには：** Signalを開く → プロフィール写真をタップ → **設定** → **プライバシー** → **消えるメッセージ** → 希望の時間に設定（リスクの許容度に応じて長めにも短めにも）。
2. **（Androidのみ）メッセージの保存期間の上限を変更する：**消えるメッセージがオンになっていないスレッドでも、メッセージが削除されるようになります。（削除されるのは自分の端末上のメッセージだけです。） Signalを開く → プロフィール写真をタップ → **設定** → **データとストレージ** → **ストレージを管理** → **メッセージを保持** → 希望する最大期間に設定。前の画面に戻り、**リンク済み端末にも制限を適用**をオンにします。
3. **既存のスレッドを変更するには：** Signal → 変更したいメッセージスレッドを開く → 画面上部の相手の名前（またはグループ名）をクリック → **消えるメッセージ** → 希望の時間に設定。
4. **古いメッセージ／スレッドを削除する：**消えるメッセージは、過去のメッセージにはさかのぼって適用されません。なので、スマホに残っている古いスレッドは削除しておくといいかもしれません。ただ残念ながら、相手のスマホからは削除されません。なので、とても機密性の高い内容なら、相手にもスレッドを手動で削除してもらうよう頼む必要があるかもしれません。（ついでに、消えるメッセージをデフォルトでオンにするよう勧めてみましょう！）

消えるメッセージの時間を選ぶ：消えるまでの時間をどのくらいに設定するかは、メッセージの機密性によって変わります。自分にこう問いかけてみるといいかもしれません。「もし誰かの端末が押収されたりハッキングされたりしたら、これらのメッセージが見られないことはどのくらい重要？」

- 友だちとリスクの低い話をするなら、4週間でもいいかもしれません。
- 一般的な政治的な組織活動なら、1週間がいいかもしれません。
- リスクの高いアクションでは、1日、1時間、あるいは5分に設定して、アクションが始まる前にメッセージが消えるようにするのもいいでしょう。

注意：メッセージが消えるのは、メッセージが既読になった後です。たとえば、受信者が2週間メッセージを読まず、消えるメッセージを4週間に設定していた場合、実際にメッセージが消えるのは送信から6週間後になります。

共同作業には（Google Docsではなく）Proton Docsを使う

閲覧するドキュメントをすべてGoogleに追跡されないよう、グループのデータを守る

DO: 組織活動にはProton Docs（またはCryptpad）を使う

DO NOT: 組織活動にGoogle Docsを使う

Googleはユーザーのあらゆる行動を追跡しています。どのドキュメントを開き、共有し、アクセスしたかも含めてです。警察は召喚状や令状を使ってこのデータを入手できますし、正当な許可なく共有した例も知られています。Google Docsの外で組織活動をすることで、お互いをより安全に守れます。

Proton Docs[11]は、Google Docsに代わる高品質なツールです。ドキュメントはエンドツーエンドで暗号化されています。つまり、たとえ当局がProtonのサーバーにアクセスしても、ドキュメントの中身を見ることはできません。

Proton Docsはデフォルトでは匿名になりません！よりリスクの高い組織活動をしているなら、Protonの限界と安全な使い方[12]を必ず確認してください。

PROTON DOCSの使い方

1. まだ持っていなければ、Protonアカウントを作成[13]しましょう。無料プランで大丈夫です
2. Proton Drive[14]にアクセス → **新規**ボタンをクリック → **新規ドキュメント**を選択
3. ドキュメントを共有する準備ができたら、「共有」ボタンをクリックします。他のProtonアカウントと共有するか、「公開リンクを作成」を有効にして、Protonアカウントを持っていない人と共有できます。リンクはセキュリティが低くなるので、共有する場所には気をつけてください！「リンクを知っている全員が閲覧可能」モードをオンにする場合は、パスワードを設定することをおすすめします。

一緒に活動している仲間にもProtonアカウントを作るよう勧めて、全員でより安全な状態を目指しましょう。

フォームをお探しですか？ ProtonにはGoogleフォームのような機能はありません。Cryptpadのフォーム[15]や、エンドツーエンド暗号化オプションを有効にしたJotform[16]を試してみてください。

Don't write down anything you wouldn't want read back to you in court

Chats, docs, and notes can end up in the hands of cops.

DO: Talk through sensitive details in person, with phones put away

DO NOT: Put who is risking arrest, or the details of the plan, in group chats or shared docs

We are in an era where the federal government is surveilling and prosecuting activists with a level of intensity we haven't seen in decades.

When doing mass organizing, we're always balancing the need for security with the need to grow our movements and build power.

One way we can reduce unnecessary risk is to be careful about what we write down. What we write down often ends up being used against us in court, even if we're using encrypted tools like Signal.

For any organizing involving risking arrest (or highly targeted organizing like ICE watch[17] or Palestine solidarity), it's important to have agreements about what folks will not write down.

How the data ends up in court:

- **Someone's phone is seized.** If anyone in a chat is arrested and police get into their phone, they can read every message and document on it.
- **A company hands over your account.** Services like Google Docs aren't end-to-end encrypted, so the company can see your documents and give them to police who get a subpoena or warrant. In 2025, Google gave ICE a graduate student's account information in response to a subpoena, without telling the student first[18].
- **Someone in the group is an informant or undercover cop.** In the 2026 federal case against the Minnesota 15, undercover agents joined activists' Signal group chats[6] and passed along what they read, which prosecutors then used in court.

HOW TO KEEP YOUR PLANS OUT OF THE WRITTEN RECORD

Avoid putting riskier things in writing in messages, documents, or even paper notes.

