旅行とフライトのセキュリティ

ACTIVIST CHECKLIST

最終更新日： **2026年3月23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/travel/

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]。

米国市民は国境でスマホのロック解除を拒否できますが、端末が留め置かれる可能性があります。ビザ保持者や旅行者が拒否すると、入国を拒否される可能性があります。保安検査の前にスマホの電源を切り、長くランダムなパスコードを使い、生体認証でのロック解除をオフにしておくこと。紙の書類を持参すれば、税関を通過するまで端末の電源を切ったままにできます。リスクの高い旅行者は、データを最小限にしたサブのスマホの利用を検討してください。

このチェックリストの対象者：

- ✅ **海外へ**渡航し、米国の国境を越えて入国または再入国する人（陸路・空路・海路を問わず）。
- ✅ 米国内の**国内線**での移動にも、このチェックリストが役立つかもしれません。検査を受けたり不利な扱いを受けたりするリスクが高まる可能性があるためです（特に米国市民でない場合）。
- ❌ このチェックリストは、**米国市民権を持たず、強制送還のリスクがある米国在住の人向けには作られていません**。さまざまな在留資格を持つ移民として飛行機に乗る際のアドバイスが必要な場合は、こちらのリソースを参照してください：Immigrants Rising[2]、National Immigration Law Center[3]

以下のステップは米国への入国時・出国時のどちらにもおすすめしますが、**米国に入国するとき**のほうがはるかに厳しくチェックされるため、最も注意すべきなのはそのタイミングです。これらのステップを一度しか実行しないなら、必ず米国に入国するときにしてください。

セキュリティの基本[4]チェックリストもあわせて実行することをおすすめします。

空港でのICE： 2026年7月現在、ICE（移民・関税執行局）は空港でより多くの人を拘束しているようです。亡命申請が審査中の人も含まれています。いくつかの例：有効なビザを持ち、亡命申請が審査中の人がデンバーで飛行機に搭乗しようとしたところ拘束された件[5]、ラスベガスでの拘束未遂[6]、ボストンでの二件の拘束[7]。

このガイドの要約版

旅行の前に、サブのスマホを持っていくか、デバイスをバックアップして初期化するか、デバイスから機密性の高いものをすべて消去しておきましょう。スマホの電源は切っておき、生体認証をオフにして、ランダムに生成したパスコードを使いましょう。自分の権利を知っておきましょう。米国市民ではなく米国への入国を予定している場合は、ビザを申請する前にSNSのプロフィールを非表示にすることを検討してください。リスクが高い場合は、法律の支援チームを確保し、信頼できる連絡先と安否確認の計画を立てておきましょう。

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。

これまで耳にしたデバイス検査のほとんどは、国境の警察がスマホを手作業で見て回り、気に入らないもの（政権への批判、パレスチナへの支持など）を探すというものでした。たいていはスマホのロックを解除するよう指示され、相手はあなたが従うことを当てにしています。米国市民であれば、スマホのロックを解除したり、要求に従ったりする義務はありません。市民でない場合、要求に従わずスマホのロックを解除しないと、出身国へ送り返されるリスクがあります。

- [ ] **国境を越えるときに知っておくべきあなたの権利**
  あなたの権利は移民ステータスによって変わります

  免責事項：これは情報提供のみを目的としたもので、法的助言ではありません。自分の状況についてのアドバイスは弁護士に相談してください。

以下に情報をまとめましたが、細かいニュアンスを理解するためにも、これらの記事を読んでおくことを強くおすすめします。

自分の権利を知るために、以下の記事を読んでおきましょう：

- stop AAPI HateのKnow Your Rights旅行ガイド[8]
- The Vergeの今、スマホを持って旅行しても安全？[9]
- 国境警備官は電子機器を検査できるのか？話は複雑[10]

> 空港や国境では、あなたのステータスに関係なく、**国境警察は令状なしでどんな電子機器でも検査できます**。スマホのロック解除を拒否できるかどうかは、移民ステータスによって変わります。

米国市民：

- 米国への**入国を拒否されることはない**
- **答える必要があるもの：** 身元と市民権に関する質問のみ
- **拒否できるもの：** 機器の検査やその他の質問（ただし、足止めされることは覚悟しておきましょう）。機器を没収される可能性があります
- **権利：** 国境で弁護士をつける権利

グリーンカード保持者：

- **入国を拒否されることはない**（移民裁判官による審問なしには）
- **答える必要があるもの**：身元と永住権に関する質問
- **拒否できるもの**：その他の質問や機器の検査（ただし、足止めされたり、強制送還手続きにかけられたりする可能性があります）
- **手放さないこと**：グリーンカード。圧力をかけられても渡してはいけません

