Signalセキュリティチェックリスト

ACTIVIST CHECKLIST

最終更新日： **2026年4月3日** 所要時間の目安： **15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/signal/

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]。

Signalは現在主流なメッセージアプリの中では最も安全。ただしそれはきちんと設定した場合の話。このチェックリストでは、抗議行動でスマホが押収されたり、グループに潜入者が入り込んだりしたときに、メッセージと組織のネットワークを守るための設定変更を紹介。オーガナイザーや、米国でICEの監視行動に頻繁に参加する人向けの、より踏み込んだ設定も含めて。

このガイドでは、Signal[2]でのプライベートな会話を自分でしっかり管理する方法を紹介します。 Signalはもともと送信内容すべてを暗号化していますが、ここで紹介する追加の対策をしておけば、スマホをなくしたり、取り上げられたり、乗っ取られたりしても、チャットのプライバシーを守れます。メッセージ、通知、自分の身元を守るための簡単な方法を学びましょう。

Signalを使うのは初めて？ まずはこちらのSignal初心者向けガイド[3]をチェックしてみてください。

ヒント： Signalの設定は、友だちと集まってやる[4]のがおすすめ。ほとんどの項目は、腰を据えてやれば5〜10分で終わります。

Signalで自分の身元を隠す

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。

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[5]や警察[6]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[7]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。

ユーザー名を設定して電話番号を非表示にする

Signalで匿名でいられる選択肢を持っておきたいなら、電話番号を守ることが身元を守ることにつながります。

ユーザー名[8]が導入された2024年3月より前にSignalをインストールした場合、電話番号がまだ他の人に表示される設定になっているかもしれません。

ユーザー名を設定して電話番号を非表示にする方法

1. まず、プロフィールの表示名を変更しておきましょう（上の項目を参照）。 Signalのプロフィールの表示名がフルネームのままだと、電話番号を隠してもあまり意味がありません。
2. **ユーザー名を変更したい場合：** Signalを開く → プロフィール画像をタップ → **設定** → 上部にある自分の名前／アイコンをタップ → @ マークをタップ → **ユーザー名を編集** → 自分の身元とも、これまでどこかで使ったことのあるユーザー名とも**まったく関係のない**ユーザー名に設定する。ユーザー名の最後は2桁以上の数字にする必要があります。
3. **電話番号を非表示にする：** Signalを開く → プロフィール画像をタップ → **設定** → **プライバシー** → **電話番号** → **Who Can See My Number**（電話番号を見られる相手）で → **Nobody**（誰にも）を選択。
    1. 必要に応じて、「Who Can Find Me By Number」（電話番号で自分を見つけられる相手）の設定も変更できます。ただしそうすると、既存の連絡先の人たちは、あなたから先にメッセージを送らない限り、あなたがすでにSignalを使っていることに気づけなくなります。 「Nobody」（誰にも）に変更するのは、非常に高いレベルのプライバシーが必要な場合だけにしましょう。
4. **電話番号の代わりにユーザー名を伝える：** 政治的な目的で新しい人とつながるときは、ユーザー名を伝えましょう。 Signalを開く → プロフィール画像をタップ → **設定** → 上部にある自分の名前／アイコンをタップ → **QRコードまたはリンク** → 連絡を取りたい相手にQRコードかリンクのどちらかを共有する。もっと簡単に、ユーザー名を口頭で伝えるだけでも大丈夫です。

リンクプレビューをオフにする

おおよその位置情報が漏洩するのを防げる

これで特定の攻撃から身を守れます。ただし、送られてきたURLは必ずよく確認して、安心して開けるサイトかどうかを見極めてください。

リンクプレビューをオフにする方法

Signalを開く → プロフィール写真をタップ → **設定** → **チャット** → **リンクプレビューを生成する** をオフにする

技術的な背景： 2025年に、攻撃者が位置を約250マイルの範囲内で推測できる攻撃手法が公開されました[9]。

「Always Relay Calls」をオンにする

Signalの通話は、デフォルトではあなたと相手の間で直接つながります。つまり、相手のデバイスからあなたのIPアドレスが見えるということです。インターネットプロバイダーに裁判所命令が出されれば、IPアドレスからあなた個人が特定されてしまいます。

「常に通話を中継する」をオンにすると、通話がSignalのサーバーを経由するようになり、相手にあなたのIPアドレスが見えなくなります。（すでにVPN[10]を使っているなら、IPアドレスはもう隠されています。）

