ICE監視行動のデジタルセキュリティ

ACTIVIST CHECKLIST

最終更新日： **2026年2月2日**　所要時間の目安： **20分〜2時間**

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。

あなたのスマホには、Signalのグループ、連絡先、コミュニティの仲間の写真、他のオーガナイザーとのやり取りが入っています。 ICEに押収されたら、あなたのネットワーク全体がさらされてしまいます。撮影する人も、ラピッドレスポンスの緊急対応に参加する人も、パトロールをまとめる人も、裏方でサポートする人も、このチェックリストはあなたと一緒に活動する仲間を守ります。

対象： ICEの責任を追及するためにその活動を監視しているすべての人。撮影、徒歩パトロール、アダプト・ア・コーナー（担当地点の見守り）、ラピッドレスポンス（緊急対応）など。ここにはICE／DHS（国土安全保障省）／CBP（税関・国境警備局）や、それらと協力しているあらゆる機関が含まれます。（注：同行支援や相互扶助の活動には、また別のリスクがあります。このガイドの多くはそうした場面でも役立つかもしれませんが、そのためのニーズに特化して作られたものではありません。）

範囲： このガイドは、あなたのプライベートなデータが国家や右翼勢力にさらされるリスクを減らすためのものです。身元、居場所、通信、組織活動の計画、自宅住所を守るためのステップが含まれています。

注： このガイドでは、ICE監視に関わる身体的な安全、オペレーショナル・セキュリティ（作戦上の安全管理）、法的リスクについては直接扱っていません。そうした分野に関わる実践も含まれているかもしれませんが、このガイドの目的はデジタルのリスクに対処できるようにすることです。

リスク： ICEの主な活動は、拘束と強制送還です。でも、デジタルインフラは彼らの活動に欠かせないもの。責任追及の取り組みを監視し、弾圧し、罰しようとするときにも使われています。たとえば、ICEが自分たちを撮影する人全員を追跡しようとしていることがわかっています。エージェントは 顔 認識とソーシャルメディアのモニタリングを使用し、 監視者たち の自宅に張り込み、令状なしの 位置情報 トラッキングを行います。連邦政府は、合衆国憲法修正第1条で保障された権利（表現の自由など）を行使した活動家を立件しようとしてきました。また、右翼の敵対勢力がSignalのスレッドに潜入したり、活動家をドクシングしたりしていることもわかっています。

それでも、自分たちを守るためにできることはたくさんあります！ 大変そうに聞こえるかもしれませんが、連邦政府は（彼らがそう思わせたいほど）全能ではありません。彼らのデジタル監視を難しくし、弾圧的な手口に直面しても互いの安全を守るために、取れるステップはたくさんあります。

私たちの安全は私たちで守る： あなたのスマホに入っているのは、**あなた**のデータだけではありません。 Signalのグループ、連絡先、コミュニティの仲間の写真、ほかのオーガナイザーとのスレッドなども入っています。もしスマホが押収されたら、あなたの組織活動のネットワークが明るみに出て、危険にさらされるおそれがあります。このガイドでは、あなたとあなたのコミュニティの安全を守るためのステップを紹介します。

背景： このガイドは、ミネアポリスでのICEによる侵攻（2026年初頭）を受けて作成されたもので、現地や全米各地のICE監視行動のオーガナイザーと相談しながら作られました。

仲間と一緒に取り組もう。 ICE監視のセキュリティは、チーム全員が同じ認識を共有しているときに一番うまく機能します。パトロール、緊急対応、撮影のチームでセキュリティパーティーを開いて、全員で一緒に設定を済ませるのもおすすめです。

ICEを監視するすべての人のための実践

すべての人 このセクションは、パトロール、ICEの撮影、ホイッスルを鳴らすこと、同行支援など、ICEの活動に対する責任追及に関わるすべての人のためのものです。

15〜20分しかないなら、まずはこの項目から始めましょう。

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。

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。

社会運動や政治的な会話では、メッセージや通話の暗号化にSignalを使おう

通常の通話やSMSは秘密が保たれず、簡単に監視されて警察に提出されてしまう可能性があります

DO: Signal を使う

DO NOT: Facebook Messenger、Telegram、通常のSMSなどを使う（WhatsAppもできれば避ける。訳注：Lineも）

通常のSMSや通話のほとんどは、携帯電話会社や政府に見られる可能性があります。 Telegram はまったくもって安全でない。 （WhatsApp についての考え方は下記を参照。）

メッセージを安全に保ち、誰とやり取りしているかを秘密にするには、Signal が最善の選択肢。

SIGNAL の設定方法

1. スマホに Signal をインストール。
2. これで既存の連絡先に電話番号を使ってメッセージを送れます（相手も Signal をインストールしている必要あり）。まだ信頼関係のない新しい相手とやり取りする場合は、できるだけ電話番号ではなくユーザーネームを交換しよう。
3. 新しいメッセージを始めるには：Signalの右上にある「作成」アイコンを押して、相手の電話番号またはユーザー名を入力
4. 消えるメッセージをデフォルトで有効にする：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** → 適切な時間に設定。
5. セキュリティとプライバシーを最大限に高めるため、Signal セキュリティチェックリストに沿って設定を

Signal を使うべき場面

特に Signal を使いたい場面の例

- 公にしない抗議行動やアクションについて話し合うとき
- 公な抗議行動やアクションを組織するが、オーガナイザーが自分たちのプライバシーを守りたいとき
- 政府やその他の権力者を批判するとき

公の場で声を上げ続けよう！ セキュリティのために一部の会話をSignalに移すのは、沈黙するためではない。権力者への批判を公然と続けつつも、安全に組織活動をするため。あらかじめ服従してしまってはいけない。

