ドクシング対策チェックリスト

最終更新日： **2026年5月22日**　所要時間の目安： **基本的な対策に45分**

ACTIVIST CHECKLIST

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**。

オンラインでの嫌がらせキャンペーンの多くは、公開されているデータから始まります。人物検索サイトに載っている住所、SNSの写真、Venmoの電話番号などです。人物検索サイトから自分の情報を消す、SNSのセキュリティを固める、新しいサービスの登録には別名を使う。こうした対策を早く始めるほど、攻撃者が使える材料は少なくなります。

ドクシングとは、嫌がらせをする人が、相手に嫌がらせをしたり脅したりする目的で、その人の個人を特定できる情報を集めて公開することです。ネット上での嫌がらせにつながることが多く、失職や法的な影響（ICEが集められたデータを使って人々を拘束した例もあります）、まれに対面での危害につながることもあります。

さらされる情報には、法的な氏名（本名）、自宅の住所、職場、電話番号、メールアドレス、写真、家族の情報などが含まれることがあります。

なぜ大切なのか： 敵対する人たちがドクシングやオンラインハラスメントを使うのは、**恐怖を植えつけて**、私たちに活動をやめさせたいから。前もって身を守る対策をとっておくほど、私たちはもっと力強く行動できます。ドクシングされてから対策しようとしても、情報はすでに出回っていて、もう自分ではコントロールできません。

ドクシングが嫌がらせや危害につながる仕組み

ドクシングから起こりうる嫌がらせの例： あなたの情報が拡散された後、次のような嫌がらせが起こる可能性があります。嫌がらせのメールやメッセージを送る、オンラインアカウントへの不正アクセスを試みる、あなたの住所に荷物を送りつける、ネット上であなたになりすます、評判を傷つけたりクビにさせたりするためにあなたの勤務先を標的にする、あなたの名義でクレジットカードを作ろうとする、あなたを逮捕させるためにICEや警察に情報を提供する、あるいはこうした攻撃を家族や友人に対して行う、などです。

ほとんどのドクシングはネット上にとどまります。 まれに対面にエスカレートしたケースとしては、器物損壊、攻撃者が自宅や職場に押しかけて嫌がらせをする、「ドクシングトラック」を雇って公の場であなたの信用を落とそうとする、スワッティング（あなたを標的にSWATチームを出動させる虚偽通報）、そして最も深刻なものとして、政府当局者が集められたデータを使って人々を拘束する、といったことがありました。あなたが著名人でない限り、こうしたことが起こる可能性は低いです。

攻撃者が使いうる手口：

- 検索エンジン（Googleなど）やSNSであなたの名前を検索する
- LinkedInであなたを調べたり、履歴書のコピーを見つけたりして、勤務先や学校、職歴を把握する
- あなたがネットに投稿した写真から、住んでいる場所やよく過ごす場所を推測するかもしれない
- 「人物検索」サイトであなたを調べて、名前や電話番号から住所を突き止めるかもしれない
- Venmoであなたの電話番号を検索して、誰にいつ支払っているかから、あなたがどこで過ごしているかを把握するかもしれない

- （ネットで手に入れたり、抗議行動で撮ったりした）あなたの写真で「画像の逆検索」をして、ネット上のあなたのプロフィールを見つけるかもしれない。

そして、こうした情報をさまざまな方法で公開することがあります。公開の「ドクシングサイト」（例：Canary Mission、ソーシャルメディア、あるいはTelegramやダークウェブのフォーラムのような半公開のチャンネルなどです。

自分自身とコミュニティを守るためにできること

守りたいもの： 目標は、あなたの個人を特定できる情報や機密性の高い情報を、はるかに集めにくくすることです。まずは最も重要なもの、つまり自宅の住所と勤務先から始めます。

一緒にやる。 公の場で活動している多くのグループは、このチェックリストをセキュリティパーティーで進めて、全員が同時にセキュリティを固められるようにしています。

私たちがこの活動をしているのは、社会の仕組みや文化を変えることに本気で取り組んでいるから。こういうガイドを読むと、「全部隠して、二度と外に出ないようにしなきゃ」と思ってしまいがち。でも、そういう恐怖こそ、敵対する人たちが私たちを脅して狙っているものです。そうではなく、これらの防御策を、**大胆な行動を続けていく**ための力にしてほしいと思います。

活動がうまくいけばいくほど、いずれ何らかのドクシングやオンラインハラスメントに直面する可能性は高くなります。それは、あなたが正しい方向に進んでいるサインだと考えよう。

今まさにドクシングやオンラインハラスメントを受けていますか？ その場合は、下のドクシングへの対応セクションへ進んでください。

基本的な対策

すべての人　敵対する人たちの注目を集めそうなアクティビズムやアドボカシーに関わっているなら、このセクションはあなたのためのものです。

- [ ] **名前や電話番号だけで、自宅の住所がGoogleでどれだけ簡単に見つかるか確かめよう**

公開プロフィールを守ることがどれだけ大切か実感するには、自分で自分を検索してみるのが一番です。

このガイドの後半では、手作業で詳しくGoogle検索をしてもらいます。でも今は、**自分のどんな個人情報が簡単に手に入ってしまうのかを知ることだけが目的です。**

