セキュリティの基本

最終更新日： **2026年7月18日**　所要時間の目安： **45分**

ACTIVIST CHECKLIST

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/essentials/

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]。

アクティビストを守るうえで最も効果的なステップ：メッセージには Signalを使う 。位置情報が不要なアプリでは共有をオフに。プライバシー重視のBraveなどのブラウザやDuckDuckGo などの検索エンジンに切り替える。そしてスマホに強力なパスコードを設定する。これで一番大きなリスク範囲をカバーできます。チェックリストの残りは、さらに一歩進みたい人向け。

クリック、メッセージ、位置情報の一つひとつがデジタルの痕跡を残し、アクティビストやオーガナイザーに対して不利な形で使われることがあります。警察は、社会を変革しようと活動する人々を特定・監視するために、テック企業にデータの提出を日常的に求めています。

このガイドは、デジタルの痕跡を最小限にするためのもの。 これらのステップで完全に姿を隠せるわけではないものの、当局が次のことをするのはかなり難しくなります：

- 居場所や行動パターンを追跡する
- 通信や政治的な議論を監視する
- 人間関係やネットワークを洗い出す
- 活動やつながりのプロファイルを構築する

仲間と一緒だと取り組みやすい。 ほとんどの人は、いつかやろうと思いつつ、結局やらずじまいになりがち。友達とセキュリティパーティー[2]を開いて、このリストに一緒に取り組んでみませんか。90分の時間を使って、おやつをつまみながら、コミュニティ全体の安全につながる確かな前進を。

はじめよう

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。

この四つのステップは30分以内でできて、すぐにプライバシーを大きく強化できます。何よりもまず、ここから始めよう。

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[3]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[4]。

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。

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。

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[5]。 （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[6]。
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[7]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[8]

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[9]。

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%[10]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[11]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[12]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。

普段のブラウジングには（Chromeではなく）プライバシー重視のブラウザを使う

トラッキングを最小限にして、デジタルな痕跡を減らす。

DO: Brave Browser[13]（いちばん簡単）かFirefox[14]（設定が少し必要）を使う

DO NOT: Google ChromeやMicrosoft Edgeなどを使う

おすすめは**Brave**。追加の設定なしで最も高いプライバシー保護が得られるからです。それこそがこのサイトの目指すところです。

Braveの設定に関するおまけのヒント：

- 保護を少し強化するなら、Privacy Badger[15]をインストールしましょう。
- iPhone[16]やAndroid[17]向けのBraveアプリもインストールできます。

その他のブラウザの選択肢：

BRAVE BROWSERの設定方法

Braveはプライバシー重視のブラウザで、Google Chromeの拡張機能もインストールできます。

1. パソコン（またはスマホ[18]）に**Braveをインストール**[18]します。
2. 起動したら手順に従って、Chromeや他のブラウザ[19]から設定をインポートします。（プラグインによって身元を特定されやすくなる点について、下の警告を参照してください。）
3. **プライバシー設定を行う：**デスクトップ版ブラウザでBrave → **設定** → **シールド**を開き、次の項目を選択します（モバイルアプリにはこれらの設定がすべてあるわけではありません）：
   - 「Trackers & ads blocking」で**Aggressive**を選択
   - 「Upgrade connections to HTTPS」で**Strict**を選択
   - **Social media blocking**の項目のチェックをすべて外す
   - （任意）**Forget me when I close this site**を有効にします。（モバイルアプリでは「Shred Site Data」という名前の設定です）ブラウザをリセットした後、サイトはあなたに関する情報を何も保存できなくなります。

     これで、サイトがネット上であなたを追跡しにくくなります。プライバシーには効果的ですが、特定のサイトでは手動で例外にしたほうがいい場合もあります。サイトにアクセス → URLバーにあるBrave（ライオン）のロゴをクリック → **Advanced controls** → **Forget me when I close this site** をオフにする