WhatsApp はどう？（できれば避け、どうしても必要なときだけ使う。訳注：Lineも一緒）

WhatsAppのメッセージはSignalが開発した暗号化方式で保護されているため、メッセージの内容自体は安全です。ただし、Metaは誰とどのくらいの頻度でやり取りしているか、どのグループに入っているかといった情報を大量に収集しています。 2024年だけでも、政府からの要請の78%に応じてデータを提供しています。メッセージの中身は守られても、誰とやり取りしているかは守られません。一緒に活動しているコミュニティがSignalに移行しそうにない場合は、検討してもいい選択肢です。通常のSMSやTelegramなどよりは安全です。 WhatsAppを使う場合は、WhatsAppセキュリティチェックリストに沿って「Strict Account Settings」をオンにし、プライバシー設定をしっかり固めよう。

- [ ] 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。

Signalをできるだけ安全でプライベートに設定する

本名、本人の写真、メッセージのプレビューを隠して、ユーザー名を設定する

以下の手順は、デバイスが警察に押収された場合や、Signalグループ内の敵対者（警察や右派）があなたの身元を突き止めようとしている場合に、あなたを守るのに役立ちます。

以下のリストに、最も重要な手順をまとめました。より詳しい手順や上級者向けのステップは、Signalセキュリティチェックリスト →をご覧ください

SIGNALをより安全でプライベートに設定する方法

Signalの以下の設定を変更する：

- [ ] **消えるメッセージをデフォルトで有効にする：**
  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** → 好きな時間に設定（これは自分が始めたスレッドにのみ適用されます。）

- [ ] **表示名を本名以外に変更する：**
  Signalを開く → プロフィール写真をタップ → **設定** → 上部にある自分の名前/アイコンをタップ → 人のシルエットがある一番上の項目をクリック → プロフィールの表示名を編集

- [ ] **プロフィール写真を自分の顔以外に変更する：**
  Signalを開く → プロフィール写真をタップ → **設定** → 上部にある自分の名前/アイコンをタップ → **写真を編集** → ネットで見つけた、自分の身元、仕事、居場所、趣味・関心と関係のない一般的な写真をアップロード。

- [ ] **ユーザー名を作成し、電話番号の代わりにそれを共有する：**
  Signalを開く → プロフィール写真をタップ → **設定** → 上部にある自分の名前/アイコンをタップ → **@**マークをタップ → **ユーザー名を編集** → 自分の身元とまったく関係がなく、これまでどこでも使ったことのないユーザー名を設定。末尾は2桁以上の数字にする必要があります。（ツール：ランダムユーザー名ジェネレーター）。プライバシーを高めるために、電話番号の代わりにこのユーザー名を伝えましょう。
  例：`@CarefreeMoose.22`

- [ ] **通知でメッセージのプレビューを非表示にする：**
  Signalを開く → プロフィール画像をタップ → **設定**（Settings） → **通知**（Notifications） → **通知内容**（Notification Content） → **名前もメッセージも表示しない**（No Name or Content）を選択

- [ ] **電話番号を非表示にする：**
  Signalを開く → プロフィール画像をタップ → **設定**（Settings） → **プライバシー**（Privacy） → **電話番号**（Phone Number） → **電話番号を表示する相手**（Who Can See My Number）で **誰にも表示しない**（Nobody）を選択

- [ ] **シークレットキーボードを有効にする（Androidのみ）：**
  Signalを開く → プロフィール画像をタップ → **設定**（Settings） → **プライバシー**（Privacy） → **アプリのセキュリティ**（App security） → **シークレットキーボード**（Incognito keyboard）をオンにする

Signalを使い続けるうえでの習慣：

- ほかの人が新しいスレッド（またはグループ）を始めた場合、消えるメッセージがオンになっていないことがあります。相手が設定していなければ、そのスレッドで消えるメッセージを必ず有効にしましょう。
- 本当の電話番号ではなく、Signalのユーザー名を伝えましょう。

- [ ] **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。

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

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）を完全にオフにする

警察にスマホのロック解除を強制されそうになったときに、あなたを守ります。

警察は顔や指紋を使ってスマホのロックを解除させようとすることがあります（本来は令状が必要なはずですが、いつもそれが守られるとは限りません）。

生体認証よりもパスコードのほうが、法的に強い立場に立てます。

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

（その他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・指紋認証を使えば、毎回入力しなくても済むので、強いパスコードを使いやすくなるという面もあります。長いパスコードと生体認証のオフ、どちらかを選ばなければならないと感じるなら、より長いパスコードの方をおすすめします。

iPhoneのロックのヒント： 次のロック解除時にパスコード入力を必須にするには、サイドボタンをすばやく5回押すか、サイドボタンといずれかの音量ボタンを数秒間長押しします。

まずは試してみてください：設定によっては、この操作で緊急通報のカウントダウンが始まることもあります。この設定は変更できます。

注意：これをしても、警察が使うスマホのハッキングツールからデータを守ることはできません。それを防ぐ唯一の方法は、デバイスの電源を完全に切ることです。

Androidのロックのヒント： ほとんどのAndroidスマホでは、電源ボタンを長押しして、表示されたメニューで「ロックダウン」をタップすれば、顔認証・指紋認証によるロック解除を一時的に無効にできます。

iPhoneカメラのヒント： ロック画面で**左にスワイプ**すれば、ロックを解除しなくても写真を撮れます。（撮影中に逮捕された場合に備えて。）

Androidのカメラのヒント： ほとんどのAndroidスマホでは、電源ボタンをダブルプレスすると、ロックを解除せずにカメラを起動できます。

安全に撮影するために

すべての人　このセクションは、ICEやその他の政府職員を撮影するすべての人に向けたものです。

警察や当局を撮影する目的は二つあります：

1. **抑止** - 撮影で危害を防げるわけではありません。それでも、危害が起きる可能性を下げられることもあります。
2. **記録／責任追及** - 誰かが危害を受けたとき、裁判所や社会に示せる記録が手元に残ります。