Before you type/write something, ask yourself: "Would I be ok hearing this read aloud in a court case against me?" If not, save it for an in-person conversation (ideally with all phones/devices in a different room).

Things you may want to avoid writing down:

- That you are planning to do something that carries the risk of arrest (even a very mild sit-in is usually breaking a trespassing law)
- Who is participating in the group or action
- Who is leading
- For actions: the location, the tactics, identifying information about people involved
- Other groups involved
- Jokes/venting/sarcasm that could read as a serious threat/intention.

Last step: Build practices to **delete/destroy things you did write down as soon as you no longer need them**. This often gets forgotten, so building in accountability systems can help.

Treat large or open groups as if an informant is in them. You usually can't tell who is an informant. And it's bad practice to start trying to "find the snitch" in a group. The more people in a group, the harder it is to know everyone. Keep the most sensitive conversations to small groups of people you know and trust.

☐ 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[19]。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。

スマホのロックダウン（スマホを持っていく人全員）

スマホを持っていく人のうち、メインのスマホにとても機密性の高いデータが入っている人や、警察に狙われるリスクが高い人は、データの少ないサブのスマホ[4]を使って、このガイドのステップをすべて実行することをおすすめします。

- [ ] **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[20]
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[20]
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[20]
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[20]
3. **Microsoft Store アプリ：** 自動更新[21]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。

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[22]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[22]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[22]のリンクを参照してください。

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[23]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。

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。

アクション中（スマホを持ってきた場合）

☐ 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。

逮捕されるリスクのない人にスマホを預けよう

拘束されたときにスマホを持っていないこと。それが自分のデータとムーブメントを守るいちばんの方法です。次善の策は、電源を完全に切っておくこと。

逮捕されるリスクのない人にスマホを預ける方法

- **逮捕されるリスクを負うつもりなら**：現場に出る前にスマホの電源を切り、あらかじめ決めておいたサポート担当の人に預けましょう。
- **アクション中にスマホが必要なら**：サポート役（タクティカル、救護、ディエスカレーションなど）の人は、アクション中にスマホが必要になることもあります。アクションの計画や、警察の動きがどれだけ読めないかによっては、逮捕のリスクが高まったときにその場を離れられないこともあります。
  - アクションの計画上それが可能で、ギリギリまでスマホが必要なら、最後に誰かに預けましょう。
  - スマホが必要で誰にも預けられない場合は、逮捕される前に必ず電源を完全に切っておきましょう。

行動の後

After the action, delete the planning docs and Signal groups

Old chats and docs can still be read if a phone is seized or an account is subpoenaed later.

Once the action is over, the documents and chats you made are no longer needed. The longer they stick around, the more chances that they can end up in the hands of the cops through a seized phone, a subpoena, or an informant in the group.

Before the action, agree on a cleanup plan. Create an accountability system to help you follow through.

> **If anyone was arrested or charged, check with your legal support team or a lawyer before deleting anything.** Deleting records once you know about an investigation, subpoena, or charges can be treated as destroying evidence, which is a separate crime. This is another reason to turn on disappearing messages with a short timer before the action, so most messages are already gone.

HOW TO CLEAN UP AFTER AN ACTION

1. **Delete the documents.** This includes planning docs, Proton/CryptPad docs, spreadsheets, jail support forms, and any written notes. Then empty the trash.
2. **Shut down the Signal groups**: Signal groups can be useful for ongoing organizing but the list of members also presents a risk to everyone if anyone's phone gets seized in the future. Consider moving everyone into a bigger announcement-only group for ongoing organizing rather than keeping that one small group going.
   - Post a message letting everyone know the group is closing, and ask them to delete the chat from their phones. Remove each member yourself to make sure it happens.
   - Delete the chat from your own phone: Signal → Main screen → Swipe left on the thread → **Delete**. (This won't remove the group from other people's phones, just yours. Disappearing messages will auto-delete from everyone's phones, though.)
3. **If you're not an admin,** leave AND delete the group and encourage everyone else to do the same.
4. **Shred any paper notes**, maps, or lists.

さらに詳しく

- CLDC - Expect the Unexpected: Secure Your Phone Against Confiscation or Loss[24]（2021年・英語）
- Freedom of the Press Foundation - What to do if your phone is seized by the police[25]（2016年・英語）

関連ガイドでさらに学ぼう

Safety checklist for action organizers

Physical, digital, and legal safety for organizers.

セキュリティパーティーを開こう

グループで一緒にチェックリストを進める用の予定表テンプレート。

デモや行動に参加する前の準備

デモや行動に参加するすべての人のためのデジタルセキュリティ。

リンク

1. activistchecklist.org/ja/contribute/
2. activistchecklist.org/ja/action-safety/
3. activistchecklist.org/ja/protest/
4. activistchecklist.org/ja/secondary/
5. activistchecklist.org/ja/party/
6. unwall.app/www.wired.com/story/ice-is-running-one-of-the-largest-anti-left-surveillance-operations-in-us-history/
7. signal.org
8. signal.org/download/
9. activistchecklist.org/ja/signal/
10. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
11. proton.me/drive/docs
12. activistchecklist.org/ja/proton/
13. proton.me
14. drive.proton.me
15. cryptpad.fr
16. jotform.com
17. activistchecklist.org/ja/ice/
18. eff.org/deeplinks/2026/04/google-broke-its-promise-me-now-ice-has-my-data
19. nlg.org/chapters-2/
20. activistchecklist.org/ja/updates/
21. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
22. strongphrase.net/passcode
23. ssd.eff.org/module/attending-protest
24. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
25. freedom.press/training/mobile-security-for-activists-and-journalists/