# 連邦職員のための デジタルセキュリティ

ACTIVIST CHECKLIST

最終更新日： **2025年2月24日**　所要時間の目安： **1時間**

**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/federal/

**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]。

このガイドは作成から**1年**以上経っています。内容の一部が古くなっている可能性があります。

トランプとDOGEによる政府乗っ取りに対抗して組織活動をする連邦職員のために。政府のデバイスやWi-Fiは監視されているものと考えましょう。抗議や異議に関わることは、所属機関の電話、ノートパソコン、メールには一切持ち込まないこと。運動に関する会話は、個人のデバイスでSignalを使いましょう。政府のデバイスで個人的なメールやチャットを書かないこと。そこで作成したもの（書いたメッセージや保存したファイル）はすべて、FOIA（情報公開法）で開示請求される可能性があります。 Signalの設定、LinkedIn、自宅のWi-Fiについて順を追って解説します。

**今、政府のデバイスを使っていませんか？** 政府の携帯電話やパソコンからこのページを見ている場合や、政府のWi-Fiに接続している場合は、このサイトを閉じて、あとでもう一度アクセスしてください。政府のシステムからは、あなたの通信を簡単に監視できます。

**このチェックリストの対象：** トランプ／マスク／DOGEによる政府の乗っ取りに抵抗しているすべての連邦職員。

以下のガイドでは、抵抗活動のデジタルな痕跡を最小限に抑え、報復から身を守るためのヒントを紹介します。完全な匿名性や安全を保証できるデジタルセキュリティはありません。それでも、以下のステップのひとつひとつが大切な防御の層になります。

**私たちが私たちを守る！** セキュリティとは、自分だけでなく**お互いを守る**ために取る行動のことです。このガイドを同僚に転送して、周りの人がデジタルセキュリティについて考えるきっかけを作りましょう。これであなたもアンバサダーです！

さらにおすすめなのは、セキュリティパーティーを開いて[2]、ランチタイムや仕事帰りに一緒にこのチェックリストに取り組むこと。リンクを転送するだけより、実際に実行してもらえる確率がずっと高くなります。

---

## 基本のセキュリティ対策

- [ ] **抵抗や批判の話は、政府支給のデバイス（スマホやノートPC）から離れた場所でだけする**
  政府のデバイスはすべて、キー入力やマイクの近くで話した言葉を監視していると考えておく

政府支給のデバイスはすべて自分を監視している、という前提で行動するのが妥当です。実際に監視が行われているとは限りませんが、あなたの活動の痕跡を簡単にたどられてしまう可能性があります。

❌ **抵抗や反対意見について話してはいけない場面...**

- **政府支給のスマホ**で入力しているとき
- **政府支給のパソコン**で入力しているとき
- **政府のWi-Fi**に接続しているとき。個人のスマホやパソコンを使っていても同じです
- **マイク**付きの政府のスマホやパソコンの近くにいるとき（自分に支給されたデバイスでなくても）
- **政府がホストするビデオ通話**に参加しているとき（相手が信頼できる人であっても）

### ✅ 代わりにやるべきこと

- 一緒に組織活動ができる、信頼できる同僚を見つけよう！
- まずは相手の反応を探ってみる。まだ信頼関係がないなら、時間をかけて築いていく。
- マイク付きの政府のデバイスから離れ、政府の建物の外で、直接会って話す。
- 信頼できる相手とのメッセージや通話には、暗号化されたSignalアプリを使う（次のチェックリスト項目を参照）

**例えば：** 反対意見や批判、不満、計画について話し合うときに、（個人のスマホで）Signalを使うのはとても良いことで、大切なことです。でも、政府支給のノートPCのすぐ隣でそれをやると、会話が監視される可能性があります。可能性は低いかもしれませんが、別の部屋に移動する価値はあります。

---

## ☐ 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[3]。 （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[4]。
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[5]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[6]

**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[7]。

**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%[8]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[9]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。

## ☐ Signalのプロフィールに本名や自分の写真を使わない

身元を暴こうとする警察や攻撃者から身を守るのに役立つ。メンバーの身元確認がされていないSignalグループに参加している場合は特に有効。

コミュニティでの組織活動の多くは、メンバーの身元確認がされていないSignalグループで行われています。そうしたグループでは、メンバー全員をどこまで信頼できるかはわからない。こうしたグループには、右翼の敵対者[10]や警察[11]が潜入していることもあります。

偽名を使えば、Google検索で自分の身元を突き止められるのを防げる。

自分の顔ではない写真を使えば、画像検索や顔認識でSNSアカウントを見つけられるのを防げる。

どちらもドクシング[12]やネット上の嫌がらせから身を守るのに役立ちます。

プロフィールの変更方法

1. **プロフィールの表示名を変更する：** 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 → 人のシルエットが表示された一番上の項目をクリック → プロフィールの表示名を編集
2. **プロフィール写真を変更する：** 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・関心・趣味・居場所に関係のない一般的な写真をアップロード。