警察や当局を撮影することは完全に合法であり、合衆国憲法でも守られた権利です。ACLUのビデオトレーニングもチェックしてみてください。

- [ ] **スマホのロックを解除せずに動画を撮る（左にスワイプするだけ！）**
  撮影中にスマホを押収されても、データを守れる

動画や写真の撮影中にスマホを没収されると、警察にすべてのデータを見られてしまうおそれがあります。

スマホはロックを解除しなくても写真を撮れるので、データをより安全に保てます。

スマホのロックを解除せずに撮影する方法

まず、顔認証によるロック解除をオフにしていることを確認しましょう。オンになっていると、ロック画面のままでもスマホが自動的にロック解除されてしまうことがあります。

IPHONE

ロック画面で**左にスワイプ**します。（またはカメラアイコンを長押しします。）

ANDROID

ロック画面で**左にスワイプ**するか、電源ボタンを素早く二度押しします（**設定** → **システム** → **ジェスチャー** → **カメラをすばやく起動**がオンになっている場合）。

- [ ] **ICEとの遭遇を撮った動画は慎重に共有する（すぐにネットに投稿しない）**
  状況によっては、投稿することで他のアクティビストが法的なリスクにさらされることも

DO: 共有・投稿する前に、アクティビストのネットワークと相談する

DO NOT: 撮影してすぐにネットに投稿する

警察とのやりとりを撮った動画は、私たちの活動にとってとても重要です。その一方で、アクティビストや他の人たちを法的なリスクにさらしてしまうこともあります。

投稿する前に、アクティビストのネットワークや運動に理解のある弁護士に相談しましょう。

動画や画像を安全に共有する方法

- **アクティビストのコミュニティに相談する：** 自分たちのコミュニティを守りながら、相手に責任を取らせるような動画の使い方を一番よく知っているのは、あなたのネットワークの人たちです
- **運動に理解のある弁護士に相談する：** あなたの活動に賛同してくれる地元の弁護士がいないか、コミュニティで聞いてみましょう。誰に相談すればいいかわからない場合は、CLDC（緊急対応ホットライン：541-603-6891）またはNLGに連絡してください。

- [ ] **動画や写真は安全に共有する（Signalなどで）**

DO: 暗号化された手段で写真を送る：Signal、Proton Drive、OnionShareなど

DO NOT: Google フォトやiCloudのようなクラウド共有サービスを使う

センシティブな動画や写真を信頼できるアクティビストや弁護士と共有するなら、安全な手段を使いましょう。AppleやGoogleのようなクラウド事業者は、裁判所の命令があればあなたのデータを警察に渡す可能性があります。

動画を安全に共有する方法

- Signal：Signalでメディアを共有するのが、いちばん簡単で安全です。「メタデータ」（位置情報など）も自動で削除してくれます。ただし、長い動画だと画質が落ちる点には注意してください。

  画質： Signalの設定で、メディア共有を「高画質」にしておきましょう。 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** → **メディアの画質** → **送信するメディアの画質** → **高画質**に設定

- Proton Drive：無料アカウントで最大5GBまでファイルを保存できます。
- OnionShare：大きなファイルをたくさん送る必要があるときに最適です。エンドツーエンド暗号化されています。受け取る側はTor Browserを使う必要があります。

上級編： さらに一段階強いセキュリティ・暗号化で動画を保存したいなら？ Tellaをチェックしてみてください。動画を特定の時刻に撮影したこと、そして改ざんされていないことを証明できる、検証可能なメタデータを追加したいなら？ Proofmodeをチェックしてみてください。

撮影には（できれば）スマホではなく「普通の」カメラを使うことも検討しよう

このページのデジタルセキュリティのアドバイスのほとんどは、スマホが押収されたり監視されたりする場合に関するものです。

スマホなしでも何とかなり、「普通の」カメラを用意できるなら、さらに安全性を高められます。

スマホの電源を完全に切っておけば、警察が使う監視ツールや「スマホハッキング」ツールからずっと守られやすくなります。

"普通のカメラ"で撮影する方法

選択肢1：スマホを持っていかない。 逮捕されたときに備えて、撮影中はスマホをまったく身につけないのが一番安全です。とはいえ、多くの人にとってスマホは欠かせないものでもあります。

選択肢2：スマホは持っていくが、電源を完全に切っておく。 強力なパスコードを設定し、最新のOSにしておきましょう。

検討したいカメラ：

- アクションカメラ（GoPro、Akaso、Crosstour など）
- ボディカメラ（BOBLOV など）
- コンパクトデジタルカメラを用意する
- または、サブのスマホを持っていくだけでもOK

写真の隠れた情報（位置情報など）を削除する投稿・共有する前に

共有する写真から、先にそのデータを削除しておかないと、位置情報や身元がバレてしまうことがあります

スマホで撮った写真や動画には、デフォルトで隠れたデータ（「メタデータ」）が含まれています。そこには正確なGPS位置情報、撮影日時、スマホの機種がわかる情報が入っています。