ビザ保持者：

- 検査や質問を拒否すると**入国を拒否される可能性がある**
- **答える必要があること**：入国したい場合、渡航内容・経歴・渡航目的に関する国境警察の質問にはすべて答えなければなりません。
- **デバイスの検査**：拒否するとビザの取り消しや強制送還につながる可能性がある

拘束されて取り調べを受けた場合：

- **絶対に嘘をつかない** - ささいな虚偽の説明でも刑事訴追につながる可能性がある
- **落ち着いて**、事実を話す
- **すべてを記録する** - 担当官の名前、バッジ番号、聞かれた質問
- 誰かに知らせるために**電話を一回**かけられる場合があります。
- **受領書をもらう：**デバイスが返却されない場合は、後で行方を追えるように受領書をもらいましょう。

質問に答えないことのメリットとデメリットを知っておく：

- 基本的には常に警察とは話さない[11]ことをおすすめしていますが、国境での状況はもっと複雑です。国境では、市民権を持つ人も持たない人も、認められる権利が少なくなります。

- US市民であれば、（上に挙げた基本的な質問以外は）答えを拒否できますが、長時間の取り調べを受けたり、デバイスが返却されなかったりする可能性があります。
- グリーンカード保持者（永住者）やビザ保持者の場合、リスクはさらに高くなります。上にリンクした記事を読んで、自分の権利について把握しておきましょう。

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

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[1][2]
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[1][2]
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[1][2]
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[1][2]
3. **Microsoft Store アプリ：** 自動更新[3]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。

重要 セキュリティチェックポイントに近づく前に、スマホとノートパソコンの電源を完全に切る

豆知識：データが最も安全なのは、スマホやノートパソコンを起動後に一度もロック解除していない状態で電源を切ったとき。

ほぼすべてのスマホ（と一部のノートパソコン）は、デフォルトで暗号化されています。警察はデバイスを押収すると、暗号化を回避しようとします。警察にとって一番侵入しにくいのは、電源が完全に切られた（そしてOSが最新の状態にアップデートされている）デバイスです。起動後にパスコードやパスワードが一度でも入力されていると、警察はずっと簡単にデータを抜き出せるようになってしまいます。

暗号化とは、データがスクランブルされ、パスコードやパスワードを知らない人には読めない状態になっていることです。

スリープにするだけではダメ：画面が真っ暗でも、デバイスはスリープしているだけかもしれません。

デバイスの電源を完全に切る方法

iPhone： サイドボタンと**音量を下げる**ボタンを長押し → **スライドで電源オフ**

Android： 電源ボタンを長押し → **電源を切る**

ノートパソコン：

- システムメニューから**シャットダウン**を選択します。
- 緊急時には、ほぼすべてのノートパソコンで電源ボタンを5〜10秒長押しすれば、強制的に電源を切れます

デバイスの電源を切る：電源を完全に切ったデバイスは、画面をロックしただけのデバイスよりはるかに安全です。

生体認証にも効果あり：デバイスの電源を入れた直後の最初のロック解除には生体認証が使えないため、電源を切っておけばチェックポイントを通過する間は**実質的に生体認証が無効になります**（ただしWindows Helloを使うものは例外なので、移動時はオフにしておきましょう）。

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**[14]**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[14]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[14]のリンクを参照してください。

☐ 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[15]、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。

紙の搭乗券と渡航書類を印刷しておく

保安検査や税関を通るあいだ、スマホの電源を完全に切っておけるように。

DO: スマホの電源を切って、紙の搭乗券を使う

DO NOT: スマホを搭乗券として使う

渡航書類を印刷する方法

1. 搭乗券はたいてい空港で印刷できます
2. 観光ビザや就労ビザ、税関申告書などのほかの渡航書類については、紙で対応できるよう余裕をもって準備しておきましょう。国によっては、アプリを使わないと手続きがかなり面倒になることもあります。

空港での顔認証を拒否する（そしてマスクを着用する）

政府があなたのプロファイルを作りにくくなります

DO: 身分証明書を渡す前に、「顔認証を拒否します」と英語で伝えましょう：「I want to opt out of facial recognition」

アメリカでは、市民には保安検査（TSA）を通過する際に顔認証を拒否する権利があります。 2026年1月以降、アメリカへの入国時と出国時には、市民でない人は顔認証に応じることが義務付けられています[16]。

TSAは、ほとんどの場合24時間以内に写真を削除すると主張しています。でも、これまでにも他の顔認証システムで大規模なデータ漏洩[17]が何度も起きていて、同じことがここでも起こりえます。義務付けられている身分証明書やパスポートの写真以上に、政府に顔をスキャンさせても、あなたが得るものは何もありません。

YK HongのInstagramのリール動画[18]では、顔認証の拒否のしかたと、それがなぜ大切なのかを紹介しています。生体情報の盗用[19]に関する彼らのコンテンツもおすすめです。