任意：

1. うっとうしい新しいタブページをオフにする：Brave → **Settings** → **Get started** → **New Tab Page** → ドロップダウンから **Blank page** を選択
2. ツールバーの項目をオフにする：Brave → **Settings** → **Appearance** → **Toolbar** → 不要なツールバーボタンをすべてオフにする（Brave Rewards、VPN、Wallet、Leo AIなど）

プラグインに関する警告：プラグインをインストールするたびに、あなたのブラウザは「その他大勢」の中で目立つようになり、身元を特定されやすくなります。その結果、Braveに組み込まれたプライバシー機能の効果が弱まってしまいます。

- **Firefox**は、時間をかけて適切なプラグインを入れてきちんと設定すれば[20]、さらに高いプライバシー保護が得られます。
- 非常にセンシティブな内容を本当に匿名で閲覧したいときは、**Tor Browser**[21]を使う

Google検索をやめて、Brave Searchのような検索エンジンを使おう

検索履歴からは、あなたの関心や政治的な傾向がかなり見えてしまいます。

DO: Brave Search[22]やDuckDuckGo[23]のような、プライバシーを尊重する検索エンジンを使う。

DO NOT: Google検索、Bing、Yahooなどを使う。

- **Brave Search**は検索結果の質が比較的よく、私たちも信頼していますが、そのビジネスモデルに賛同できない人もいます
- **DuckDuckGo**は検索結果の精度ではやや劣りますが、プライバシー面での実績は少しだけ上です。

プライベート検索の設定方法

- **Brave Search:** Braveブラウザを使っているなら、最初からデフォルトになっています。ほかのブラウザを使っている場合は、こちらの手順[24]に従って設定できます。
- **DuckDuckGo:** こちらの手順に従って、DuckDuckGoをデフォルトの検索エンジンに設定しましょう[25]。

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[26]（iPhone のみ）または Magic Earth[27]（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[28]、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[26] 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[27]（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[27] 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[29]（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。

基本の対策

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。

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[30]
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[30]
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[30]
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[30]
3. **Microsoft Store アプリ：** 自動更新[31]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。

「人物検索」サイトから自分の情報を削除して、ドクシング（ネット上の嫌がらせ）から身を守ろう

あなたの自宅の住所や電話番号は、すでに何十ものウェブサイトで公開されている可能性が高いです。

「人物検索」サイトは、私たちの名前、住所、電話番号、プロフィール写真、メールアドレス、SNSアカウントなどを集めて、プロフィールとして公開しています。下のリンク先のチェックリストで、自分の情報を削除する方法を紹介しています

ドクシングは、アクティビストに対してますます頻繁に使われるようになっている手口です。悪意のある人物があなたのメールアドレスや電話番号、住所などを公開し、ネット上で、ときには直接、他の人たちにあなたへの嫌がらせをさせようとします。

ドクシングから身を守る方法

1. まずは、ドクシング対策チェックリストの**最初の三つの項目**を済ませましょう。

   ドクシング対策チェックリスト →

2. その後、チェックリストの残りの項目にも取り組んでいきましょう。

パスワードマネージャーを使い、パスワードを使い回さない

複数のサイトで同じパスワードを使っていると、そのうちひとつのサイトがハッキングされただけで、ハッカーが他の多くのアカウントにもアクセスできてしまいます。弱いパスワードを使っていると、警察があなたを狙いやすくなります。

DO: おすすめは 1Password[32]（月額3ドル）または Bitwarden[33]（無料）

DO NOT: パスワードを使い回したり、AIが生成したパスワードを使ったりする。 LastPass の使用はおすすめしません[34]。

時間があるなら、パスワードマネージャーを使うのがベストです。サイトやアプリ、アカウントごとに、強力でランダムな、使い回しのないパスワードを自動で作ってくれます。

強力なパスワード（長くてランダム）と、使い回さないパスワード（サイト間で同じパスワードを使わない）のどちらかを選ばなければならないなら、使い回さないパスワードを優先しましょう。そうすれば、ひとつのサイトでパスワードが盗まれても、他のすべてのサイトに被害が広がるのを防げます。