写真をネットに投稿すると、このメタデータを使って警察や右翼の敵対者に追跡され、身元を特定されるおそれがあります。

メタデータを残しておくべき場合： 不正行為や暴力（警察や右翼などによるもの）を記録しているなら、法的に使える可能性に備えて、メタデータ付きのオリジナルを保存しておきましょう。ただし、公開で共有するときは必ずメタデータを削除しましょう。

共有する前に写真から隠れた情報を削除する方法

おすすめ：Signalで送る

Signalで送った写真や動画は、メタデータがすべて自動で削除されます。

ネットで共有したい場合は、写真を自分宛てに送ってから、Signalから保存し直し、オリジナルを削除しましょう。

その他の安全な方法

- ウェブアプリのImage Scrubberでもメタデータを削除できます。ただし、画像のみの対応です。
- ExifCleaner - デスクトップアプリ（Mac、Windows）
- ImageOptim - Macアプリ

ICEを頻繁に監視する人のための対策

中程度の脅威 このセクションは、ICEの責任を追及する活動に頻繁に関わっているすべての人に向けたものです。より大きなリスクを負っているからこそ、セキュリティを強化することが大切です。

☐ 重要 **ICEウォッチや緊急対応にはサブのスマホを使うことを検討しよう**

スマホが押収されても漏れるデータが少なくなるので、自分とコミュニティを守れる

ICEウォッチや緊急対応の活動は、逮捕されるリスクが高くなります。自分だけでなくコミュニティの安全も守るための一番の方法は、押収されるスマホに入っているデータを**できるだけ少なくしておく**ことです。そのための一番簡単な方法は、リスクの高い活動をするときにサブのスマホだけを持っていくことです。

スマホをもう一台用意するのは誰にでもできることではないかもしれません。でも、まずは周りのネットワークに頼ってみてください。まだ使える古いスマホを眠らせている人は意外と多いものです。

サブのスマホがないからといって、この活動をあきらめる必要はありません。

サブのスマホに入れておくもの：

- 連絡を取る必要がありそうな人の電話番号（友だち、家族、子どもなど）
- その日の活動に関するSignalのスレッドだけ（他のSignalスレッドからはすべて退出し、DMはすべて削除）
- Magic Earthのようなプライバシーに配慮した地図アプリ
- ICEを記録した写真・動画（今日以外のものは、安全な場所に保存してから削除）
- …それ以外は、ほぼ何も入れない！

選択肢1：匿名性を高める方法

匿名性の高いサブのスマホを手に入れる方法

- より高い匿名性が必要なら、詳しいサブのスマホのガイドに従ってください。政治活動を理由に国家の監視（スマホの位置情報の追跡など）の対象になっているかもしれないと思う場合に役立ちます。このガイドを最後までやるには数時間かかります。

選択肢2：より手軽な方法

匿名性は低めのサブのスマホを手に入れる方法

上の選択肢1ほどの匿名性が必要ない人もいます。この手軽な方法では、スマホはあなたの身元と結びつきます。主な目的は、スマホに入れるデータを最小限にすること。そうすれば、押収されても一緒に活動する仲間を危険にさらさずに済みます。

1. **スマホを用意する：** どんなスマホでもOK。古いものがないか周りに聞いてみましょう。機械に詳しい友だちに、「SIMフリー」（どのSIMカードでも使える状態）かどうか確認してもらいましょう。
2. **回線を契約する：** Costco、Walmart、または近所の小さな店でプリペイドSIM（Tracfone、Mint Mobileなど）を買いましょう。または、今の契約に回線を追加する方法もあります。
3. **新しいApple/Googleアカウントを作る：** 普段のアカウントでログインしないこと。データが同期されてしまい、意味がなくなります。
4. **メインのスマホは家に置いていく：** リスクの高い活動には、サブのスマホだけを持っていきましょう。緊急時にはそちらに連絡するよう、親しい人たちに伝えておきましょう。
5. **データは最小限に：** このスマホをすべてのアクティビズム用にしないこと。押収されたら、結局危険なデータが残っていることになります。参加するのは当日用のSignalスレッドだけにして、全体の調整用チャンネルには入らず、自分のシフトが終わったらスレッドから抜けましょう。

注意： 緊急時のためにどうしてもメインのスマホを持っていく必要がある場合は、1) 電源を切っておく、2) オペレーティングシステムを最新の状態にしておく、3) 完全にランダムな8桁のパスコードを設定しておく、を必ず守りましょう。これらを組み合わせれば、警察がロックを破るのは難しくなります。

プライバシー重視の地図・ナビアプリを使う（Apple Maps または Magic Earth）

Google があなたのデータを警察に渡すのを防ぐ

DO: Apple Maps（iPhone のみ）または Magic Earth（無料）を使う

DO NOT: Google Maps を使う

位置情報の履歴からは、あなたの興味や交友関係、政治活動について多くのことがわかってしまいます。裁判であなたに不利な証拠として使われることもあります。

スマホは常に、どの基地局に接続しているかによって、おおよその位置を携帯キャリアに知らせています。でも、正確な GPS 位置情報を渡しているアプリは、それよりはるかに詳しい情報を持っています。

プライバシーを守ってくれる地図アプリを使えば、自分の身を守れます。

Apple Maps（iPhone のみ）は、意外なほど強力なプライバシー保護機能を備えていて、Google よりずっとプライバシーが守られます。ただし、巨大テック企業のサービスなので、慎重さが求められる組織活動ではなく、日常的な用途に向いています。プライバシー重視の他のアプリにはないリアルタイムの交通情報や公共交通機関の機能があるので、おすすめしています。