空港で顔認証を拒否する方法

顔認証を求められたら、毎回拒否できますし、そうするべきです：

- 保安検査（TSAなど）
- 搭乗ゲート（ゲートで顔認証を使っている航空会社もあります）
- 入国審査・出国審査（写真を撮るカメラがありますが、拒否できます）。

拒否するのは簡単です：

1. 英語で**「I want to opt out of facial recognition.」**と伝えるだけです。意味は「顔認証を拒否します」です。
2. **係員があなたの申し出を受け入れるまでは、身分証明書を渡したり、スキャナーに入れたりしないでください。**そうしないと、顔認証の手続きから抜けられなくなることがあります。
3. さらに身を守るために、空港内では**マスクを着用しましょう**。マスクを着用している場合は、TSAの係員が身分証明書の写真と顔を照合できるよう、マスクを下げる必要があります。
4. どうすればいいかわからないときは、近くの係員に英語で「I'd like to opt-out of facial recognition, where do I go to do that?」と聞いてみましょう。「顔認証を拒否したいのですが、どこに行けばいいですか？」という意味です。たいていは手動検査用の別の列に案内されます（そのほうが早く通れることもあります！）

強化した対策

中程度の脅威 移民問題やパレスチナなど、政府が標的にしている問題について積極的に声を上げている人は、このセクションが参考になるかもしれません。

注意 - データを削除しても消えたわけではありません： このセクションではアプリやデータの削除を勧めています。ただし、政府はフォレンジックツールを使って、削除されたあとのデータにもアクセスできます。そのため、以下のガイダンスで確実に身を守れるのは、相手がデバイスを手作業で調べる場合だけです。ただし、米国の国境ではそれが最もよくあるケースです。

リスクが高く、警察がスマホやパソコンのデータにアクセスするためにより多くのリソースを投じるかもしれないと思う場合は、ここにある内容に加えて、下の注目度の高い人向けの保護セクションのステップも必ず実行してください。

- [ ] **スマホとノートPCから、機密データが入ったアプリ（メール、ドキュメント、SNSなど）をアンインストールする**
  警察に簡単に調べられたくないものは、すべて削除しましょう。

デバイスに入っているものは、少なければ少ないほどいい。

アンインストールすべきアプリ

機密データが入っているなら、以下のアプリを（スマホとノートPCの両方から）アンインストールすることを検討しましょう：

- メール・カレンダーアプリ（スマホの標準アプリを使っている場合は、スマホの**設定** → **アカウント**からサインアウトする必要があるかもしれません）
- ドキュメント・メモ（Google Docs、Evernoteなど）
- その他のコミュニケーションアプリ（Slack、WhatsAppなど）
- Googleマップ（せめてロケーション履歴をオフにする[20]）
- SNSアプリ

ヒント：アプリを非表示にする： アプリを非表示フォルダに移動することもできます。やり方：iPhone[21]、Android[22]。ただし、警察のほとんどはこのフォルダもチェックすべきだと知っているので、効果はわずかです。削除するほうがはるかに安全です。

残しておくアプリについても、**特定のコンテンツを削除**しておくといいでしょう：

- iOSの標準「メモ」アプリ内のメモ
- 個別のテキストメッセージのスレッド
- 見られたくない写真は非表示アルバム[23]に移動する（または、どこかにバックアップしてからデバイスから完全に削除する）

> **ゴミ箱を空にする：** 写真、メモ、メール、ドキュメントを削除しても、「ゴミ箱」や「最近削除した項目」フォルダに30日間保存されていることがよくあります。必ずそこを開いて、すぐに手動で削除しておきましょう。

- [ ] **リスクのある状況に入る前に、Signalのメッセージをバックアップしてアプリを削除する**

Signal[24]のメッセージには機密性の高い内容が多く、政府の監視から守りたいものです。

スマホが押収されたり調べられたりするかもしれない状況に向かうとき、Signalのバックアップ機能[25]を使えば、メッセージを安全に守ることができます。

Signalのデータをバックアップして、Signalを削除する

SIGNALのデータをバックアップして、SIGNALを削除する方法

1. **Signalのバックアップを有効にする**： Signalを開く → プロフィール画像をタップ → **設定** → **バックアップ** → **バックアップを有効にする**
2. **リカバリーキーを保存する**： リカバリーキーのコピーを安全な場所に保存しましょう。 1Passwordのようなパスワードマネージャー[4]の利用をおすすめします。
   - できるだけ安全にしたいなら、信頼できる友人や家族にリカバリーキーを送っておき、あとでバックアップを復元するときに読み上げてもらう方法もあります（そうすれば、どこにもデジタルで保存されません）。
3. **リカバリーキーを確認する**：保存したことを確かめるため、Signalがリカバリーキーの入力を求めてきます。
4. **プランを選ぶ**：ほとんどの人は「無料」プランで十分です。直近45日分より前のメディア（写真・動画・添付ファイル）も必要な場合は、有料プランにアップグレードできます。
5. 次に**今すぐバックアップ**をタップして、バックアップを開始します。
6. **Signalを削除する**： 最後に、スマホからSignalアプリを削除します。こうすれば、端末が押収されてもデータにアクセスされにくくなります。