GOOGLEで自分の個人情報を最初に検索する方法：探してみるのは

例の部分を自分の実際の情報に置き換えて、次のようにGoogleで検索してみましょう：

- `"555-867-5309"`（自分の電話番号）
- `"Jamie Garcia" 住所`（自分の名前＋「住所」）
- `"Jamie Garcia" 電話番号`（自分の名前＋「電話番号」）
- `"Jamie Garcia" "Springfield High School"`（自分の名前＋出身高校や大学）
- `"Jamie Garcia" 勤務先`（自分の名前＋「勤務先」、または実際の職場の名前でも試してみよう）

引用符 "" を使うと便利ですが、必須ではありません。何も見つからなければ、引用符なしで試してみましょう。

課題：**自分の自宅住所を見つけるのに、どれくらい時間がかかる？**

おそらく、それほどかからないはず。このガイドの残りの部分では、こうした情報の多くを削除する方法を紹介します。

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。

☐ 重要 **自動では対応されない「人物検索」サイトから手動でオプトアウトする**

最も効果的な「人物検索サイト」削除ツールでも、カバーできるのはサイト全体の70%ほどです。

プロフィールの削除をとても難しくしているサイトもあり、EasyOptOutsのようなサービスでは代わりに対応できません。こうしたサイトでは通常、プロフィールを削除しようとしているのが本人であることを確認するため、メールを受け取る必要があります。

リスクの高い人物検索サイトから自分の情報を手動で削除する方法

まずは、特にリスクの高いサイトから手動でオプトアウトしましょう：

1. **People Connect (Intelius)からオプトアウトする** - 多くの人物検索サイトを所有しているので、一度のオプトアウトで大きな効果があります。非表示申請フォーム「suppression form」に記入します。メールアドレスや電話番号の確認を求められます。
   - もし自分がアクセスできない電話番号やメールアドレスの確認を求められたら、テクニカルサポート (877) 564-3253 に電話して、「personal information suppressed」と伝え、個人情報の非表示を依頼してください。私たちの経験では、メールより電話のほうがずっと効果的です。
2. **National Public Dataで自分を検索する。** 結果が見つかったら、ページの一番下までスクロールして「Do Not Sell My Info」をクリックし、オプトアウトします。

Googleで自分の情報を手動で検索しないと見つからないサイトもあります（後のチェックリスト項目で説明します）。

すべて手動で： オプトアウトをすべて手動で行いたい場合は、Yael GrauerのBig Ass Data Broker Opt-Out Listが使えます。 EasyOptOutsのようなサービスはこれらの大半に対応してくれますが、すべてではありません。このリストを使えば、無料で手動で手続きを進めることも、各データベースを手動で検索して漏れがないか確認することもできます。

「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。

Googleの「Results About You」通知をオンにする

自分の個人情報が載っているページについて、通知を受け取れるようになります。

Googleは、あなたのプライベートな情報がネット上で公開されたときに知らせてくれるツールとして、Results About Youを提供しています。日本語版では「自分に関する検索結果」という名前です。検索結果を削除するうえではあまり役に立ちませんが、情報を削除してもらうために自分で動く必要があるタイミングを知るのには役立ちます。

GOOGLEの「RESULTS ABOUT YOU」をオンにする方法

1. **Googleの「Results About You」をオンにする**：フルネーム（とほかに使っている名前）、住所、電話番号、メールアドレスを入力します。

   > **注意：** 活動専用に使っていて、本当の身元から完全に切り離されている**偽名**や**使い捨ての電話番号**は、絶対に入力しないでください。それらがGoogleのシステム内で紐づけられてしまうのは避けたいところです。

2. 最初のスキャンが終わるまで**待つ**（数時間かかります）
3. **結果を確認して、削除してもらう方法を探す：**
   1. Googleのツール内にある「削除をリクエスト」ボタンを使っても、たいていは役に立ちません。理由は二つ。1）「人物検索」サイトや意図的なドクシングによるものでない限り、Googleはほとんどのリクエストを却下します。 2）Googleが削除したとしても、元の情報はネット上に残ったままです。ほかの検索エンジンや元のサイトから、直接見つけられてしまいます。
   2. それよりも、サイトの管理者に連絡して情報を削除してもらいましょう。ウェブサイトの場合は、問い合わせフォームやメールアドレスを探して、削除してほしい情報が載っているページを伝えます。 SNSの場合は、自分の投稿を削除したり、投稿者に削除を頼んだりすることになるかもしれません。
   3. 一つ対応するごとに「確認済みにする」をクリックします。
4. **Googleに「削除リクエスト」を送る：** この削除リクエストフォームを使って、個人情報やその他のドクシングにあたる内容が載った検索結果の削除をGoogleに依頼できます。これはGoogleの「Results About Me」機能とは別のものです。
5. 新しい結果が見つかったときに届く**通知メールをチェックする**。たいていは、登録してから最初の数週間にいちばん多く届きます。

プライバシー： Googleアカウントが必要です。ここにはトレードオフがあります。ほかの名前、電話番号、住所といった追加の識別情報をGoogleに渡すことになり、Googleはそれをあなたのアカウントに紐づけて保管することになります。それでも、たいていはその価値があります。Googleはすでにこうした情報のほとんどを持っていますし、住所などのプライベートな情報がネット上の新しい場所に出てきたときに通知してもらえるというメリットがあるからです。