APPLE MAPSの設定方法（IPHONEのみ）

1. Apple Maps は最初からインストールされています（削除した場合は再インストールできます）。
2. **設定** → **プライバシーとセキュリティ** → **位置情報サービス** → **システムサービス** に移動し、**iPhone 解析、経路と交通状況、マップの改善** をオフにします。

Magic Earth（iPhone・Android 対応、無料）は、強力なプライバシー保護を備えています。もう一つのおすすめのクロスプラットフォームアプリ（CoMaps）よりも、ずっと使いやすいです。ただし、一部の機能は有料版でしか使えません。

MAGIC EARTHの設定方法（IPHONE・ANDROID）

1. Magic Earth をインストールする（無料。リアルタイムの交通情報は有料）
2. 使い方は Google マップや Apple Maps とほぼ同じです！

CoMaps（iPhone・Android 対応、無料）は、Magic Earth や Apple Maps ほど使いやすくはありませんが、プライバシー保護の約束は最も強力です。完全にオフラインで使えるので、慎重さが求められる活動をしているアクティビストには特に役立ちます。とはいえ、リアルタイムの交通情報や公共交通機関のルート検索がないので、メインのナビアプリとして使うのは難しいかもしれません。

☐ 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**、Androidでは**高度な保護機能プログラム**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。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。

重要 自動サービス（EasyOptOutsなど）を使って「人物検索」サイトから自分の情報を削除する

ツールを使ってこうしたサイトすべてから自動で情報を削除すれば、かなりの時間を節約できます。

DO: EasyOptOuts（年間20ドル）に登録する。より広くカバーしたいならOptery Ultimate（年間249ドル）

DO NOT: DeleteMeはEasyOptOutsより効果が低いので、おすすめしません

「人物検索」サイトは、「データブローカー」の一種です。公的・私的な記録から情報を集めて、ほぼすべての人の「プロフィール」を作り上げています。電話番号を持ったことがある、クレジットカードを使ったことがある、または投票したことがあるなら、たぶんこうしたサイトのどこかに載っています。

試してみよう： このサイトで自分の名前や電話番号を検索してみてください（登録なしですぐに結果が出るので、例としてこのサイトを使っています）。どれだけ多くの情報が簡単に手に入るか、ほとんどの人が驚きます。このカテゴリーの主なサイトには、Whitepages、Spokeo、BeenVerifiedのほか、増え続けるAIを使った検索ツールなどがあります。

なぜ自動削除サービスにお金を払うのか： この「オプトアウト」の手続きは手作業でもできますが、とんでもなく時間がかかるうえ、データブローカーのサイトが変わるたびに数か月ごとにやり直さなければなりません。プライバシーを守るためにお金を払わなきゃいけないなんてばかげていますが、そのぶん時間が浮いて、組織活動に集中できます。

どの自動削除ツールを使えばいい？

- **EasyOptOuts （おすすめ）** - 年間20ドル - 最も効果的なサービスのひとつで、しかも最安です。
- **Optery Ultimate** - 年間250ドル - 追加の出費に余裕があるなら、こちらのほうが少し効果的です。身分証のコピー（ID番号は消したもの）を預ければ、身分証が必要なサイトからもオプトアウトしてくれます。
- **DeleteMeはどう？** - 最も有名なサービスですが、プロフィールの削除率はわずか27%で、EasyOptOuts（65%）やOptery Ultimate（68%）に比べてかなり低い結果でした。（出典）。

EASYOPTOUTSを使って"人物検索"サイトから自分の情報を削除する方法

所要時間：5〜15分

1. **EasyOptOuts に登録する**（年間20ドル）
2. **個人情報を入力する：** 画面の指示に従ってください。いちばん大事なのは、**現在の**情報（住所、電話番号、メールアドレス）を入れることです。過去の住所を全部見つけられなくても大丈夫です。

   > **注意：** 活動専用に使っていて、すでに本当の身元と完全に切り離されている**偽名**や**使い捨て携帯の電話番号**は入力しないでください。このシステムの中でそれらが結びつけられるのは避けたいはずです。

3. 次のチェックリスト項目に進んで、EasyOptOutsが対応できないサイトの**手動オプトアウト**をしましょう。
4. 同じ家に住んでいる人にも登録してもらうよう頼むことを検討してください。一緒に住んでいることが知られたら、その人のことも同じくらい簡単に調べられて、あなたが狙われるかもしれません。

期間： 最初の削除が完了するまでに数日かかり、サイトによっては最大で数か月ほどかかることもあります。

ちなみに： リンクしている有料サービスから、私たちは一切手数料を受け取っていません。おすすめしているのは、私たちが見つけた中で一番効果的だからです。

EasyOptOutsのプライバシー： こういったサイトに自分の情報をすべて入力することに不安を感じる人もいます。データ漏洩と無縁なサイトはありませんが、これまでの実績と評判から、私たちはこのサイトを信頼しています。それに、削除を行うにはこうした情報が必要です。

代わりのツール：Kanary は、Googleであなたの個人情報を検索し、手動で削除する手順を案内してくれる無料アプリです。ただ、それでもかなり時間がかかるため、すべての削除を終える前に途中で挫折してしまう人が多いです。

☐ Clearview AIからオプトアウトして、警察による顔認識を難しくしよう

合法的な抗議活動を理由に警察があなたを犯罪者扱いするのを難しくする

移民・関税執行局ICEはClearview AIを使って、抗議者やオブザーバーを標的にしています。多くの警察機関も、令状なしの監視にこのプラットフォームを使っています。