リカバリーキーは厳重に管理しましょう。 このキーを手に入れた人は、あなたのSignalのメッセージをすべて読めてしまいます。

ノートパソコンも忘れずに：ノートパソコンを持っていく場合、Signalのデスクトップ版をインストールしているなら、そちらのアプリも削除しておきましょう。

データの削除は完全とは限らない：Signalを削除すると、関連するデータもすべて削除されます。ただし、国家が手段を選ばず本気で取り組めば、端末から削除したデータを復元できてしまう場合もあります。非常にリスクの高い立場にいる場合は、メインのスマホでSignalを削除する代わりに、データを最小限にしたサブのスマホ[26]を使うことを検討してください。

Signalのデータを復元する

Signalのデータを復元する準備ができたら、次の手順で復元できます：

SIGNALのデータを復元する方法

1. スマホにSignalアプリを再インストールします。
2. 手順に従って電話番号を確認します。
3. 表示されたら**バックアップから復元**を選んで、Signalのデータを復元します。
4. 求められたら、復旧キーを入力します。

- [ ] **パスワードマネージャーをアンインストールする（ログイン情報のバックアップを忘れずに！）**

スマホとノートパソコンの両方からアンインストールしてください。

パスワードマネージャーを使っていない場合：パスワードの保存に使っている方法（メモやスプレッドシートなど）を削除しましょう。ただし、必ず別の場所にバックアップしておくこと！！

ヒント： 1Passwordを使っているなら、移動に必要なもの以外のすべての保管庫にトラベルモード[27]を使うだけでOKです。以下の手順は飛ばしてください。

パスワードマネージャーを安全に削除する方法

1. すべてのデバイスからアプリをアンインストールする場合は、マスターパスワードを覚えている（または書き留めている）ことを**絶対に**確認してください。 1Passwordを使っている場合は、「Secret Key[28]」も書き留めて、安全な場所に保管してください。持ち物が検査されることはないと思うなら、この情報を持って移動してもかまいません。
2. 二要素認証（2FA）にスマホのアプリを使っている場合、そのコードは削除しないでください。コードは復元が難しく、しかもパスワードも知られていない限り役に立たないものです。

移動中にパスワードが必要な場合：

- マスターパスワード（該当する場合は1PasswordのSecret Keyも）を紙に書き留めておく。パスフレーズは目立たないように隠しておく（紙の日記や手帳の中など）。国境を越えたら、またログインする。使い終わったら、その紙はすぐに燃やす。
- または、パスフレーズ（またはその一部）を信頼できる人に預けておき、安全な場所から安全な手段（Signalなど）で共有してもらう方法もあります。

SNSアカウントを非公開にするか、一時停止する

SNSアカウントをネットで調べられた場合（デバイスがなくても調べられます）に身を守るのに役立つ

あえて広く公開されたSNSでの存在感を保とうとしているのでない限り、少なくとも一時的にはアカウントのセキュリティを固めておくのがおすすめです。（プライバシーとセキュリティをさらに高めるために、長期的にそうすることも考えてみてください。できるなら、アカウントをきっぱり削除してしまうのもひとつの手です。）

ビザ申請者の方へ： 学生ビザ以外のビザを申請する場合は、申請する前に必ずSNSを非公開にしておきましょう。オーストラリア人ジャーナリストのケース[29]からわかるように、渡航の1週間前まで待っていると、すでにネットで調べられてしまっている可能性があります。

学生ビザ申請者の方へ： 2025年6月、米国務省はすべての学生ビザ申請者にSNSのプロフィールを公開にすることを義務付け[30]始めました。これに当てはまる場合は、Block Party[31]のようなツールを使って、過去の投稿を実際に削除しておくといいかもしれません。

SNSアカウントを非公開にする・一時停止する方法

手順：

1. **X / Twitter：** 非公開にする[32]またはアカウントを一時停止する[33]
2. **LinkedIn：** 非公開にする[34]またはアカウントを一時停止する[35]
3. **Instagram：** 非公開にする[36]またはアカウントを一時停止する[37]
4. **Facebook：** 非公開にする[38]またはアカウントを一時停止する[39]
5. **TikTok：** 非公開にする[40]またはアカウントを一時停止する[41]
6. ブログ記事やYouTube動画など、ほかの公開投稿も非公開にすることを検討しましょう。

この作業にはBlock Party[31]を使うと便利です。また、Cyd.social[42]を使えば、先に手元に非公開のバックアップを作っておくこともできます！