SNSアカウントのプライバシー設定を強化する

プライバシーを守りたいと思うようになる前は、多くの人がSNSで自分の情報をかなりたくさん公開していました。

SNSのプロフィールをしっかり守れる状態にするには、時間がかかることもあります。

守りたい情報の例： 位置情報、メールアドレス（非表示にしていても、あなたを検索するのに使われることがある）、友達リスト、勤務先、生年月日のすべて（銀行など他のアカウントへのアクセスに悪用されることがある）、そしてよく過ごす場所がわかる写真や投稿。

堂々と公開するか、非公開にするか： アクティビズムや組織活動に使っているため、フォロワーのいる公開プロフィールをあえて維持している人もいます。たとえば、プロフィールを誰でも見られる状態にしておく人もいれば、友達だけが見られるように非公開にする人もいます。

方法1：BLOCK PARTYでSNSのプライバシー設定を強化する

手動でも設定できますが（下記参照）、どのプライバシー設定を変更すべきかを案内してくれるBlock Partyの利用をおすすめします。 Facebook、LinkedIn、Instagram、X/Twitter、TikTok、Snapchat、Reddit、Strava、Venmo、Google、Googleマップのクチコミ、YouTube、Blueskyの設定強化をサポートしてくれます。無料プランでも十分役に立ちます。私たちはプライバシーポリシーを確認していて、開発者も概ね信頼できると考えています。

1. ブラウザに**Block Partyの拡張機能をインストール**します（無料）。（まだなら、これを機にBraveをインストールするのもおすすめです！）画面の指示に従ってインストールします。
2. **「Start Scan」を押して**、使っているSNSを選びます。すべての設定をチェックするまで、数分ほどそのまま待ちます。
3. **各サイトの横にある「To Do」をクリックして**、おすすめの変更内容を確認します。手動で変更を始めることもできますし、その多くをBlock Partyに自動で任せることもできます。
4. **多くの変更は自動化できる：** 設定変更の50〜70%はBlock Partyが自動でやってくれます。自動化には7日間の無料トライアルか有料アカウントが必要です（プロモコードJOINTHEPARTYを使うと年額50ドル。私たちに紹介料は一切入りません）。
5. **残りは手動で変更する：** 自動でできない項目は、各サイトの「To Do」リストに従って変更します。
6. 最後に、Block Partyでカバーされていない可能性のある、自分が使っている他のSNSも確認しましょう。Cash App、Venmo（まだカバーされていなければ）、Partiful、Nextdoor、AllTrails、Strava、Pinterest、Goodreads、MapMyRun、マッチングアプリなどです。

X/Twitterの過去の投稿を削除したい、またはBlueskyに移行したい場合は、Cydをチェックしてみてください。

方法2：SNSのプライバシー設定を手動で強化する

Block Partyを使いたくない場合は、メインで使っている各SNSアカウントで次の手順を行ってください。

優先したいサイト（おおよそリスクの高い順）：

- Facebook
- LinkedIn
- Venmo
- Cash App
- Google マップのクチコミ
- Yelp
- Strava
- All Trails
- Instagram
- X/Twitter **（過去の投稿を削除するなら、Cydをチェックしてみてください。）**
- Bluesky
- YouTube
- TikTok
- Snapchat
- Reddit
- Partiful
- Nextdoor

各サイトでの手順：

1. もう必要ないなら、**このプロフィールの削除を検討しましょう**。多くのサイト（Facebook、Instagram、Googleなど）では、写真やメッセージを失わないよう、先にデータのコピーをダウンロードできます。削除したら、それで完了です。削除しない場合は、次に進みましょう。
    - **Facebook Marketplaceだけ使いたい場合は？** Marketplace用に別のダミーのFacebookアカウントを作り、メインのアカウントは削除することを検討しましょう。
2. **プライバシー設定の画面を開き**、すべての設定をできるだけ非公開寄りに変更しましょう。
3. **住んでいる市町村を削除する**
4. **友達リストを非公開にする**
5. **フォロワーやつながりを整理する。** 共通の友達が一人か二人もいない人は削除しましょう。実際に知らない人ならなおさらです。「非公開」のプロフィールでも、フォロワーとして承認した人なら誰でも投稿を見たり、スクリーンショットを撮ったりできます。
6. 住んでいる場所、よく過ごす場所、一緒に過ごす相手について詳しくわかってしまう**過去の投稿や写真を削除しましょう**。

よく使うユーザー名でDigital Footprint Checkを試してみるのもおすすめです。忘れていたプロフィールがどこに残っているか確認できます。

警察や右翼の敵対者と遭遇する場面ではマスクを着用する

悪意のある人物があなたの顔から身元を突き止めようとしたとき、身を守る助けになります

警察やICE（移民・関税執行局）は、反対意見を持つ人々に対して顔認識技術を使っています。

右翼の敵対者は、抗議参加者を撮影して逆画像検索にかけ、参加者を特定することがよくあります。中にはCanary Missionのように、アクティビストのプロフィールをまとめたデータベースを運営しているところもあります。顔の一部、または全体を隠すことで、特定されにくくなります。