Clearview AIからオプトアウトすることで、自分の身を守れます。（参考までに：ICEはオプトアウトできないほかの顔認識ツールにも投資しています。）

CLEARVIEW AIの顔認識からオプトアウトする方法

Clearview AIのオプトアウトフォームを送信する - 自分の写真を送る必要があります。

もどかしいことに、オプトアウトできるのはプライバシー法が成立している州だけです。

☐ 広告ブロック機能付きの信頼できるVPNアプリをインストールして、警察による令状なしの監視を難しくしよう

VPNを使うと、ウェブサイトがあなたを追跡しにくくなり、インターネットプロバイダーに通信を記録されるのも防げます。

DO: 信頼できるVPNアプリをデバイス（複数ある場合はすべて）にインストールして、常にオンにしておく。おすすめはIVPN（月額6ドル）です。

DO NOT: ネットで見つけた適当なVPNを使う。 Nord VPN、Surfshark、ExpressVPNなどは人気があるけれど、それほど信頼できるわけではありません。

インターネットに接続するたびに（スマホでもパソコンでも）、インターネットプロバイダー経由であなたのおおよその位置情報が、使っているすべてのサイトやアプリに伝わっています。

警察などの機関が、あなたのスマホのアプリや表示される広告から集めたデータを使って位置を追跡するツールを使っていることがわかっています。広告ブロック機能を有効にしたVPNを使えば、追跡はずっと難しくなります。また、信頼性が確認されたVPNは閲覧履歴を追跡しません。インターネットプロバイダーに記録された通信データは、警察が召喚状を取れば手に入れられてしまいます。

VPNは位置情報を隠すのに役立ち、身元を少しだけ特定されにくくしてくれます。

スマホで広告ブロックを有効にしたVPNを使えば、（広告ネットワークを通じた）令状なしの位置追跡を防ぐのに役立ちます。

VPNが実際に役立つ場面とそうでない場面について詳しくは、VPNのページをチェックしてください。

VPNを使っても完全に匿名になれるわけではありません。 より高い匿名性が必要なセンシティブな閲覧には、普段のブラウザとは別に、もう一つのブラウザとしてTor Browserを使うことを検討しましょう。

選択肢： ほとんどのアクティビストにおすすめのVPNはこちらです（検証済みVPNの全リストも参照）：

- **IVPN（一番のおすすめ）**：使いやすく、自動更新されます。
- **Proton VPN**には充実した無料プランがありますが、使えるのは1台のデバイスだけです。広告ブロックを使うには有料プランが必要です。（Protonを使う場合は、Protonを安全に使うためのガイドを参照してください。）

IVPNの設定方法

1. **アカウントを生成する：** IVPNにアクセスし、Generate IVPN Accountをクリックします（月額6ドルまたは年額60ドル）。 **Standard Plan**の下にある**Select**をクリックします（デバイスが2台を超える場合は**Pro Plan**を選んでください）。
2. **アカウントIDを控えておく：** パスワードマネージャーなど、安全な場所に保存しましょう。「パスワードを忘れた場合」のオプションはないので、なくしてしまうと誰も復元できません。
3. **支払う：** 月払いか年払いを選び、**Automatic renewal**のボックスにチェックを入れ、支払い情報を入力して**Make Payment**をクリックします。
   - クレジットカードの代わりにIVPNのバウチャーカードを注文することもでき、身元をさらに守れます。
4. **デスクトップアプリをインストール**し（Mac、Windows）、アカウントIDでサインインします。
5. **自動接続を有効にする：** ツールバーのIVPNを探す → **Show IVPN** → ⚙️ **歯車アイコン** → **Settings** → **General**を開き、**Launch at login**、**Autoconnect on launch**、**Allow background daemon to manage autoconnect**を有効にします。
6. **広告ブロックを有効にする：** IVPNアプリのメイン画面で**AntiTracker**をオンにして広告をブロックします（特にスマホでは、位置情報を守るのに役立ちます）。
7. **モバイルアプリをインストール**し（iPhone、Android）、同じアカウントIDでサインインして、上記と同じ設定をオンにします。 （iPhoneでは自動接続がデフォルトでオンになっているため、設定項目はありません。）

サイトへの接続に問題がある場合を除き、VPNは常にオンにしておくのがおすすめです（VPNを使うデメリットの一覧も見てください）。

Mullvadをもうおすすめしない理由： Mullvadは以前、アクティビストや危険にさらされやすい人たちの間で、おすすめVPNの第1位でした。VPNの技術そのものは今でもトップクラスです。でも最近、共同創業者の一人がスウェーデンの極右政党に数十万ドルを寄付したことで、その素晴らしい評判は台無しになってしまいました。なので、もうおすすめすることはできません。

グループのコーディネーターのための対策

高い脅威 **このセクションの対象：**

→ ICE監視ネットワークの中で**コーディネート**役を担っている人

→ 意図的に**表に立つ**役割を担っている人

上のセクションの項目もすべて実行しておきましょう。

アクティビズムにはGoogle DocsやGmailではなく、Proton DocsとProton Mailを使おう

知らないうちに行われる政府のデータ開示要求から、自分とコミュニティを守ろう。

DO: Proton DocsとProton Mailを使う

DO NOT: アクティビズムの連絡にGoogle DocsやGmailを使う

テック企業（Googleなど）は、アクティビストのアカウントデータをすべて引き渡すよう求める政府からの要求をよく受けています。こうした要求には「緘口令」が付いていることが多く、その場合、企業は数か月から数年後までユーザーに知らせることができません。

Proton Mail、Drive、Docs、Sheetsのような暗号化されたクラウドツールなら、運営会社があなたのデータを読める形で持っていないので、引き渡しを求められても渡せるものがありません。政府がデータを手に入れたいなら、あなた本人に直接要求しなければなりません。つまり、あなたは事前に通知を受け、法的サポートを受けながら異議を申し立てるチャンスを得られます。