**同じ原則は、ソーシャルメディアではさらに強く当てはまります。** Instagram、Facebook、LinkedInのプロフィールにフルネームの本名と顔がはっきり写った写真がそろっていると、プロフィールの他の部分を非公開にしていても、攻撃者は簡単に身元を特定できてしまう。詳しくはSNSのセキュリティを固めるを参照してください。

グループの仲間にも、同じ対策をするよう声をかけよう。セキュリティはチームスポーツなので。

## ☐ LinkedInなどのSNSプロフィールの公開範囲を狭めることを検討しよう

SNSの投稿内容をもとに標的にされないよう身を守る

DOGEがLinkedInなどのSNSプロフィールにある「DEI」への言及を手がかりにしているという報告が、複数寄せられています

SNSプロフィールを非公開にする方法

**LinkedIn：**

- **公開プロフィールの表示設定：** LinkedIn → **Edit Profile**[13] → **Edit Visibility** → 完全に無効にするか、プライバシーと履歴を守るために非表示にしたい項目を選ぶ。
- **プロフィールを完全に休止する：** 一定期間、すべての人（自分のネットワーク内の人も含む）に対してプロフィールを完全に休止[14]しても問題なければ、それが最も安全な選択肢です。将来また再開するために、リマインダーを設定しておくといいかもしれません。
- **その他の表示設定も厳しくする：** LinkedIn → **Profile Icon** → **Settings** → **Privacy** → **Visibility** → それぞれの設定を、より非公開寄りに調整する。
- **LinkedInのアクティビティフィード：** LinkedInですでにつながっている人は、引き続きあなたのフィードを見ることができます。標的にされるのを避けたいなら、過去の投稿を見直して削除する[15]ことも考えてみてください。

**X/Twitter：** こちらの手順[16]に従って、投稿を非公開にしましょう。

## ☐ 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**[17]**（いちばん簡単）か****Firefox**[18]**（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[19]をインストールしましょう。
- iPhone[20]やAndroid[21]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[22]）に**Braveをインストール**[22]します。
2. 起動したら手順に従って、Chromeや他のブラウザ[23]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[24]、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**[25]を使う

# 連邦政府の建物にいるとき

普段からオフィスで働いている場合も、たまに訪れるだけの場合も、これらのステップで防御の層を増やせます。

- [ ] **連邦政府の建物には、個人のスマホやノートPCを持ち込まない（できれば）**
  可能なら、スマホやノートPCを持ち込まないのがいちばん安全

いちばん安全なのは、スマホやノートPCを持っていかないことです。

とはいえ、誰かの緊急連絡先になっている（たとえば）場合など、個人のスマホを置いていくのがいつもできるとは限りません。

デバイスを持っていく場合は、次のチェックリスト項目の手順に従ってください。

- [ ] **個人のデバイスを持っていく場合は、次の手順でできるだけ安全に保とう**
  できるだけ電源を切っておく。政府のWi-Fiには接続しない。 Wi-Fiに接続する場合は、信頼できるVPN[26]を使う。

政府のネットワークやデバイスは、たとえ自分の個人デバイスを使っていても、私たちの行動をすべて監視できると考えておくべきです。

**おすすめ：**

1. できれば個人のデバイスは持っていかない
2. どうしても持っていく必要がある場合は、できるだけ電源を切っておく
3. どうしても電源を入れる必要がある場合は、政府のWi-Fi（または有線LAN）には接続しない
4. どうしてもWi-Fiに接続する必要がある場合は、必ず信頼できるVPNをオンにした状態で接続し、自分の通信を守ること。事前にVPNをインストール[27]しておこう。

---

# 政府のデバイスを自宅に持ち帰る場合

家に政府のデバイスがある場合でも、自宅で身を守るためにできることがあります

- [ ] **作業が終わったら（そして反対意見について話す前に）、スマホとノートパソコンの電源を切ってしまっておく**

DO: デバイスの電源を切り、引き出しやクローゼットにしまう

DO NOT: デバイスの電源を入れたまま、会話が聞こえる場所に置いておく

政府支給のスマホやノートパソコンが近くにあるなら、そのマイクには会話が聞かれている可能性があると考えておきましょう。

やり方

1. 一日の終わりや、自宅で反対意見について話すときは、**必ずデバイスの電源を切っておく**
2. **デバイスは必ず引き出しやクローゼット、またはドアを閉めた部屋にしまっておく**。こうしておけば、万が一マイクがオンのままになっていても、会話を聞かれずに済みます。（多くの人にとっては起こりにくいことかもしれませんが、ほんの一分でできる予防策です。）