KN95マスクは、顔認識ツールを避けるのに役立ちます。完璧ではありません（目だけで識別できるツールもあります）が、大きな効果があります。

他の特徴にも注意が必要です。 顔を覆っても、体の他の部分が見分けやすければ十分とは言えません。敵対者は、目立つタトゥー、髪の色や髪型、体型、肌の色、服装などから、マスクをした抗議参加者を特定することがよくあります。特に、これらの特徴が複数組み合わさると特定されやすくなります。複数のアクションをまたいで追跡されにくくしたいなら、長袖で見えるタトゥーを隠す、帽子やフードをかぶる、抗議に着ていく服を毎回変える、といった対策を検討してみてください。

> このリストの他の項目と同じく、プライバシーと可視性は両立しにくいことがあります。顔や目を覆ってリスクを最小限にしたい人もいれば、信頼を築き、感情をより直接的に伝えるために顔をすべて見せたい人もいます。

法律上の注意：一部の都市では、マスクの着用を違法とする反マスク法が制定されています。地元の市の条例を確認しておくとよいでしょう。

「デジタルセキュリティの基本」チェックリストを完了しよう

このガイドでは、パスワード、アプリの位置情報の許可、ソフトウェアのアップデートなど、ドクシング対策として大切なその他のステップを紹介しています。

ドクシングが心配なら、「デジタルセキュリティの基本」チェックリスト →にあるステップを済ませておくのがおすすめです。

ドクシングの標的になった場合、その多くが、あなたのアカウントやデバイスに誰かがアクセスしようとするのを防いでくれます。

「基本」チェックリストの中でも、特に大切なのは次の項目です：

- ほとんどのアプリで**位置情報の追跡をオフにする**
- パソコン、スマホ、アプリに**最新のソフトウェアアップデートをインストールする**
- **パスワードマネージャー**を使う
- 弱いパスワードや複数のサイトで使い回しているパスワードがあれば、**今使っているパスワードを変更する。**
- 重要なアカウントで**二要素認証**を有効にする
- **怪しいリンク**はクリックしない

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、右翼の敵対者や警察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。

強化された対策

中程度の脅威　政治的な抵抗活動に関わる中で、人目につく立場にいる人向けのセクションです。

☐ 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。

☐ メインの電話番号を公開する代わりに、別の電話番号を用意しよう

電話番号があれば、「人物検索」サイトを使ってあなたの自宅住所をすぐに突き止められてしまうことがあります。

DO: Google Voice（無料、プライバシー保護は弱め）やMySudo（月2ドル、プライバシー保護は強め）を使う

DO NOT: ネット上や、参加者の身元が確認されていない大人数の場で電話番号を公開する

メインの電話番号を公開すると、嫌がらせの電話やメッセージを受けるリスクがあるだけではありません。「人物検索」サイトのどこかにあなたの情報がまだ残っていれば、その電話番号から自宅住所を突き止められてしまうおそれもあります。

別の電話番号を用意する方法

- 電話番号を公開する必要があるときは、**別の電話番号を用意しましょう**。
  - Google Voiceは無料ですが、警察がsubpoenaと呼ばれる情報開示命令を出すときに真っ先に向かうのがGoogleなので、プライバシー面では最も弱い選択肢です。
  - MySudoは月2ドルで、テキストメッセージ100通と通話30分が使えます。
  - メッセージや通話を無制限に使いたいなら、Sideline（月15ドル）やLine2（月10ドル）
- **Signalで連絡してもらいたいときは、電話番号ではなくSignalのユーザー名を伝えましょう。**（もちろん、できるだけSignalを使いましょう。組織活動をするときは特にです。また、設定で消えるメッセージをデフォルトでオンにしておきましょう。）

一緒に住んでいる人にも「人物検索」サイトから個人情報を削除してもらう

住所を知られないようにするには、同じ家に住む全員が自分の情報を守る必要があります。

私たちの大きな目標のひとつは、悪意のある人たちからあなたの自宅住所を守ることです。

本気で狙ってくる相手なら、SNSの投稿や友達リスト、家系図サイトなどから、あなたが誰と住んでいるかを突き止められるかもしれません。あなたが人物検索サイトから自分の情報を削除しても、同居人や家族がまだなら、相手はそこからあなたの自宅住所を見つけられてしまう可能性があります。

名字が同じ家族は特に強いつながりになります。攻撃する側は、その中の誰か一人から「人物検索」サイトをたどって、共通の住所に直接たどり着けてしまうからです。

同居している人の個人情報削除をサポートする方法

1. 一緒に住んでいる**一人ひとりにお願いして**、「人物検索」サイトから個人情報を削除してもらいましょう。伝え方の例：

   > 私たちがもっと安全に暮らせるように、うちの住所や自分の個人情報をネット上から消す作業をしているところ。ネットでうちの住所が簡単に見つからないように、数分だけ時間をとって、このチェックリストの最初の二つの項目をやってもらえないかな：https://activistchecklist.org/doxxing> 今週時間があれば、一緒に座ってやるのも大歓迎。

2. 必要なら、Googleで自宅の住所を検索して、その人の名前が住所と結びついている具体的なページを見つけてみるのも手です。なぜ大切なのかを伝えるために、このページのリンクを送ってもいいでしょう。こうした情報がネット上でどれほど簡単に見つかるかを知ると、たいていの人は驚きます。
3. 一週間ほどしたら様子を聞いて、サポートが必要か確認できるよう**リマインダーを設定しておきましょう**。