> **暗号化メールの限界：** Protonはサーバー上のすべてのデータを暗号化しています。でも、暗号化によって送り手と受け手の両方が守られるのは、受信者も暗号化メールを使っている場合だけです。 Gmailユーザーにメールを送れば、Googleの手元にコピーが残り、それを引き渡される可能性があります。
>
> **機密性の高いやり取りには、必ずSignalを使いましょう。**消えるメッセージもオンにしておくこと。

PROTON DOCSとPROTON MAILの設定と使い方

Protonアカウントを作成する

> **おすすめ：** ランダムなユーザー名とランダムな表示名を選びましょう。そうすれば、このメールアドレスを自分が使っていることを明かさずに済みます。

1. 無料のProtonアカウントに**登録する**。
2. **認証：** 人間かどうかの確認を求められたら、「メール」ではなく「CAPTCHA」を選びましょう。そうすれば本当の身元と結びつきません。
3. 復旧用の電話番号やメールアドレスの設定を求められたら、**Maybe later**を選びましょう。

Proton Drive/Docs/Sheetsを使う

- Google Docsと同じように、ドキュメントを**共同で作成・編集**できます。直接共有するには、相手もProtonアカウントを持っている必要があります。
- **安全に共有する：** 「リンクで共有」は必要なときだけ使い、ドキュメントにパスワードを設定し、「公開リンク」には有効期限を設定しましょう。

Proton Mailを使う

- **Proton Mailを使う場面：** ウェブサイトのアカウント、ニュースレター、匿名性が必要な対外的な連絡、そして機密性の低い組織活動。
- **どんなメールも使うべきでない場面：** 誰かを法的なリスクにさらしかねない、本当に機密性の高いやり取り。
- **暗号化されるもの・されないもの:** Proton Mailユーザー同士のメッセージは、自動的にエンドツーエンド暗号化されます。ほかのメールサービスを使っている人へのメッセージは暗号化されませんが、パスワード保護付きメールを送ることはできます。

CryptPadも暗号化ドキュメントの選択肢として人気ですが、使いこなすのはかなり大変です。必要な機能がそろっていれば、同じ結果が得られます。

> **Protonを安全に使うために:** ProtonはGmailやGoogle ドキュメントと比べて大きな改善ですが、知っておくべき実際の限界もあります。何が暗号化され、何がされないのか、そしてよくある落とし穴を避ける方法については、Protonを安全に使うためのガイドをチェックしてください。

「顔検索」サイトからオプトアウトする

写真から身元を特定されないように身を守ろう。

「逆画像検索」サイトからオプトアウトすることで、自分の身を守れます。そうすれば、ネット上のプロフィール写真から本名を突き止められにくくなります。本名がわかると、上で紹介した人物検索サイトで見つけられてしまう可能性があります。

"顔検索"サイトから自分の情報を削除する方法

どのサイトも、（皮肉なことに）顔写真のアップロードを求めてきます。削除してもらいたいなら、これは避けられない必要悪です。相手にさらにデータを渡すリスクと、オプトアウトできるメリットを比べて、やる価値があるかどうかを自分で判断する必要があります。

> **身分証明書のアップロードについての注意**：これらのサイトの中にはひどいものもあり、機密情報を隠した状態の身分証明書やパスポートの写真のアップロードを求めてきます。一番簡単なのは、身分証明書の名前と写真以外の部分をすべてテープで隠してから撮影する方法です。

オプトアウトすべきサイト：

1. Clearview.aiからオプトアウトする - 必要なのは写真だけで、身分証明書は不要です。もどかしいことに、オプトアウトできるのはプライバシー法が成立している州だけです。 **Clearviewは主に警察が使っているため、オプトアウトしておくことが重要です。**
2. PimEyesからオプトアウトする - 身分証明書の写真が必要です。 （ID番号は必ず隠して！）
3. FaceCheck.IDからオプトアウトする - 身分証明書の代わりに、二本の指をあごに当てて撮った自撮り写真をアップロードすることもできます。また、削除してほしい写真を自分で一つずつ選ぶ必要があります。

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

iCloudの「高度なデータ保護」（iPhone）またはGoogleの「高度な保護機能プログラム」を有効にする

Apple、Googleなどのサービスは、アカウントやデータを狙った標的型攻撃から守るための追加のセキュリティ機能を提供しています。これらが守るのは各社のオンラインアカウントで、デバイスそのものではありません。

Appleの「高度なデータ保護」を使うと、ほとんどのコンテンツでエンドツーエンド暗号化が有効になります。

メール／クラウドアカウントで高度な保護を有効にする方法

データを守る：

- iCloudの「高度なデータ保護」 - iCloudに保存されているほぼすべてのデータでエンドツーエンド暗号化が有効になり、政府の裁判所命令から情報を守れます。復旧キーは必ずとても安全な場所（パスワードマネージャーなど）に保存しておきましょう。

アカウントを守る：

- Googleの「高度な保護機能プログラム」 - フィッシングや不正アクセスからアカウントを守るのに役立ちます。
- MicrosoftのAccount Guard
- Proton Sentinel

☐ Signalで電話番号から自分を見つけられないように設定する

Signalでは初期設定で電話番号が表示されないようになっていますが、それでも誰かがあなたの電話番号を入力すれば、あなたを見つけることができてしまいます。嫌がらせを受けるリスクがある場合は、電話番号の代わりにSignalのユーザー名だけを伝えるようにするのもひとつの手です。