> 政府から投稿を隠しておけば、より安全にアメリカに入国できるかもしれません。それでも、投稿や抗議活動、ボイコットを通じて公の場で声を上げ続けることは必要です。黙っていれば個人としては身を守れるかもしれませんが、それは私たちが闘っている権威主義的なシステムを助けることになってしまうからです。

CBP（税関・国境警備局）やTSA（運輸保安局）に、SNSのアカウント名を伝える義務はありません。「答えたくない」「その質問が渡航とどう関係するのかわからない」と伝えてかまいません。どんな質問に対しても、聞かれていない情報を自分から話さないようにしましょう。

- [ ] **機密性の高い情報があるウェブサイトからログアウトする（スマホとパソコンの両方）**
  ログインしていなければ、パスワードを明かさないことについて法的に主張しやすくなります

ログアウトすべきウェブサイト

スマホ**と**ノートパソコンの両方でログアウトするのを忘れずに。

ログアウトすべきウェブサイト：

- メールとカレンダー（仕事用と個人用）
- ドキュメント（Google Drive など）
- SNS
- 掲示板・フォーラム（Reddit など）

そのほか、警察に見られたくないものすべて。

- [ ] **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[26]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。

☐ 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[43]（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[44]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[45]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[46]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[45]も参照）：

- **IVPN**[47] **（一番のおすすめ）**：使いやすく、自動更新されます。
- **Proton VPN**[48]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[49]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[50]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[51]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[52]、Windows[53]）、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[54]、Android[55]）、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[45]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[56]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。

注目度の高い人向けの対策

高い脅威 **このセクションは、次に当てはまる人向けです：**

→ 出生による米国市民ではない。

→ アクティビズムや組織活動など、政権に対抗する活動をしていて、**影響力のある立場**にいる、または**世間から注目されている**。

→ 政権に対して非常に公の場で声を上げてきた著名人（アーティスト、科学者、人権弁護士など）である。

→ ほかにも、国境を越える一般的な人より自分が標的になりやすいと考える理由がある。

このセクションでは、国境の係官がさらに踏み込んで、フォレンジック抽出ツール[57]を使ってデバイスをハッキングしようとする可能性を想定しています。この場合のベストな方法は、サブのデバイス（「使い捨てスマホ（burner phone）」や「旅行用ノートPC」と呼ばれることもあります）を持っていくことです。入国を拒否されたり、デバイスを無期限に押収

されたりする可能性があるので、国境の係官にロックを解除して見せられるデバイスだけを持って移動することを目標にしましょう。デバイスを手から取り上げられたり、目の届かないところに持っていかれたりするのは、できる限り避けてください。

☐ サブのスマホを用意する（中に入れる情報はできるだけ少なく）

データがほとんど入っていないスマホを持っていけば、たとえ中を見られても大きな問題にはなりません。

サブのスマホを用意する方法

サブのスマホ用チェックリスト[26]の手順に沿って進めつつ、次の点だけ変えてください：

1. アメリカの電話番号のSIMを用意する代わりに、行き先の国で使えるプリペイドSIMを事前に買えないかネットで調べましょう。

   または、現地に着くまではSIMも電話番号もなしでWi-Fiだけでスマホを使い、到着してから空港の近くでSIMカードを買う方法もあります。 eSIM対応のスマホなら、alosim.comが便利かもしれません。

   - この方法はアメリカを出国するときだけにしてください。アメリカに再入国するときは、税関を通る前に、空港のWi-Fiか使えるSIMで緊急連絡先と連絡が取れる状態になっているか必ず確認しておきましょう。
2. サブのスマホ用チェックリストにもあるとおり、端末には本当に必要な最低限の情報だけを入れておきましょう。
3. 新しい電話番号（新しいSIMカードの番号）でSignalを設定する場合は、本当に必要な連絡先だけを追加するようにしてください。
4. メールやSNSなど、センシティブな情報があるウェブサイトには絶対にログインしないこと。

別の方法： サブのスマホを用意できない場合は、スマホ全体を**クラウドではなく**パソコンにバックアップする方法もあります（iPhone[58]、Android[59]）。そのうえでスマホを初期化して、旅行中はその状態で使います。帰ってきたら、もう一度初期化してからバックアップを復元すればOKです。この方法をとる場合は、バックアップのバックアップを別の場所にも必ず保存しておいてください。 iPhoneの場合、「高度なデータ保護」をオンにしていれば、クラウドへのバックアップも安全だと考えてよいでしょう。

☐ サブのノートパソコンを用意する（必要な場合）

ノートパソコンなしでもなんとかなるなら、そのほうが安全です。旅行中にノートパソコンが必要なら、サブのデバイスを用意して、そこに入れるデータはできるだけ少なくしておくのがおすすめです。