「常に通話を中継する」をオンにする方法

Signalを開く → プロフィール画像をタップ → **設定** → **プライバシー** → **詳細設定** → **常に通話を中継する**をオンにする

メッセージと通話を守る

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。

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[11]が***デフォルトで***有効になっているか確認することです。私たちが話を聞くアクティビストの多くは、これをデフォルトで有効にしていません。（しかも、新しいスレッドごとに手動で有効にするのは、ほとんどの人が忘れてしまいがち。）

これはあなた自身の安全も、ほかの人の安全も守ります。誰のスマホが警察に押収されるかはわかりません。たとえ完全に合法的なことを話しているつもりでも、政府は私たちの言葉をねじ曲げて、異議を唱えた私たちを罪に問おうとする手を見つけてくることがあります

消えるメッセージについて、気をつけておきたいことが二つあります：

1. **まず、デフォルト設定を変更して**、自分が作るスレッドすべてでこの機能が有効になるようにしましょう。
2. **次に、ほかの人が始めたスレッドでも有効になっているか確認しましょう：**ほかの人がスレッドを始めた場合、消えるメッセージが有効になっていないことがあります。その場合は自分で有効にする必要があるかもしれません。

消えるメッセージを有効にする方法

1. **デフォルトを変更するには：** Signalを開く → プロフィール写真をタップ → **設定** → **プライバシー** → **消えるメッセージ** → 希望の時間に設定（リスクの許容度に応じて長めにも短めにも）。
2. **（Androidのみ）メッセージの保存期間の上限を変更する：**消えるメッセージがオンになっていないスレッドでも、メッセージが削除されるようになります。（削除されるのは自分の端末上のメッセージだけです。） Signalを開く → プロフィール写真をタップ → **設定** → **データとストレージ** → **ストレージを管理** → **メッセージを保持** → 希望する最大期間に設定。前の画面に戻り、**リンク済み端末にも制限を適用**をオンにします。
3. **既存のスレッドを変更するには：** Signal → 変更したいメッセージスレッドを開く → 画面上部の相手の名前（またはグループ名）をクリック → **消えるメッセージ** → 希望の時間に設定。
4. **古いメッセージ／スレッドを削除する：**消えるメッセージは、過去のメッセージにはさかのぼって適用されません。なので、スマホに残っている古いスレッドは削除しておくといいかもしれません。ただ残念ながら、相手のスマホからは削除されません。なので、とても機密性の高い内容なら、相手にもスレッドを手動で削除してもらうよう頼む必要があるかもしれません。（ついでに、消えるメッセージをデフォルトでオンにするよう勧めてみましょう！）

消えるメッセージの時間を選ぶ：消えるまでの時間をどのくらいに設定するかは、メッセージの機密性によって変わります。自分にこう問いかけてみるといいかもしれません。「もし誰かの端末が押収されたりハッキングされたりしたら、これらのメッセージが見られないことはどのくらい重要？」

- 友だちとリスクの低い話をするなら、4週間でもいいかもしれません。
- 一般的な政治的な組織活動なら、1週間がいいかもしれません。
- リスクの高いアクションでは、1日、1時間、あるいは5分に設定して、アクションが始まる前にメッセージが消えるようにするのもいいでしょう。

注意：メッセージが消えるのは、メッセージが既読になった後です。たとえば、受信者が2週間メッセージを読まず、消えるメッセージを4週間に設定していた場合、実際にメッセージが消えるのは送信から6週間後になります。

Signalの通知でメッセージのプレビューと送信者名を非表示にする

スマホが押収されると、警察に通知履歴を見られてしまう可能性があります。

スマホが押収された場合、警察が通知履歴にアクセスする方法は二つあります：

1. スマホのロックを解除しなくても、ホーム画面に表示された通知を見ることができます。
2. ハッキングツールを使えば、スマホが受信した通知のログにアクセスできます。 （Prairieland事件での実例[12]）

これは受信したメッセージだけが対象です。そして、（消えるメッセージを有効にしている場合）Signalからメッセージが消えた後でも、このリスクは残ります。

SIGNALの通知をオフにする方法

IPHONEの場合

Signalを開く → プロフィール画像をタップ → 設定 → 通知 → 通知内容 → **「No Name or Content」を選択**

ANDROIDの場合

Signalを開く → プロフィール画像をタップして設定を開く → 通知 → 表示 → **「No name or message」を選択**

スマホのOS側でSignalの通知をオフにすると、Signalの着信も通知されなくなります。

Signal Desktopを使っている場合は、そちらでも通知をオフにしておきましょう。

参考： iOSにすでに保存されている通知ログを消去したい場合、唯一の方法はスマホを工場出荷状態にリセットし、新しいデバイスとして設定し直すことです。バックアップには通知履歴も含まれているので、バックアップからは復元しないでください。