今の住所に以前住んでいた人にも、同じお願いをしてみるといいかもしれません。その人たちの旧住所として、今もこの住所が「人物検索」サイトに載っているからです。

- [ ] **自分の個人情報を手動でGoogle検索する**
  手動で見つけて削除しなければならない検索結果は、どうしても出てきます。

EasyOptOutsのような自動データ削除ツールだけに頼っていると、個人情報が載った検索結果がまだたくさん残っている可能性が高いです。

いちばん優先したいのは今の自宅住所の削除。その次が電話番号です。メールアドレスが公開されていて嫌がらせにつながることもありますが、こちらは比較的対処しやすいです。

Kanaryアプリ（無料プラン）を使えば、こうした検索作業の一部を手伝ってもらえます。

GOOGLE上で自分の個人情報を見つけて削除する方法

1. **自分の情報ごとに別々にGoogle検索する。** 検索ワードを引用符で囲むと、より正確な結果が得られます。それぞれの検索で、Googleの最初の2〜3ページに目を通しましょう（この作業ではBrave Searchなどのプライバシー重視の検索エンジンは使わないでください）。
   - **自宅住所を引用符で囲む：** `"742 Evergreen Terrace, Springfield"`、あるいは単に`"742 Evergreen Tr"`でもOK。ただしこの場合、別の街の結果が大量に出てくるかもしれません。
   - **電話番号を引用符で囲む：** `"555-867-5309"`、`"5558675309"`、`"(555) 867-5309"`
   - **フルネームと市町村名（それぞれ別の引用符で囲む）：** `"Jamie Garcia" "Springfield"`
   - **フルネームだけを引用符で囲む：** `"Jamie Garcia"`（自分とは関係ない結果もたくさん出てきます）
2. 見つけたもののうち、センシティブな個人情報が含まれているものは**リストにまとめておく**。住所や電話番号が載っているサイトを優先しましょう。
3. **それぞれを削除してもらうための計画を立てる。**
   - 「人物検索」サイトの場合は、個人情報の販売停止を求める「do not sell my info」や、オプトアウト用の「opt out」といったフォームを探して記入しましょう。
   - SNSの場合は、投稿した本人に削除してもらう必要があります。削除に応じてもらえない場合は、「コンテンツを報告」を押してみるのも手です。
   - それ以外のサイトの場合は、問い合わせフォームを探して、オンライン攻撃の標的になるのが心配だからと伝えて削除を依頼しましょう。ほとんどのサイトは対応してくれます。
   - **検索エンジンに検索結果の削除を依頼する。** 嫌がらせやドクシング、その他の有害なコンテンツについては、Google（フォーム）やBing（フォーム）に直接削除リクエストを送ることができます。成功するかどうかはケースによりますが、特に有害な検索結果については試してみる価値があります。
4. **確認し直すためのリマインダーを設定する。** 一週間後にチェックしましょう。どこからも返事がなければ、もう一度連絡してみましょう。
5. 上記の検索それぞれについて**Googleアラート**を**設定して**、新しい結果が出たら通知が届くようにしましょう。（Googleの「あなたに関する検索結果」も便利ですが、見落としは確実にあります。）
6. **Googleの検索結果を更新する。** 元のサイトで掲載を削除できたのに、Googleの検索結果にまだ表示される場合は、コンテンツの更新をリクエストできます。
7. **ほかの検索エンジンも試す。** 検索エンジンによって表示される結果は異なりますし、攻撃してくる相手が使うのはGoogleだけとは限りません。 BingやDuckDuckGoでも同じ検索をして、ほかに何が出てくるか確認しましょう。

☐ 信用情報をフリーズする

誰かがあなたの名義で勝手にクレジットカードを作るのを防ぎます。

悪意のある人物があなたの名義でクレジットカードを作ろうとするかもしれません。そうなると、クレジットスコアが下がり、長期的にお金の面で苦労することになりかねません。

信用情報をフリーズすれば、誰もあなたの名義でカードやローンを作れなくなります。必要なときには、一時的にフリーズを解除できます。

信用情報をフリーズする方法

三社すべての信用情報機関で、自分で「フリーズ」を設定する必要があります：

- **Equifax**
- **Experian**
- **TransUnion**

これは常に無料です。有料サービスを勧められても、申し込まないでください。

将来、新しい口座やカードを作るために信用情報の照会が必要になったときは、一時的にフリーズを解除するのを忘れないようにしましょう。

- [ ] **Google マップと Apple マップで自宅にぼかしをかける**
  悪意のある人に、家や庭の配置を知られにくくなります。

悪意のある人があなたの住所を手に入れた場合、直接押しかけて嫌がらせや危害を加えようとして、Google マップで家を探そうとするかもしれません。あるいは、自宅の駐車スペースにどんな車が停まっているかといった情報まで知られてしまうこともあります。

地図サイトで自宅にぼかしをかける方法

注意： 一度ぼかしをリクエストすると、元に戻すことはできません。とはいえ、ほとんどの人にとって、ストリートビューに自宅が映っていることのメリットはほぼありません。

Google マップで自宅にぼかしをかける（詳細）：

1. Google マップで自宅を探します。
2. ぼかしをかけたいストリートビューの画像を開きます。
3. 右下の「問題の報告」をクリックし、プライバシー上の理由で自宅にぼかしをかけてほしいことをフォームに記入して送信します。

Apple マップで自宅にぼかしをかける：

1. mapsimagecollection@apple.com にメールを送ります。自宅の住所を書き、プライバシー上の理由でぼかしをかけてほしいと伝えましょう。