サブのノートパソコンをセットアップする

1. 友達から使っていない古いものを譲ってもらうか、ネットで安いものを買いましょう。
2. デバイスを工場出荷時の状態にリセットする（Mac[60]、Windows[61]）
3. いつも使っているApple/Microsoftアカウントにはサインインせずにデバイスをセットアップする（サインインすると、大量のデータがパソコンに同期されてしまうおそれがあります）。
4. インストールするのは、入っているデータを国境の係官に見られても問題ないアプリだけにする。
5. Signalやパスワードマネージャーのようなセキュリティ系のアプリや、Google Drive（デスクトップ版）やGmailのように大量の情報が入っているアプリは、ダウンロードもインストールも絶対にしない。
6. メールやSNSなど、機密性の高い情報があるウェブサイトには絶対にサインインしない。

国境を越えたあとにアプリを追加でインストールした場合は、再び国境を越える前に必ず削除しておきましょう。

心配なのがアメリカの国境を越えることだけなら（アメリカからリスクの低い渡航先へ行く場合）、旅行にはいつものノートパソコンを使い、アメリカに戻る前に工場出荷時の状態にリセットする、という方法もあります。これで「サブのノートパソコン」と同じ役割を果たせます。この場合は、上記のステップ2から始めてください。

普段使いのノートパソコンを旅行用として使う場合は、出発前に**ノートパソコンを完全にバックアップ**しておきましょう。そして工場出荷時の状態にリセットする前に、**残しておきたい旅行中の作業をすべて**安全なクラウドに**同期**する計画を立てておきましょう（機密性の高いものにはProton Driveが最適ですが、それほど機密性が高くなければGoogle Driveなどでも大丈夫です）。まず、ノートパソコンのディスクが暗号化されていることを確認しましょう。

ノートパソコンにランダムなパスフレーズを設定する（持っていく場合）

デバイスの暗号化の強さは、パスフレーズの強さで決まります。自分で考えたパスフレーズは、ランダムに生成されたものよりずっと破られやすい可能性が高いです。

ランダムに生成したパスワードをノートパソコンに設定する方法

1. StrongPhrase.net[62]などのサイトを使って、コンピューターでランダムなパスフレーズを生成する
2. デバイスのパスワードを変更する：

MACOS

システム設定 → **ユーザとグループ** → 自分のアカウントの横にある丸い「i」アイコン ℹ️ をクリック → **変更...** をクリック

そのあと、上で生成したパスフレーズを使います。

WINDOWS

設定 → **アカウント** → **サインイン オプション** → **パスワード** → **変更** → 現在のパスワードを入力

そのあと、上で作成したパスフレーズを入力します。

2人以上の緊急連絡先を決めて、安全計画を立てる

国境で拘束されたときに、助けてくれる人がいるようにしておきましょう。

国境を越えるときの安全計画の立て方

1. **連絡先：** 2〜3人に緊急連絡先になってもらうよう頼む
2. **連絡先情報：** その人たちの電話番号は必ず暗記しておきましょう。できれば出発の一週間以上前にやっておくのがおすすめです。
3. **グループ：** 緊急連絡先の人たち同士をつないでおきましょう。あなたをサポートする必要が出たときに連携できるようにするためです。
4. **出発・到着の情報：** 出発・到着の時刻と便名を伝えておきましょう。遅延があった場合に、オンラインでフライトを追跡してもらえます。
5. **法的な情報：** 政府発行の身分証の番号、パスポート番号、法的なフルネーム、生年月日も伝えておきましょう。拘束されたときに役立つことがあります。
6. **通信環境：** 空港でWi-Fiが使えるか、使えるSIMカードがあるかを必ず確認しておきましょう。
7. **法的サポート：** あなたが拘束された場合に、どうやって法的サポートを探せばいいかを伝えておきましょう。すでにつながりのある弁護士を決めておくか、活動家を支援している弁護士の探し方を伝えておきましょう（ACLU[63]やNLG[64]をチェック）。特にリスクが高い場合は、事前に弁護士と連絡を取り、緊急連絡先が誰なのかを伝えておきましょう。
8. **連絡の計画：** 国境で米国の税関・入国審査を通る前と後に、**いつ、どうやって**連絡するかを伝えておきましょう。あなたから連絡がなかった場合に**どう動けばいいか、はっきりした手順**を共有しておきましょう。

たとえば：

> 「飛行機が着陸したら、税関を通る前にSignalでメッセージを送ります。 555-123-4567から送ります。Signalのグループはもう作ってあります。最後に連絡してから1時間以上たっても連絡がなかったら、私の法的サポートに知らせてください。弁護士が戦略的に有効だと判断したら、公に支援を呼びかけてください。植物に水をやって、職場には移動中に足止めされていると伝えてください。」