「画面ロック」と「アプリスイッチャーで画面を隠す」をオンにする

スマホを誰かに渡したとき、画面ロックがセキュリティをもう一段階強化してくれます。

- **画面ロック（Screen Lock）：** ロック解除した状態のスマホを誰かに渡しても、Signal を開く前に顔認証・指紋認証・PIN でのロック解除がもう一度必要になります。
- **アプリスイッチャーで画面を隠す（Hide in App Switcher）：** アプリを切り替えるときに、メッセージが見えないように隠してくれます。

アプリスイッチャーで画面を隠す方法

IPHONE

Signal を開く → プロフィール写真をタップ → **設定** → **プライバシー** → **画面ロック**（Screen Lock）をオンにしてから、**アプリスイッチャーで画面を隠す**（Hide Screen in App Switcher）をオンにする

ANDROID

Signal を開く → プロフィール写真をタップして **設定** を開く → **プライバシー** → **画面ロック**（Screen lock）をオンにしてから、**画面セキュリティ**（Screen Security）をオンにする

「Show Calls in Recents」をオフにする（iPhoneのみ）

これで、スマホを没収されても警察にSignalの通話履歴を見られずに済みます。

"SHOW CALLS IN RECENTS"をオフにする方法

この設定はiPhoneにしかありません： Signalを開く → プロフィール写真をタップ → **設定** → **プライバシー** → **通話** → **Show Calls in Recents**をオフにする

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[13]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。

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[14]。

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[15]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[16]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。

☐ Signal用にプライベートなキーボードを有効にする（Androidのみ）

Androidでは、標準のキーボードが入力内容を記録している場合があります。

ANDROIDでプライベートなキーボードを使えているか確認する方法

注：これはAndroidスマホ専用です。 iPhoneのキーボードは、カスタムキーボードをインストールしていない限り、もともとプライベートです。

オプション1（簡単）- シークレットキーボードを有効にする
Signalを開く → プロフィール画像をタップ → **設定** → **プライバシー** → **アプリのセキュリティ** → **シークレットキーボード**を有効にする

オプション2（よりプライベート）- システム全体で標準キーボードを置き換える

- 上のオプションは、キーボードの提供元（Google）にキー入力を記録しないよう「お願い」しているだけです。それが守られている保証はありません。より安全なのは、カスタムキーボードをインストールすることです。
- FlorisBoard[17]はおすすめの選択肢のひとつです。先に、よりプライバシーに配慮したアプリストアであるF-Droid[18]をインストールする必要があります。

☐ AIによる通知の要約をオフにする

GoogleもAppleも、自社のAIツールがいつ私たちのプライベートな情報（Signalのメッセージなど）をデバイスから自社のサービスに送信しているのか、はっきりさせていません。もし情報が企業のサーバーに送られていれば、政府の裁判所命令によってアクセスされるおそれがあります。

私たちの理解では、これらのAI機能は**今のところ**通知を要約するだけです。でも今の流れを見ると、今後もっと踏み込んだことをしようとするかもしれません。

記事「Apple IntelligenceはSignalのメッセージを読んでいる？[19]」もチェックしてください

オプションA：SIGNALだけ、AIによる通知の要約をオフにする方法

オプションA：Signalだけ、AIによる通知の要約をオフにする

IPHONE

設定アプリを開く → **通知** → **通知を要約** → **Signal**をオフにする

ANDROID

設定 → **通知** → **Notification summaries** → **Manage apps**（**Don't include these apps**の下） → **Signal**をオフにする

AIによる通知の要約を完全にオフにする方法

オプションB：AIによる通知の要約を完全にオフにする

IPHONE

設定アプリを開く → **Apple Intelligence**と**Siri** → **Apple Intelligence**をオフにする

ANDROID

設定を開く → **通知** → **Use notification summaries**（または**Notification summaries**）をオフにする

MAC

> **システム設定** → **Apple Intelligence**と**Siri** → **Apple Intelligence**をオフにする → **確認**