- [ ] **不動産サイト（Zillow、Redfinなど）から自宅の情報を削除する**
  自宅の室内写真を非公開にすることで、周りの人も含めて安全を守りやすくなります。

Zillow、Redfin、Realtor.comなどのサイトでは、家の外観（これだけでもある程度のリスクがあります）だけでなく、室内の詳しい間取りまで見られてしまうことがよくあります。こうした情報は、敵対する人たちによる嫌がらせや危害に使われるおそれがあります。

自分の住所の画像を削除するようリクエストすれば、このリスクから身を守れます。

不動産サイトから自宅の画像を削除する方法

持ち家でない場合は、各サイトでアカウントが必要になるため、大家さんに削除を依頼する必要があるかもしれません。大家さんが各不動産サイトで物件を「claim」して、所有者として登録する必要があります。

まずサイトで検索して、写真がどれくらい詳細か、削除したいかどうかを確認するのもおすすめです。

1. Zillowから削除する
2. Redfinから削除する
3. **Realtor.com**: Log in → **Claim Home** → **Edit Photos**
4. 不動産エージェントに頼んで、不動産業者間の物件情報データベースであるMLSから写真を削除してもらえば、ほかのサイトからも消えます。

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**、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。

SignalのPINと登録ロックを有効にする

誰かがあなたの電話番号を「乗っ取って」Signalに登録する、高度な攻撃から身を守ります

強い動機を持った攻撃者があなたの電話番号を突き止めた場合、「SIMスワップ」と呼ばれる手口や、あなたの通信会社に電話して電話番号を新しい会社へ移す「ポート」の手続きを始めることで、番号の乗っ取りを試みる可能性があります。そうなると、相手はあなたの電話番号を使ってSignalアカウントを登録し、あなた宛てのメッセージを受け取れるようになってしまいます。

これは高度な攻撃で、ほとんどの人には起こりません。それでも、Signalアカウントを守るのは簡単です。

Signalで**登録ロック**を有効にすれば、身を守ることができます。たとえ電話番号を盗まれても、アカウントを乗っ取られるのを防げます。あなたのアカウントが7日間使われない状態にならない限り、誰もあなたの番号で新しいSignalアカウントを登録できなくなります。

PINを忘れてしまった場合、新しいアカウントを作成できるまで7日間待つ必要があります（連絡先も復元されません）。 PINと登録ロックについて詳しくはこちら。

SIGNALのPINと登録ロックを有効にする方法

登録ロックを有効にする： Signalを開く → プロフィール写真をタップ → **設定** → **アカウント** → **登録ロック**を有効にする

PINを強化する： Signalのセットアップ時に、PINを設定しているはずです。 PINを覚えていない場合や、もっと強力なPINを使いたい場合は、次の手順で変更できます：

1. **強力なPINを生成する：** セキュリティを最大限に高めるには、8桁か10桁のPINを使い、必ずコンピューターで生成したものにしましょう。こちらのランダムPIN生成ツールが使えます。
2. **SignalのPINを設定する：** Signalを開く → プロフィール写真をタップ → **設定** → **アカウント** → **PINを作成／変更**（自分のPINがわからない場合）。
3. **PINを保存するか、PINのリマインダーを有効にする：** 普段からしっかり使っているパスワードマネージャーがあれば、そこにPINを保存しましょう。 PINをどこに保存したか忘れてしまいそうなら、「PINのリマインダー」を有効にしたままにしておきましょう。

注目度の高い人のための対策

高い脅威 抵抗活動に関連して大きくメディアに取り上げられる可能性がある人や、相手側が豊富なリソースを持っている人向けのセクションです。

- [ ] **高度なデータ削除サービスにお金をかける（例：Optery Ultimate）**

政治的な立場を理由に攻撃されるリスクが非常に高い場合は、ネット上の自分のデータを徹底的に消しておきましょう。

まずは、自動データ削除ツールを EasyOptOuts から Optery Ultimate（年額250ドル）のようなものにアップグレードしましょう。自動オプトアウトツールの中でも、特にカバー範囲が広いツールのひとつです。さらにカバー範囲を広げたいなら、Kanary Pro プラン（月額10ドル）も検討してみてください。

リスクのレベルによっては、データの消去を代わりに徹底的にやってくれる高品質なサービスにお金をかけることも考えてみましょう。

アクティビストに寄り添ったデータ消去・ドクシング対応サービス：

- Brightlines
- Convocation Research & Design

Access Now Helpline を利用する手もあります。たいていは無料ですが、対応はずっと遅く、徹底度も劣ります。

☐ ソーシャルメディアを徹底的に整理して、すべてロックダウンする

上で紹介したソーシャルメディアの基本的なロックダウン手順は、最初の一歩として有効標的にされるリスクが高いなら、もっと細かく整理しておこう。

ソーシャルメディアを細かく整理してロックダウンする方法

1. プロフィールを載せている、あるいは以前に載せていたすべてのサイトのリストを作成。何年も使っていなかったものも含めて。大手プラットフォーム以外についても思い出してみてください。デートアプリ、フィットネスアプリ、レビューサイト、決済アプリ、古いフォーラムサイトなどとにかく全部。
2. Digital Footprint Checker と Instant Username で共通で使っているユーザー名を検索して、忘れてしまったプロファイルを見つける。それらをリストに追加。
3. リストをたどり、各サイトで以下の手順を実行:
   - もう使わないプロフィールを削除する
   - 表示名を変更
   - ユーザー名を変更
   - プロフィール写真を削除する
   - 自己紹介欄から居住地を削除する
   - 居場所がわかってしまいそうな投稿や写真を非表示にする
   - 友達リストを非公開にする
   - メールアドレスを変更(DuckDuckGo Email Protection または Gmail で「プラス記号を足す方法」を検討)。
   - プライバシー設定を変更する。
4. 終わるまでに何時間もかかるかも。次のところから再開できるように、チェックを終えたサイトを記録しておいてください。