連絡を取る必要がある人の連絡先を書き留めておく

連絡先を手動で管理する方法

1. メインのスマホから連絡先をすべて同期するのではなく、旅行中に必要になる大事な連絡先だけを紙に（またはデジタルで）書き留めておきましょう。電話番号とメールアドレスも書いておきましょう。
2. どの電話番号やメールアドレスから連絡するのかを相手に必ず伝えておきましょう。また、なりすましではなく本人だと確認できるように、確認用の質問と答えを事前に決めておくのもおすすめです。

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[65]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[66]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[67]。

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。

- [ ] **このガイドの最初の二つのセクションのステップをすべて実行する**

サブの端末を使う場合でも、上の基本のセキュリティ対策と中レベルのセキュリティ対策のセクションにあるステップはすべて必要です。

さらに詳しく

- 今、スマホを持って旅行しても安全？（英語）[9] - The Verge（2025年）
- 米国の国境を通過する前のデバイスの準備（英語）[68] - Freedom of the Press Foundation（2025年）
- 米国国境におけるデジタルプライバシー（英語）[69] - Electronic Frontier Foundation（2017年）
- 空港での顔認証はオプトアウト（拒否）することを強くおすすめします（米国市民のみ）。自分の権利を知るために、こちらの印刷用カード（英語）[19]をチェックしてください。さらに詳しく知りたい人は、YK Hong（Instagram[70]、ブログ[71]）をフォローしてください。

よくある質問

米国の国境でCBP（税関・国境警備局）にスマホを検査されることはある？
はい。米国税関・国境警備局（CBP）は、国境を越えるあらゆる電子機器を令状なしで検査する権限があると主張しています。ほとんどの検査は手作業で、職員がスマホの中身をスクロールして見ていきます。一部はフォレンジック検査で、端末を抽出ツールに接続し、削除済みのコンテンツも含めてデータを抜き取ります。

国境の職員にスマホのロック解除を求められたら、応じなければならない？
米国市民は拒否しても入国は認められますが、端末がさらなる検査のために留め置かれることがあり、それが数週間に及ぶこともあります。永住権保持者にも同様の権利がありますが、より強いプレッシャーを受けます。ビザ保持者や旅行者が拒否すると、入国を拒否され、送り返される可能性があります。自分の在留資格を把握し、それに合わせて計画を立てること。拒否することがリスクになるなら、サブのスマホを検討してください。これは一般的な情報であり、法的助言ではありません。法律やCBPの方針は変わります。自分の状況については弁護士に相談してください。

国境を越えるときはバーナーフォン（使い捨てスマホ）を使うべき？
リスクの高い旅行者にとって、データを最小限にしたサブのスマホは、現実的に取れる最も強力な対策です。目的は怪しく見えることではなく、検査されたときに職員が見られる情報を限定することです。到着前に電源を切り、長くランダムなパスコードを使い、いかにも空っぽなスマホではなく、自然に見えるように設定しておきましょう（実際に使うアプリや本物の写真をいくつか入れておくなど）。

機内モードにすれば位置情報は隠せる？
いいえ。機内モードがオンの間は無線通信が止まりますが、スマホはGoogle マップやiOSの「利用頻度の高い場所」、さまざまなアプリに、数週間から数か月分の位置情報を記録しています。デバイスを検査されると、その履歴を抜き取られる可能性があります。これを防ぐには、空港に着いてからではなく、事前に位置情報の履歴を削除し、位置情報にアクセスできるアプリを制限しておきましょう。

ビザを申請する前のSNSはどうすればいい？
政治的な投稿は、フライトの直前ではなく、ビザを申請する前に非公開にするか隠しておきましょう。最近の入国拒否の事例では、係官がパレスチナや移民政策についての過去の投稿や、政権を批判する投稿を読んだあとに拒否されています。ビザが承認されたら、たいていはまたオープンにしても大丈夫です。ただし、領事官には広い裁量権があることを忘れずに。

国境でのデバイス検査の報告

読むと怖くなるような話もありますが、国境を越える人たちが直面している具体的な脅威を理解する助けにもなります。この状況では移民ステータスや市民権の有無によって違いが出るため、事例を分けて紹介します：

非市民：

- 2025年6月 - コロンビア大学のパレスチナ連帯キャンプを報道したオーストラリアの独立系ジャーナリストが国外追放（英語）[29]。教訓：SNSや公開情報の管理は、フライトの前ではなく、ビザを申請する前に固めておくこと。
- 2025年3月 - トランプ政権に批判的だったことを理由にフランス人研究者が入国拒否（英語）[72]

市民：

- 2025年4月 - 黒人でムスリムのパレスチナ支持アクティビストが、米国への再入国時に拘束され、デバイスを没収される（英語）[73]

- 2025年4月 - パレスチナ支持の抗議者の弁護を担当していたことを理由に、公民権弁護士が拘束され、スマホを押収される（英語）[74]