（Macの場合、M1以降のプロセッサを搭載したAppleのコンピュータが必要です。）

- [ ] **Signal PINや認証コードを聞き出そうとする「Signal Support」からの偽メッセージに注意**
  認証コードやPINを他人に教えないよう気をつけて、アカウントを守ろう

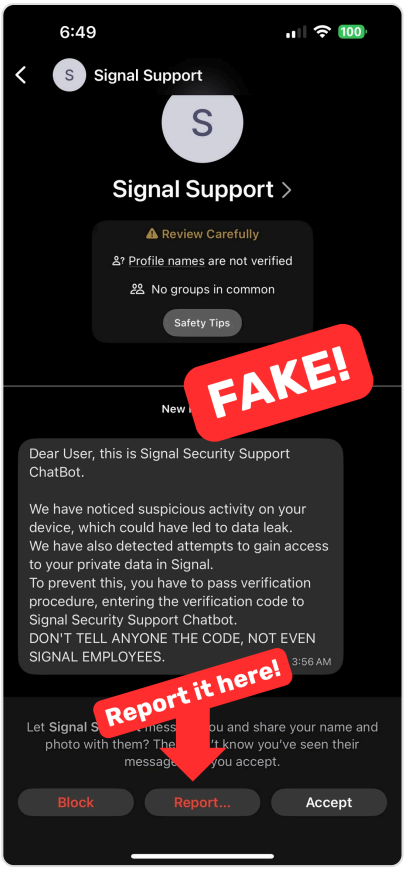
アカウントの乗っ取りを狙う「Signal Support」からの偽メッセージ[20]が増えています。

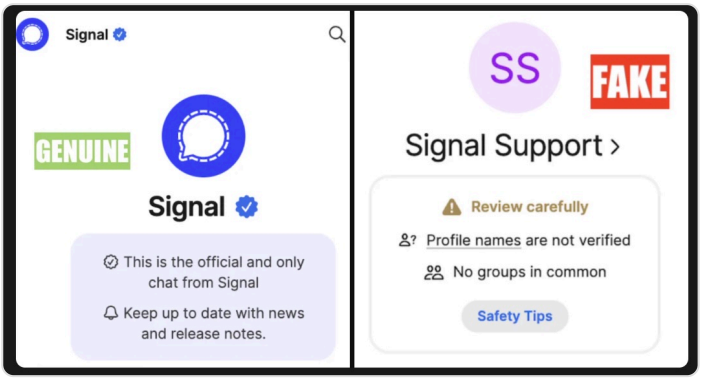
以下の例を参考に、Signalの偽メッセージに気をつけてください。

覚えておいてほしいこと：SignalがPINや認証コードを送るよう求めてくることは絶対にありません。 これらを入力するのは、デバイスに初めてアプリをインストールするときだけです。

Signalの詐欺・フィッシング[21]について詳しくはこちら。

詐欺メッセージの例をいくつか紹介します：





スマホの安全対策

Signalの安全性は、スマホの安全性で決まります。端末が押収されたりハッキングされたりした場合、警察はフォレンジックツールを使って弱いパスコードを突破し、端末から直接メッセージを抜き取ることができます。ここで紹介するステップで、デバイスレベルでSignalのメッセージを守れます。

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[15]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[15]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[15]のリンクを参照してください。

☐ 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[22]
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[22]
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[22]
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[22]
3. **Microsoft Store アプリ：** 自動更新[23]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。

顔認証・指紋認証によるロック解除（生体認証）をオフにする

生体認証よりもパスコードのほうが、法的に強い立場[24]をとれます。警察は、生体認証でロックを解除するよう強要してくることがあります。

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

（ほか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：顔認証や指紋認証があれば、毎回入力しなくても済むので、より強力なパスワードを使えます。どちらかを選ばなければならないなら、顔認証・指紋認証をオフにするよりも、長いパスコードにするほうが大切です。生体認証をオンのままにするなら、リスクの高い状況に向かうときにすぐオフにする方法を知っておきましょう（下のコツを参照）。

一時的に生体認証を無効にするいちばん確実な方法は、スマホの電源を完全に切ること。 そうするとデータも暗号化されます。次のロック解除ではパスコードが必要になります。

iPhoneのロックのコツ： 顔認証・指紋認証をオンのままにしている場合でも、**サイドボタンを5回押す**と、次のロック解除でパスコードの入力を必須にできます。

iPhoneのカメラのコツ： ロック画面で**左にスワイプ**すれば、ロックを解除せずに写真を撮れます。（撮影中に逮捕された場合に備えて。）

Androidのカメラのコツ： 多くのAndroidスマホでは、**サイドボタン／電源ボタンを二度押す**と、ロックを解除せずにカメラを起動できます。

より強力な保護

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。

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**[25]、Androidでは**高度な保護機能プログラム**[26]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[27]。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。