おすすめのツールはこちら：

- **1Password**：とても使いやすい。セキュリティ面でやや優れている。月額3ドル。
- **Bitwarden**：無料。こちらも十分に安全。

1PASSWORD の設定方法

1. **ダウンロード：**1Password をダウンロードしてインストール[35]（月額3ドル）
2. **マスターパスワード：**パスフレーズ生成ツール[36]を使って、強力でランダムな「マスターパスワード」を作成します。覚えやすいものにしつつ、他の場所では使っていないパスワードにしましょう。マスターパスワードはデジタルで保存せず、紙に書き留めておきましょう。覚えられたら数週間後にその紙を処分できるよう、リマインダーを設定しておきましょう。
3. **インポート：**パソコンやブラウザから既存のパスワードをインポート[37]します
4. **アプリ：** パスワードの保存や自動入力に役立つブラウザ拡張機能[38]とモバイルアプリ（iPhone[39]、Android[40]）をインストールしましょう
5. **パスワードの変更：**似たようなパスワードを使い回していた場合は、1Password に内蔵されたランダムパスワード生成機能を使って、特に重要なパスワードから変更しましょう。

これらの手順の動画は、1Password のスタートガイド[41]で見られます。

おまけ：1Password を最大限に活用する方法[42]についてのわかりやすい入門記事はこちら。

その他の選択肢：

- Proton Pass[43]：無料プランあり
- KeePassXC：[44]オープンソースで、パスワードをクラウドではなく自分のデバイスだけに保存できる。ただし、操作画面はかなり使いにくい。

☐ 二要素認証を有効にする

もしパスワードを盗まれても、二要素認証を使っていれば、相手があなたのスマホも持っていない限りログインされずに済みます。

DO: 重要なサイトでは二要素認証を有効にする

DO NOT: パスワードだけに頼る

パスワードを入力したあと、本当にあなた本人であることを証明するために、スマホに表示されるコードを入力します。家に入るのに、鍵と警報システムの暗証番号の両方が必要なようなもの。両方そろわないと誰も入れません。

二要素認証でいちばん守るべきアカウントはメールです。攻撃者にメールに入られると、ほかのパスワードを全部リセットされてしまいます。

設定方法

認証アプリをインストールする：

1. **オプション1：1Password：** 1Passwordを使っているなら、「authenticator（認証）」機能が組み込まれています。詳しくはこちら[45]。
2. **オプション2：Ente Auth：** Ente Auth[46]をインストールする（iPhone、Android）
   - 任意：アカウントを作成することもできます。データはエンドツーエンドで暗号化されます。アカウントを作らずに使うこともできますが、スマホのバックアップを取っていないと、ワンタイムパスワードを失ってしまうおそれがあります。

二要素認証の設定方法：

1. セキュリティ／プライバシーの設定を開く
2. 「2FA」「二要素認証」「二段階認証」「多要素認証」といった項目を探す
3. 「認証アプリ」のオプションがあれば、それを選びましょう！（バックアップコードは、パスワードマネージャーなど安全な場所に必ず保存しておきましょう。）
4. 「テキストメッセージ／SMSによる認証」しか選べない場合は、それを選んで指示に従ってください。
5. よく使われるサイトの2FA設定ページへのリンク：
   - Google[47]
   - Apple ID[48]
   - Facebook[49]
   - Twitter / X[50]
   - Instagram[51]
   - または、2FA Directory[52]で、ウェブサイトやサービス、アプリが2FAに対応しているか調べることもできます。

注：サービスによっては、**認証アプリ**と**SMSの認証コード**のどちらかを選べる場合があります。そのときは、いつでも認証アプリを選ぶのがベストです。攻撃者にSMSを傍受される[53]可能性があるからです。

☐ 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[54]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[54]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[54]のリンクを参照してください。

☐ 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[55]とProton Mail[56]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[57]引き渡すよう求める政府からの要求[58]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[56]、Drive[59]、Docs[55]、Sheets[60]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[61]とランダムな表示名[62]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[63]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[64]を送ることはできます。

CryptPad[65]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[66]をチェックしてください。