関連ガイドでさらに学ぼう

サブのスマートフォン

活動やデモ・行動用に、もう一台スマホを用意しよう。

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。

リンク

1. activistchecklist.org/ja/contribute/
2. immigrantsrising.org/resource/guide-for-undocumented-individuals-traveling-in-the-u-s/
3. nilc.org/resources/community-alert-immigration-arrests-at-airports/
4. activistchecklist.org/ja/essentials/
5. instagram.com/reel/DbEcBcZxK-r/
6. fox5vegas.com/2026/07/16/police-ice-agents-walk-away-attempted-arrest-leaving-man-handcuffed-harry-reid-airport/
7. boston.com/news/local-news/2026/07/18/2-arrested-at-logan-airport-as-ice-activity-ramps-up/
8. stopaapihate.org/2025/05/19/know-your-rights-when-traveling/
9. theverge.com/policy/634264/customs-border-protection-search-phone-airport-rights
10. aclu.org/news/privacy-technology/can-border-agents-search-your-electronic
11. youtube.com/watch?v=nWEpW6KOZDs
12. activistchecklist.org/ja/updates/
13. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
14. strongphrase.net/passcode
15. arstechnica.com/tech-policy/2026/02/fbi-stymied-by-apples-lockdown-mode-after-seizing-journalists-iphone/
16. visahq.com/news/2025-12-30/us/us-makes-biometric-facial-scans-mandatory-for-all-foreign-arrivals-and-departures/
17. us.norton.com/blog/emerging-threats/biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data
18. instagram.com/ykreborn/reel/DD4-diFydz5/
19. keepbeyond.com/optout/
20. support.google.com/accounts/answer/3118687?sjid=15768665358815288280-NC
21. support.apple.com/guide/iphone/lock-or-hide-or-an-app-iph00f208d05/ios
22. support.google.com/android/answer/15341885?hl=en
23. support.apple.com/en-us/104987
24. signal.org
25. signal.org/blog/introducing-secure-backups/
26. activistchecklist.org/ja/secondary/
27. support.1password.com/travel-mode/
28. support.1password.com/secret-key/?mac
29. newyorker.com/news/the-lede/how-my-reporting-on-the-columbia-protests-led-to-my-deportation
30. theguardian.com/us-news/2025/jun/18/social-media-student-visa-screening
31. blockpartyapp.com
32. lifewire.com/make-your-twitter-profile-private-3486093
33. help.x.com/en/managing-your-account/how-to-deactivate-x-account
34. linkedin.com/help/linkedin/answer/a518980/
35. linkedin.com/help/linkedin/answer/a1340802/temporarily-disable-account
36. help.instagram.com/448523408565555
37. help.instagram.com/728869160569983
38. guidingtech.com/hide-all-posts-on-facebook/
39. facebook.com/help/214376678584711
40. support.tiktok.com/en/account-and-privacy/account-privacy-settings/making-your-account-public-or-private
41. support.tiktok.com/en/account-and-privacy/deleting-an-account/deactivate-your-account
42. cyd.social
43. ivpn.net
44. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
45. activistchecklist.org/ja/vpn/
46. activistchecklist.org/research
47. ivpn.net/en/
48. protonvpn.com
49. activistchecklist.org/ja/proton/
50. ivpn.net/en/pricing/
51. digitalgoods.proxysto.re/en
52. ivpn.net/en/apps-macos/
53. ivpn.net/en/apps-windows
54. ivpn.net/en/apps-ios
55. ivpn.net/en/apps-android
56. techradar.com/vpn/vpn-privacy-security/i-dont-like-that-he-made-this-donation-mullvad-ceo-reacts-to-co-founders-donation-to-controversial-swedish-populist-party
57. sls.eff.org/technologies/forensic-extraction-tools
58. support.apple.com/guide/iphone/back-up-iphone-iph3ecf67d29/ios
59. androidauthority.com/backup-android-phone-708622/
60. support.apple.com/en-us/102664
61. support.microsoft.com/en-us/windows/reset-your-pc-0ef73740-b927-549b-b7c9-e6f2b48d275e
62. strongphrase.net/more
63. aclu.org
64. nlg.org
65. theintercept.com/2026/01/30/washington-post-hannah-natanson-fbi-biometrics-unlock-phone/
66. ssd.eff.org/module/attending-protest
67. support.apple.com/guide/personal-safety/emergency-call-text-iphone-apple-watch-ips4f0cd709b/web
68. freedom.press/digisec/blog/border-security/
69. eff.org/wp/digital-privacy-us-border-2017
70. instagram.com/ykreborn/
71. ykhong.substack.com
72. theguardian.com/us-news/2025/mar/19/trump-musk-french-scientist-detained
73. mondoweiss.net/2025/04/my-experience-confirms-that-us-citizens-especially-black-and-muslim-ones-are-also-targets-musa-springer-on-his-unlawful-detention/
74. democracynow.org/2025/4/11/lawyer_detained_border