大切な連絡先と安全番号を確認する

あなたと相手の間で、誰かがひそかにメッセージを傍受していないかを確認できます

Signal はメッセージを暗号化するので、読めるのはあなたと相手だけです。ただし理論上は、高度な技術を持つ攻撃者があなたと相手の間に入り込み、メッセージを傍受してから相手に渡すことも可能です。これは「中間者攻撃（man-in-the-middle攻撃）」と呼ばれています。**安全番号**を使えば、暗号化された通信が誰にも割り込まれず、相手に直接つながっていることを確認できます。

ほとんどの人には、この作業は必要ありません。 友だちと日々の組織活動についてやりとりするだけなら、Signal の暗号化でもう十分に守られています。でも、リスクの高いこと（直接行動、デリケートな法的問題、ジャーナリストと情報源とのやりとりなど）について連絡を取り合うなら、ひと手間かけて安全番号を確認する価値があります。

封筒に押された封蝋をイメージしてみてください。暗号化は封蝋のようなものですが、高度な技術を持つ攻撃者なら、それを破って中身を読み、自分の蝋で封をし直すこともできてしまいます。安全番号の確認は、封蝋がすり替えられていないかを確かめる方法です。

安全番号を確認する方法

1. 確認したい相手との**会話を開く** → 上部の**相手の名前をタップ** → **安全番号を表示**。
2. **相手と番号を照らし合わせる：**
   - **直接会って（いちばんおすすめ）：**「コードをスキャン」をタップして、相手の QR コードを読み取ります。一致していれば、確認できたことを示すメッセージが表示されます。
   - **直接会えない場合：**本人と話していると確信できる通話やビデオ通話で、お互いに番号を読み上げます。 Signal そのものを使って確認するのはやめましょう。
3. **検証済みにする：**番号が一致したら、チェックマークをタップします。

相手の安全番号が変わらない限り（たとえば新しいスマホに替えた場合など）、確認は連絡先ごとに一度だけで大丈夫です。番号が変わったときは、Signal が知らせてくれます。デリケートな内容を送る前に、もう一度確認しましょう。

Signalがハッキングされた？安全なの？セキュアなの？

数か月ごとに、「Signalは安全じゃない」「ハッキングされた」と主張する投稿が出回ります。

Signalはハッキングされた？ ほぼ確実にされてません[28]**。**

非営利団体による運営、暗号化、オープンソース、資金に関する噂、デバイスのリスクなど、Signalのセキュリティについてもっと詳しく知りたい人は、こちらの記事をどうぞ：Signalは安全？[29]

Signalを使うことにリスクはありますが、それはたいてい技術そのものではなく、安全な使い方ができているかどうかに関わっています。

たとえば、プライベートなSignalグループであってもだれかに潜入されてしまえば、メッセージをすべてスクリーンショットされてネットで公開されることもありえます。

警察にスマホを押収されてしまい、パスコードが弱いロックを突破されるおそれもあります。ただし、それはSignalの欠陥ではありません。誰であれ、スマホを物理的に手にしてロックを解除できれば、メッセージはすべて見られてしまう。だからこそ、強力なパスコードを設定すること[16]と、デバイスのOSを常に最新の状態にすること[16]をおすすめしています。

その他のリソース

- Signalは安全？[29] — Signalの仕組み、共有されうるデータ、セキュリティをめぐるよくある誤解について。
- アクティビズムでSignalグループを使う方法[30]についての、とても役立つガイドはこちら。
- Signalをしっかり守る設定：Locking down Signal[31] — Freedom of the Press Foundation

よくある質問

Signalって本当に安全？
安全です。 Signalは、現在使える主流のメッセージアプリの中で最もセキュアです。メッセージと通話はエンドツーエンド暗号化されていて、コードはオープンソース。さらにSignalは、メッセージの内容を保存しない非営利団体によって運営されています。最大のリスクは、たいてい技術そのものではなくSignalの使い方にあります。たとえば、スマホのパスコードが弱い、グループに潜入者がいる、誰かがスクリーンショットを撮っている、など。