強化した対策

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。

☐ ノートパソコンの暗号化を有効にする

ノートパソコンが暗号化され、十分に強力なパスワードで守られているか確認しましょう。

強力なパスワードを使い、顔認証や指紋認証によるロック解除をオフにして、ディスク暗号化を有効にすれば[67]、ノートパソコンやその他のデバイスの中身にアクセスするのはとても難しくなります。こうした防御に欠かせないのが**暗号化**です。暗号化していなければ、国家にデバイスを押収されたとき、パスワードなどの対策はほとんど意味をなしません。

ノートパソコン（とバックアップ）の暗号化を有効にする方法

ノートパソコンでは、暗号化を自分で有効にする必要がある場合があります：

MACOS

システム設定 → **プライバシーとセキュリティ** [一番下までスクロール] → **FileVault** → **オンにする...** をクリック

復旧キーはパスワードマネージャーなど、安全な場所に保存しておきましょう。セキュリティを最大限に高めるなら、iCloudを使った復旧は有効にしないでください（ただしその場合、パスワードを覚えておき、絶対に失くさないようにする必要があります！）

WINDOWS

設定 → **プライバシーとセキュリティ** → **デバイスの暗号化** → **オン**

また、**外付けハードドライブ**や作成したバックアップも、暗号化がオンになっているか確認しましょう。

スマホの暗号化： iPhoneと最近のAndroidスマホは、最初から暗号化されています。

☐ 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**[68]、Androidでは**高度な保護機能プログラム**[69]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[70]。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。

☐ スマートスピーカー（Alexa、Google Homeなど）を家から撤去する

リスクの高い立場にいるなら、マイクの近くで政治活動について話すときは常に気をつけましょう。これにはノートパソコン、スマホ、スマートウォッチ、そして**スマートスピーカー**も含まれます。

リスク： これらのデバイスには、常に音を拾っているマイクが搭載されています。

身を守るには： スマートスピーカーを家から撤去するのは、監視される可能性を減らすための簡単な一歩です。

ほとんどの人は、ほとんどの時間、積極的に監視されているわけではありません。それでも、監視されているかもしれないと想定する習慣をつけておくほうが安全です。慣れてしまえば、それほど手間はかかりません。

スマートスピーカーを撤去する方法

1. **スマートスピーカー**や、**マイクがついていてインターネットに接続されているもの**は、とにかく手放しましょう。「音声操作」「Alexa/Googleアシスタント対応」「アシスタント内蔵」といった表記を目印にしてください。たとえば次のようなものです：
   - Amazon Alexa（Echo、Dotなど）
   - Google Nestスピーカー、Google Home
   - Sonosなどのホームスピーカー
   - スマートサーモスタット（新しいモデルの中にはマイクや音声アシスタントを内蔵しているものもあります）
   - スマートテレビやストリーミングデバイス（お使いの機器にマイクが内蔵されているかどうか調べてみてください。内蔵されていれば、買い替えを検討しましょう。）
2. 音楽用のスピーカーが必要なら、マイクがまったくついていないものを探しましょう。あるいは、マイクはついていてもインターネットには接続されないシンプルなポータブルBluetoothスピーカーでもかまいません（使わないときは電源を切っておきましょう）。

買い替える場合は、電子ごみや資源採掘を減らすために中古品を選ぶのがおすすめです。

背景：

- 2017年には、CIAが一部のスマートテレビを、電源が切れているように見えるときでも常に盗聴できる状態にする[71]ハッキング手法を開発していたことが明らかになりました。
- また、Amazonは警察からスマートスピーカーの録音データを求める法的要請[72]を頻繁に受けています。

スマホを守るためのガイドを最後までやり通す

アクションのオーガナイザーは、国家による監視のターゲットになりやすい立場にあります。だからこそ、より多くの対策をとることが大切です。

やり方

抗議行動に備える[73]チェックリストの項目をすべて実行する（「強化セキュリティ」のセクションも含めて）

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[74]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。