SIGNALで電話番号から自分を見つけられないようにする方法

1. **ユーザー名を変更したい場合：** Signalを開く → プロフィール写真をタップ → **設定** → 上部にある自分の名前/アイコンをタップ → @ マークをタップ → **ユーザー名を編集** → 自分の身元や、これまでどこかで使ったことのあるユーザー名とは**まったく関係のない**ユーザー名に設定する。最後は2桁以上の数字で終わる必要があります。
2. **電話番号を非表示にする：** Signalを開く → プロフィール写真をタップ → **設定** → **プライバシー** → **電話番号** → **電話番号を表示できるユーザー** で **誰にも表示しない** を選択。
3. **電話番号から見つけられないようにする：** Signalを開く → プロフィール写真をタップ → **設定** → **プライバシー** → **電話番号** → **電話番号で私を検索できる人**で → **該当者なし**を選択。
4. Signalで誰かとつながりたいときは、電話番号ではなくユーザー名を伝えましょう。

☐ グループチャットは少人数にして、消えるメッセージのタイマーを短く設定する

50人のチャットは、押収されたり、なくしたり、侵入されたりする可能性のあるスマホが50台あるということ。そのうちどれか1台でも破られれば、会話全体が漏れてしまいます。大きなSignalグループが必要なときもありますが、組織活動のすべてをひとつの大きなグループチャットで回すのはやめましょう。アクションやプロジェクト、センシティブな意思決定など、特定のことを調整するときは、本当に必要な人だけで小さなグループを作り、メッセージがすぐに消えるように設定しましょう。

SIGNALグループを少人数に保つ方法

- そのプロセスに直接関わる人だけで**小さなグループを作る**。
- **消えるメッセージのタイマーを短く設定する**（進行中の調整なら1時間〜1日、継続的な活動でも最長1週間）。メッセージは相手が読んでからカウントが始まって消えるので、場合によっては1時間に設定しても大丈夫です。
- 調整が終わったら**グループを削除するか退出する**。消し忘れた古いチャットがないか、ときどき見直して整理しましょう。ほかのメンバーにも退出と削除を呼びかけましょう。

☐ 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。

☐ オンライン上の個人情報やソーシャルメディアのアカウントを整理して、嫌がらせやドクシングから身を守る

政府や右翼の荒らしが、公開されているデータを使ってあなたを標的にするのを防ごう。

政府はソーシャルメディアの追跡ツールを使い、令状なしでアクティビストを監視しています。右翼の敵対者は「人物検索」サイトやソーシャルメディアを使って、私たちを怖がらせ、組織活動をやめさせようとしています。

個人情報を消しておけば、こうした攻撃の標的になりにくくなります。

ドクシングから身を守る方法

こうしたドクシングや嫌がらせから身を守る方法については、詳しいガイドを用意しています。

ドクシング対策チェックリスト →

そのガイドの中から、特に重要なステップをいくつか紹介します：

1. EasyOptOuts（年20ドル）を使って「人物検索」サイトからオプトアウトする
2. Block Partyを使ってソーシャルメディアのアカウントをロックダウンする（無料、またはプロモコードJOINTHEPARTY を使えば年50ドル）

よりリスクの高いアクティビストのための対策

高い脅威 **このセクションの対象：**

→ 移民のアクティビスト（在留資格の有無を問わず）や、肌の色や外見のせいで、監視活動中にICEの標的にされるリスクが高くなりうる人

上のセクションもあわせて済ませておきましょう。

☐ 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。

- [ ] **逮捕されたとき（または自宅にいて身の危険を感じたとき）の緊急時プランを作ろう**
  前もって計画しておけば、ストレスの大きい状況でも少しは乗り切りやすくなります。

反対の声を上げることがますます犯罪化されている今、逮捕される可能性や、敵対する相手によって自宅で身の危険を感じる可能性に備えておくことは大切です。

緊急時プランの立て方

簡易版の緊急時プラン

ガイドの「ミニ版」が必要なら、まずは次の質問に答えてみてください：

1. **あなたのサポートネットワークには誰がいる？** もし今夜逮捕されたら、誰に電話しますか？その人の電話番号を暗記していますか？
2. **ハイリスクな状況になったら誰に知らせる？** シンプルなSignalグループを使うとうまくいきます。
3. **その人たちは必要なものを持っている？** ほかに連絡すべき人のリスト、あなたの医療情報、法律相談ホットラインの番号を持っていますか？あなたのペットや子どもなどの世話をするために必要なものはそろっていますか？
4. **自宅で身の危険を感じたら、どこに行く？** 身の危険を感じて今夜家を出なければならなくなったら、どこに泊まりますか？その人はそのことを知っていますか？

詳細版の緊急時プラン

余裕があれば、緊急時ガイドの完全版にも取り組んでみることをおすすめします。

個人の緊急時プランのチェックリスト →

その他のリソース

- **ラピッドレスポンスや徒歩パトロールのグループを立ち上げるには：**
  - ベイエリアのラピッドレスポンスガイドとzine
  - ミネアポリスのガイド
  - ミネアポリスから学んだこと
  - シャーロットのツールキット（Googleドキュメントのリンク）
  - Dignity Toolkit - コミュニティにすでにあるリソース同士をつなげる方法
- **安全：**
  - Vision Change Winによるリスク評価とコミュニティの安全のためのツールキット
  - Kala Mendozaによる安全のためのリソース
  - ストリートメディック101：入門講座
  - Riot Medicine Handbook：暴動医療ハンドブック

関連ガイドでさらに学ぼう

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。

緊急時への備え

拘束されたり脅威にさらされたときに備え、緊急時の支援ネットワークをつくろう。