ヒント: ランダムな表示名、ユーザー名、プロフィール画像が必要な場合は、このIDジェネレータが使えます。

☐ 私書箱（PO box）を用意して、自宅の住所を教えなくて済むようにする

DO: 私書箱（PO box）や、iPostal1のような郵便物の転送・スキャンサービスを利用する

DO NOT: 自宅の住所をそのまま人に教え続ける

サービスに登録するときや荷物を受け取るときなどに、本当の住所を伝えるのはやめたほうがいいかもしれません。

選択肢：

- **USPS（米国郵便公社）の私書箱**：最大のデメリットは、FedExやUPSが私書箱には配達してくれないこと。
- **UPSメールボックス**：料金は高めですが、USPSやFedExからの郵便物も受け取れて、プライバシーもしっかり守れます。
- **iPostal1**：郵便物のスキャンと実物の受け取りの両方に対応。私書箱には配達してくれないこともある配送業者（FedExやUPSなど）を含め、すべての配送サービスからの荷物を受け取れます。ただし、サービスがハッキングされたり、あなたに関するデータの提出を求める裁判所命令が出されたりした場合には、プライバシー上のリスクがあります。

注意： UPSメールボックスや、iPostal1のような「バーチャルメールボックス」サービスを利用する場合、政府発行の身分証明書を提示し、USPSに提出される書類（USPS Form 1583）に署名する必要があります。

☐ オンラインアカウントごとに別々のアイデンティティを使う（名前、メールアドレス、ユーザー名、電話番号）

本名やメールアドレス、電話番号などで登録する代わりに、**アカウントごとにランダムで別々のアイデンティティ**を使ってみましょう。

こうすることで、攻撃者（そしてテック企業）がサイトをまたいであなたのアカウントを結びつけ、断片的な情報からプロフィールを作り上げることが難しくなります。

アカウントごとに別々のアイデンティティを使う方法

できる限り、以下の項目をサイトごとに別々のものにしましょう：

- **表示名：** このランダムなアイデンティティ生成ツールを使う。
- **ユーザー名：** このアイデンティティ生成ツールか、ユーザー名専用のユーザー名生成ツールを使う。
- **プロフィール写真：** 空欄のままにするか、このアイデンティティ生成ツールを使う。すべてのサイトで同じ写真を使っていると、攻撃者が「画像の逆検索」をして、あなたのアカウントをすべて見つけ出せてしまいます。
- **メールアドレス** - 次のようなメールエイリアスサービスを使う：
  - @duck.com のメールエイリアスが使える Qwacky（無料、Chrome/Firefox 拡張機能）
  - Proton Mail（無料/有料）
  - Addy.io（無料/有料）
- **電話番号：** 入力を求められても、できるだけ電話番号は入力しないようにしましょう。登録時の認証のためだけに電話番号が必要な場合は、SMSPoolで電話番号をレンタルしてみてください（登録ごとに0.50ドル）。長期的に使える電話番号が必要なら、MySudoを検討してみてください。

☐ 周りの人（家族、友人、同僚、仲間、ご近所さん）が自分の個人情報を守れるようにサポートしよう

あなた自身が狙われるリスクが高い場合は、あなたへの嫌がらせや危害の一環として、身近な人たちも標的にされる可能性がどれくらいあるかを考えておきましょう。これは、アクティビストが大きなニュースになったときによく起こることです。右翼のトロールや自警団気取りの人たちは、家族、同居人、友人、同僚、仲間、ご近所さんまで狙っ

てきます。

身近な人たちにメッセージを送って、少なくともこのガイドの最初のセクションだけでも取り組んでもらうよう提案しましょう。

今見ているチェックリストのリンクはこちら：https://activistchecklist.org/doxxing

こうした話をするのは、時に難しいこともあります（特に家族の場合は）。あなたの活動のせいでその人にもリスクがあることを説明するには、時間がかかるかもしれません。

また、嫌がらせを受けるリスクがあることを、雇用主（それに受付や人事担当など、連絡の窓口になる同僚）に前もって伝えておくのもいいかもしれません。そうすれば、あなたについての不審な電話やメール、気がかりな連絡が来たときにも、状況を理解してもらえます。