怪しいリンクはクリックしない

何をクリックするかに気をつけることで、スパイウェアから身を守れます

スパイウェア[4]は、あなたを狙って、つい開かずにはいられないように作り込まれたリンク付きのメッセージやメールで届くことがよくあります。これはただのスパムではありません。あなたにとって一番大切なものにつけ込む、あなたを狙い撃ちにした攻撃です。

怪しいリンクの見抜き方と対処法

迷ったら：リンクをクリックしない！

1. 代わりに、送り主（企業でも友人でも）に別の方法（電話する、別のアプリを使うなど）で連絡して、本当に送ったのか確認しましょう。確認に2分かけるほうが、クリックしてデバイスを乗っ取られるよりずっといい。
2. bit.lyやtinyurl.comのような短縮URLの場合は、ExpandURL.net[75]を使ってリンク先のページを確認できます。ただし、そのページがスパイウェアでないという保証にはなりません。本当のURLを確認できるので、信頼できるかどうかをより正しく判断できるようになるだけです。
3. リンクがすでに悪意のあるものとして報告されているかを確認したいときは、VirusTotal[76]（Google/Alphabet傘下）のようなフィッシング・マルウェアのデータベースにリンクを貼り付けて調べることができます。VirusTotalは誰でも検索できる公開データベースなので、送信するのは公開されていて個人情報を含まないリンクだけにしましょう。

要注意のサイン：

- **知らない番号からのメッセージ：** 連絡先に登録していないサービスからメッセージが届くことはよくあるので、本物かどうかを見分けるのは簡単ではありません。連絡先にない相手からなら、より慎重に対応しましょう。
- **焦りや恐怖をあおる**：「アカウントがロックされます」「緊急セキュリティ警告」「家族の緊急事態」
- **見慣れないドメイン名：** スパイウェアのメッセージは、`adsmetrics[.]co` のような変なドメインから届くことが多い
- **個人的すぎる**：あなたの活動、最近参加したイベント、知り合いなどに触れてくる。冷静な判断をさせないための手口
- **予想外のメッセージ**：知り合いから説明なしにリンクが届く、いつもと違う言い回し、変な時間帯に届く（相手のアカウントが乗っ取られているかも）
- **短縮URL**：`bit.ly`、`tinyurl.com` など、本当のリンク先を隠す短縮サービス
- **URLの微妙なスペル違い**：`google.com` ではなく `goog1e.com`

スパイウェアのメッセージは、特定の人を狙い撃ちにしていることがあります。 Pegasusスパイウェアが実際に使われた例をいくつか紹介します：

> 「カルメンへ　弟が事故で亡くなりました。とても辛いです。葬儀の情報を送ります。来てもらえたら嬉しいです：[スパイウェアのリンク]」（出典[77]）

> USEMBASSY.GOV/ あなたのビザに問題が見つかりました。至急大使館までお越しください。詳細を見る [スパイウェアのリンク]（出典[77]）

> LX 1955 BCN-ZRH 26Jun2020 - リンクをクリックしてモバイル搭乗券を受け取ってください [スパイウェアのリンク]（出典[78]）

注意： スパイウェアの中には、リンクをクリックしなくても感染させる攻撃（「ゼロクリック攻撃」）を使うものもあります。たとえば、WhatsAppの不在着信として現れることもあります。

「[Google、Facebookなど]でログイン」は使わない

DO: 新しいサイトに登録するときは、自分のメールアドレスでちゃんとアカウントを作る

DO NOT: 「[Google、Facebookなど]でログイン」を使う

「Googleでログイン」（やそれに似たオプション）を使うたびに、どのサービスを使っているかをGoogleに追跡させ、それをあなたの本当の身元と結びつけさせることになります。（パスワードマネージャーを使って）それぞれ固有のパスワードで別々のアカウントを作れば、企業や当局があなたのオンライン活動の全体像をつかむのが難しくなります。

関連ガイドでさらに学ぼう

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。

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。

アクティビストのためのVPN 16分で読めます 79
セキュリティアップデート確認ツール 30
Protonを安全に使う方法 17分で読めます 66
リンクのトラッキングを削除する 3分で読めます 80
Signalは安全？ 5分で読めます 81
Apple IntelligenceはSignalのメッセージを読んでいる？ 6分で読めます 82