- [ ] **自宅のWi-Fiネットワークを分ける：政府支給のデバイス用に「ゲストネットワーク」をオンにする**

DO: 政府支給のデバイスは、自宅ルーターの「ゲストネットワーク」にだけ接続する

DO NOT: 個人のデバイスを接続する

優先度は低めですが、やっておくと安心です。

自宅のWi-Fiルーターで「ゲストネットワーク」を有効にすれば、政府支給のデバイスからネットワーク上の個人のデバイスにアクセスできなくなります。

ゲストネットワークを有効にして使う方法

1. Wi-Fiルーター本体を見て、機種名か、せめてメーカー名を確認する
2. （Googleではなく）Brave Search[28]で `how to enable guest network on [機種名またはメーカー名]` と検索する
3. 見つけた手順に従って、メインのネットワークとは別の名前のWi-Fiネットワークを設定します。
4. 政府支給のスマホとノートパソコンで、メインのWi-Fiの「このネットワーク設定を削除」オプションを探します。そのあと、新しいゲストWi-Fiネットワークに接続し直します。

Wi-Fiルーターの設定は、ときどき難しいこともあります。困ったときは、身近なテクノロジーに詳しい人に手伝ってもらいましょう。

### ☐ 個人のデバイスにモバイルデバイス管理ツールをインストールしたことがあるなら、削除する

モバイルデバイス管理アプリは、政府（または企業）がデバイスを安全に保つためにリモートで管理できるようにするソフトウェアです。過去にこうしたアプリを**個人の**デバイスにインストールするよう求められたことがあるなら、削除が認められている場合は必ず削除しましょう。通常は、政府の仕事を辞めたあとがそのタイミングです。

よく使われるMDMアプリ：

- Microsoft Intune
- IBM MaaS360
- VMware Workspace ONE（旧AirWatch）
- MobileIron
- BlackBerry UEM
- Master Data Management by Civica

モバイルデバイス管理アプリを削除する方法

1. デバイスをバックアップする（iPhone[29]、Android[30]）
2. デバイスを工場出荷時の状態にリセットする（iPhone[31]、Android[32]）
3. バックアップから復元する（iPhone[33]、Android[30]）

## 組織活動をするとき

### ☐ 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**[34]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[35]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[36]しましょう。無料プランで大丈夫です
2. Proton Drive[37]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[38]や、エンドツーエンド暗号化オプションを有効にしたJotform[39]を試してみてください。

- [ ] **さらに安全を強化するには、「セキュリティの基本」チェックリストを活用しよう**
  「セキュリティの基本」チェックリストで、アカウントを安全に保ち、プライバシーを守る方法を確認できます

セキュリティの基本ガイド

「セキュリティの基本」チェックリスト[40]を参考に、自分のデバイスをできるかぎり安全な状態にしておきましょう。

# よくある質問

## 政府のデバイスで個人のメールを開くのは危険？

情報公開法に基づくFOIA請求[41]では、政府のリソースを使って作成された文書などが調べられます。これは捜索令状ではありません。政府のデバイスで作成したものはすべて（文書、メール、テキストメッセージなど）、FOIAの対象になり得ます。

**（情報源：元FOIA担当職員。これは法的助言ではありません。）**

## 個人のデバイスで政府のメールやチャットを開くのは危険？

私物のデバイスでも、Outlook、Teamsなどの政府のアプリで作成したものはFOIA（情報公開法）の対象になります。FOIA請求があっても、私物のデバイス内の個人データが片っ端から調べられるわけではありません。請求の内容はかなり具体的である必要があり、情報の検索は請求で指定されたキーワードを使って行われます。含めたくない内容がある場合は、政府のメッセージや文書の中の表現（名前など）を変えておきましょう。

**（情報源：元FOIA担当職員。これは法的助言ではありません。）**

### ほかに質問は？

ここで答えられていない質問があれば、お問い合わせ[42]ください。

---

## このチェックリストをほかの連邦職員とシェアしよう

デジタルセキュリティを実践する人が増えるほど、全員がより安全になります。同僚にも送ってみてください。**送るときは必ずSignalで**：

> デジタルセキュリティを守りたい連邦職員向けのチェックリストです。役に立ったのでシェアします。**デジタルセキュリティ・チェックリスト：**
> https://activistchecklist.org/federal[43] **主なポイント：**
>
> - 政府支給のスマホやパソコンで、自分の反対意見について話さない。
> - マイク付きの政府デバイスの近くで、自分の反対意見について話さない
> - 個人のデバイスで政府のWi-Fiに接続しないこと（どうしても接続しなければならない場合は、IVPN.netやProton VPNなどのVPNを使いましょう）
> - 政府デバイスで個人のメール・チャット・SMSにアクセスしない（FOIAの対象になってしまいます）
> - 反対意見について話すときは、私物のスマホのSignalアプリだけを使う（通常のSMSや電話、メールは使わない。政府デバイスも使わない）。信頼できる同僚を見つけて、Signalでつながろう。
>
> お互いの安全を、お互いで守ろう。