☐ 自宅で脅威にさらされたときに備えて、個人の緊急時プランを立てる

ドクシングによる攻撃のなかで最も深刻なのは、誰かがあなたの自宅や日常生活の場に直接やってきて、嫌がらせや脅迫をしたり、危害を加えようとしたりすることです。

こちらの 個人の緊急時プランニング・チェックリスト → を活用しましょう

ドクシングのリスクに関しては、そのチェックリストのなかでも特に次のセクションが役に立ちます：

- セクション3：自宅の安全
- セクション4：避難計画

☐ 銀行と携帯電話のアカウントにセキュリティPINを設定する

銀行口座や携帯電話会社のアカウントは狙われやすい重要なターゲット。保護を強化しておきたいところです。こうした会社の中には、電話番号、住所、生年月日だけで本人確認をするところもあります。これらはすべて、誰かがネット上であなたについて調べられる情報です。

PINなどのセキュリティ対策を追加すれば、アクセスできるのはあなただけ、という状態を保ちやすくなります。

重要なアカウントにPINを設定する方法

保護しておきたいアカウントの例はこちら。

1. 銀行、クレジットカード、ローン、住宅ローン、投資のアカウント
2. 携帯電話会社（Verizon、T-Mobile、AT&Tなど）
3. インターネットプロバイダー
4. 電気・ガス・水道などの公共料金の会社
5. 保険（健康保険、住宅保険、自動車保険など）

各アカウントにPINを設定する方法：

1. カスタマーサービスに電話する。
2. 本人確認用のPINを設定できるか聞く。
3. アカウントごとにランダムなPINを作る。
4. それをパスワードマネージャーに保存する。
5. PINを設定できない場合は、誰かがあなたになりすましてアカウントにアクセスするのを防ぐために、ほかにどんなセキュリティ機能があるか聞いてみましょう。

ツールまとめ

このガイドではたくさんのツールを紹介しているので、ここに一覧でまとめました：

- Googleの「あなたに関する検索結果」機能：あなたの個人情報がGoogleの新しい検索結果に表示されたときに通知してくれます。
- EasyOptOuts（年間20ドル）：あらゆる「人物検索」サイトからあなたの情報を削除してくれます。
- Block Party：主要なSNSごとに、変更すべき設定を具体的に案内してくれます。
- Cyd：X/Twitterの投稿を削除・バックアップできます（希望すればBlueskyに移すことも可能）。
- StrongPhrase.netのアイデンティティ生成ツール：サイトごとに使うランダムな名前やユーザー名などを作れます。
- MySudoまたはGoogle Voice：サブの電話番号を取得して、本当の番号を教えずに済むようにできます。
- @duck.comメールを使うためのQwacky、Proton Mail、またはAddy.io：メールエイリアスサービスを使えば、サイトごとに別々のメールアドレスを作れるので、サイト間で同一人物だと結び付けられにくくなります。
- SMSPool：電話番号が必要なサービスに登録するとき、確認用SMSを受け取るためにランダムな電話番号を数分間レンタルできます。
- Optery（年間250ドル）：脅威レベルが高い人向け。 EasyOptOutsと同じことをしてくれますが、さらに一歩踏み込んで対応してくれます。 （DeleteMeがよく勧められますが、Opteryのほうが効果的です。）

注意：ツールでできることには限界があり、手作業でやらなければならないステップもあります。

ドクシングやネット上のハラスメントへの対応

ドクシング対応の完全なガイドはまだありませんが、まず取りかかれることをいくつか紹介します。

ドクシングへの対応：

1. **身の安全を最優先に：** 差し迫った危害や嫌がらせを受けるおそれがあると感じたら、友人の家や安全な場所に避難しましょう。自分の直感を信じて。周りのサポートに頼って結局何も起きなかったほうが、その逆よりずっといいのです。
2. **心のケアも大切に：** 「軽い」とされるハラスメントでも、脅しが現実になるかどうかわからないので、大きなストレスになることがあります。自分を大切にしましょう。
3. **サポートを得る：** 一人で抱え込まないでください。どのステップでも、誰かにそばにいてもらいましょう。
   - こまめに様子を気にかけてくれて、気持ちを落ち着かせてくれる友人や仲間を見つけましょう。
   - 専門家のサポートを求めましょう：Access Now 24/7ヘルプライン（無料）、Equality Labs、Brightlines（高価格帯）、Convocation Research & Design（高価格帯）。
4. **すべてを記録する：** 削除したり、誰かをブロックしたりしないでください。後で攻撃の背後にいる人物を突き止めるのに役立つことがあります。必要なら、信頼できる協力者にこの作業を任せましょう。記録の方法。
5. **警察を呼ばない：** 警察は捜査を口実に、アクティビストのネットワークについて情報を集めるかもしれません。とはいえ、状況によっては地域の嫌がらせ防止法が助けになることもあります。国家機関に連絡したり、警察を関わらせたりする前に、運動に理解のある弁護士に相談することを検討しましょう。相談先として考えられる、運動に理解のある弁護士団体：CLDC（緊急対応ホットライン：541-603-6891）またはNLG。

対応方法についてさらに詳しく：

- Brightlines - ドクシング対策リソース
- Right To Be - ドクシング対応ガイド
- Right To Be - セルフケアガイド
- PEN America - ドクシングされたり、監視リストに載せられたりした場合の対処法
- PEN America - オンラインハラスメント・フィールドマニュアル - ドクシングへの対応
- Crimethinc - ドクシングと政治的嫌がらせの標的になった人のための予防とアフターケア（2020年）

関連ガイドでさらに学ぼう

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。

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。

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。

スパイウェア対策
スパイウェアや監視ソフトウェアから身を守ろう。

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　「警察が家に来たら」ポスター