警察はSignalのメッセージを読める？
場合による。シグナルのサーバーからデータを取得することはできません。メッセージはエンドツーエンド暗号化されているので、警察の召喚令状があっても運営会社が提供できるのは基本的なアカウント情報、つまりいつ登録したか、アプリを最後に使用した日時などだけです。ただし、警察がスマホを押収すれば、顔・指紋認証を強制してロック解除したり、弱いパスコードの場合はフォレンジックツールを使って突破することがありえます。もし突破されれば、スマホに残っているすべてのメッセージが読まれてしまう。メッセージをやりとりしている人にも同じことが言える。だから強力なパスコードを設定し、 顔・指紋認証のロック解除をオフにし、消えるメッセージを全員に対してオンにするのをおすすめします。

SignalはWhatsAppより安全？

運動で使うのであれば、そのとおりです。 WhatsAppはSignalが開発したものと同じ暗号化プロトコルを使っていますが、Metaが所有していて、誰がいつ誰とやり取りしたかという詳細なメタデータを収集し、Facebookと共有しています。警察からの要請に対して、MetaはSignalよりもはるかに多くのデータを引き渡しています。

安全番号の確認は必要？

組織活動で特に近い仲間や、センシティブな計画について話し合う相手とは確認しておきましょう。一度検証すれば、そのコンタクトが本人であることを確認したとSignalに記録されます。検証していないと、電話回線ネットワークを支配できるハイレベルな攻撃者が、理論上は鍵をすり替えることができてしまいます。検証しておけば、そうしたことが起きたときに警告が表示されます。

Signalで本当の電話番号を使うべき？

電話番号の代わりにユーザーネームを使えば、よりプライバシーを守れます。 Signalでは現在、ユーザーネームを設定して、すでに自分の番号を連絡先に登録している人以外には番号を非表示にできます。さらに安全距離を確保したいアクティビストは、MySudoやGoogle Voice、プリペイドSIMなどのサブの番号でSignalを登録することも可能。

登録用PINは何のため？

PINがあれば、スマホをなくしたときや新しい端末でSignalを設定するときに、Signalのプロフィール、連絡先、参加しているグループを復元できます。また、誰かにSIMを盗まれても、その人が自分のスマホでなりすましてSignalを登録するのを防げます。長いPINを設定し、パスワードマネージャーに保存しておこう

関連ガイドでさらに学ぼう

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。

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。

旅行・飛行機移動のセキュリティ

移動・旅行するアクティビストのためのデジタルセキュリティ対策。

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。

- アクティビストのためのVPN 16分で読めます 10
- セキュリティアップデート確認ツール 22
- Protonを安全に使う方法 17分で読めます 32
- リンクのトラッキングを削除する 3分で読めます 33
- Apple IntelligenceはSignalのメッセージを読んでいる？ 6分で読めます 19

リンク

1. activistchecklist.org/ja/contribute/
2. signal.org/ja/
3. ssd.eff.org/module/how-to-use-signal
4. activistchecklist.org/ja/party/
5. nitter.net/camhigby/status/2015093531526729789
6. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
7. activistchecklist.org/ja/doxxing/
8. signal.org/blog/phone-number-privacy-usernames/
9. gist.github.com/hackermondev/45a3cdfa52246f1d1201c1e8cdef6117
10. activistchecklist.org/ja/vpn/
11. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
12. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
13. activistchecklist.org/ja/secondary/
14. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
15. strongphrase.net/passcode
16. activistchecklist.org/ja/essentials/
17. florisboard.org
18. f-droid.org/en/
19. activistchecklist.org/ja/signal-ai/
20. netzpolitik.org/2026/phishing-attack-numerous-journalists-targeted-in-attack-via-signal-messenger/
21. support.signal.org/hc/en-us/articles/9932566320410-Staying-Safe-from-Phishing-Scams-and-Impersonation
22. activistchecklist.org/ja/updates/

23. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
24. ssd.eff.org/module/attending-protest
25. support.apple.com/en-us/105120
26. landing.google.com/intl/en_us/advancedprotection/
27. activistchecklist.org/ja/lockdown/
28. hassignalbeenhacked.info
29. activistchecklist.org/ja/signal-secure/
30. micahflee.com/using-signal-groups-for-activism/
31. freedom.press/digisec/blog/locking-down-signal/
32. activistchecklist.org/ja/proton/
33. activistchecklist.org/ja/links/