---

## コミュニティ組織化のアドバイス

**政治的な組織活動が初めての方、ようこそ！** 今この時代、一人ひとりがムーブメントの中で自分の居場所を見つけることが求められています。ありがたいことに、土台にできるリソースはたくさんあるので、一から作り直す必要はありません。

まずはここから：

- Organizing: People, Power, Change[44]（ハーバード・ケネディスクール、マーシャル・ガンツ著／無料の書籍、PDF、英語）
- The Citizens Handbook[45] ※英語
- Neighborhood Anarchist CollectiveのCommunity Organizing Basics[46]（英語。ページ下部にファシリテーション、集まりの開き方、セキュリティカルチャーなどへのリンクあり）
- Activist HandbookのTeam Building（チームづくり）[47]
- Beautiful TroubleのOrganizing 101（組織化の基本）[48]
- そして最後に、経験豊富なオーガナイザーにメンターになってもらいましょう。これまでに同じことをやってきた人は何千人もいて、喜んでサポートしてくれます！

**メディアとのやりとり：** 組織活動の一環として、自分たちの体験をメディアに伝える場合は、記者のSignalユーザー名（または電話番号）を聞いて、やりとりはSignalだけで行いましょう。情報がどこに送られるのかわからないフォームに、名前やメールアドレス、電話番号を入力するのは慎重に。

## さらに詳しく

- WIRED: DOGE Sparks Surveillance Fear Across the US Government（DOGEが米国政府全体に監視への恐怖を広げる）[49]（2025年）

### 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。

ロックダウンモードのメリットとデメリット 3分で読めます [50]　「警察が家に来たら」ポスター [51]

## リンク

1. activistchecklist.org/ja/contribute/
2. activistchecklist.org/ja/party/
3. blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/
4. signal.org
5. support.signal.org/hc/en-us/articles/6829998083994-Phone-Number-Privacy-and-Usernames-Deeper-Dive
6. activistchecklist.org/ja/signal/
7. penguinrandomhouse.ca/books/558051/on-tyranny-by-timothy-snyder/9780804190114/excerpt
8. atomicmail.io/blog/is-whatsapp-safe-the-truth-about-your-privacy
9. activistchecklist.org/ja/whatsapp/
10. nitter.net/camhigby/status/2015093531526729789
11. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
12. activistchecklist.org/ja/doxxing/
13. linkedin.com/public-profile/settings
14. linkedin.com/help/linkedin/answer/a1336653/
15. linkedin.com/help/linkedin/answer/a1342513
16. help.x.com/en/safety-and-security/how-to-make-x-private-and-public
17. brave.com
18. mozilla.org/en-US/firefox/
19. privacybadger.org
20. apps.apple.com/us/app/brave-private-web-browser-vpn/id1052879175
21. play.google.com/store/apps/details?id=com.brave.browser&hl=en
22. brave.com/download/
23. support.brave.com/hc/en-us/articles/360019782291-How-do-I-import-or-export-browsing-data
24. privacyguides.org/en/desktop-browsers/
25. activistchecklist.org/ja/research/
26. activistchecklist.org/vpn/
27. activistchecklist.org/ja/vpn/
28. search.brave.com
29. support.apple.com/en-us/108366
30. support.google.com/android/answer/2819582?hl=en
31. support.apple.com/en-us/108931
32. support.google.com/android/answer/6088915?hl=en
33. support.apple.com/en-us/118105
34. proton.me/drive/docs
35. activistchecklist.org/ja/proton/
36. proton.me
37. drive.proton.me
38. cryptpad.fr
39. jotform.com
40. activistchecklist.org/ja/essentials/
41. en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States)
42. activistchecklist.org/ja/contact/
43. activistchecklist.org/federal
44. actionnetwork.org/user_files/user_files/000/041/455/original/organizing_people_power_changeadaptedfromMarshallGanz.pdf
45. citizenshandbook.org/toc.html
46. neighborhoodanarchists.org/organizing-guide
47. activisthandbook.org/organising
48. beautifultrouble.org/toolbox/set/organizing-101
49. unwall.app/www.wired.com/story/surveillance-privacy-doge-federal-employees/
50. activistchecklist.org/ja/lockdown/
51. activistchecklist.org/ja/police/