リンク

1. activistchecklist.org/ja/contribute/
2. activistchecklist.org/ja/party/
3. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
4. activistchecklist.org/ja/spyware/
5. blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/
6. signal.org
7. support.signal.org/hc/en-us/articles/6829998083994-Phone-Number-Privacy-and-Usernames-Deeper-Dive
8. activistchecklist.org/ja/signal/
9. penguinrandomhouse.ca/books/558051/on-tyranny-by-timothy-snyder/9780804190114/excerpt
10. atomicmail.io/blog/is-whatsapp-safe-the-truth-about-your-privacy
11. activistchecklist.org/ja/whatsapp/
12. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
13. brave.com
14. mozilla.org/en-US/firefox/
15. privacybadger.org
16. apps.apple.com/us/app/brave-private-web-browser-vpn/id1052879175
17. play.google.com/store/apps/details?id=com.brave.browser&hl=en
18. brave.com/download/
19. support.brave.com/hc/en-us/articles/360019782291-How-do-I-import-or-export-browsing-data
20. privacyguides.org/en/desktop-browsers/
21. activistchecklist.org/ja/research/
22. search.brave.com
23. duckduckgo.com
24. search.brave.com/default
25. duckduckgo.com/duckduckgo-help-pages/change-default-search-engine/
26. apps.apple.com/us/app/apple-maps/id915056765
27. magicearth.com
28. youtu.be/alodEeY6YAM?t=137
29. comaps.app/privacy/
30. activistchecklist.org/ja/updates/
31. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
32. 1password.com
33. bitwarden.com
34. forbes.com/sites/daveywinder/2023/03/03/why-you-should-stop-using-lastpass-after-new-hack-method-update/
35. support.1password.com/get-the-apps/
36. strongphrase.net
37. support.1password.com/import/
38. 1password.com/downloads/browser-extension/
39. 1password.com/downloads/ios
40. 1password.com/downloads/android
41. support.1password.com/explore/get-started/
42. unwall.app/www.nytimes.com/wirecutter/guides/how-to-use-1password/
43. proton.me/pass
44. keepassxc.org
45. support.1password.com/one-time-passwords/
46. ente.io/auth/
47. myaccount.google.com/signinoptions/two-step-verification
48. support.apple.com/en-us/HT204915
49. facebook.com/settings?tab=security
50. twitter.com/settings/security
51. help.instagram.com/566810106808145
52. 2fa.directory/us/
53. unwall.app/www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/
54. strongphrase.net/passcode
55. proton.me/drive/docs
56. proton.me/mail
57. cldc.org/google-is-a-fcking-snitch/
58. theintercept.com/2025/09/16/google-facebook-subpoena-ice-students-gaza/
59. proton.me/drive/
60. proton.me/drive/sheets
61. strongphrase.net/username
62. strongphrase.net/identity
63. account.proton.me/signup
64. proton.me/support/password-protected-emails
65. cryptpad.fr
66. activistchecklist.org/ja/proton/

67. arstechnica.com/tech-policy/2026/02/fbi-stymied-by-apples-lockdown-mode-after-seizing-journalists-iphone/
68. support.apple.com/en-us/105120
69. landing.google.com/intl/en_us/advancedprotection/
70. activistchecklist.org/ja/lockdown/
71. cnet.com/tech/home-entertainment/weeping-angel-hack-samsung-smart-tv-cia-wikileaks/
72. legalexaminer.com/ksmith/home-family/smart-speakers-offer-new-legal-challenges-as-privacy-goes-public/
73. activistchecklist.org/ja/protest/
74. activistchecklist.org/ja/secondary/
75. expandurl.net
76. virustotal.com/gui/home/url
77. citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
78. citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
79. activistchecklist.org/ja/vpn/
80. activistchecklist.org/ja/links/
81. activistchecklist.org/ja/signal-secure/
82. activistchecklist.org/ja/signal-ai/