



Facebookアカウント乗っ取り 復旧ガイド

被害者のための完全マニュアル

落ち着いて、この手順に沿って進めてください

目次



この文書について



まず知っておいてほしいこと：何が起きているのか

乗っ取りの仕組み / なぜSMSが届かなくなるのか



復旧の全体像

4つのステップの概要



ステップ1：WhatsAppの電話番号を取り戻す

認証コードを自分が受け取れるようにする



ステップ2：Facebookアカウントの復旧

facebook.com/hacked からの復旧手順



ステップ3：復旧後のセキュリティを固める

パスワード変更・2段階認証・ログイン端末の確認



追加チェック：犯人の「裏口」を全部ふさぐ

アカウントセンター・連絡先・連携アプリ・Gmail等



ステップ4：被害の拡大を止める

友達への周知・他サービスのパスワード変更



復旧がうまくいかない時のQ&A



今後このような被害に遭わないために

3つのルール・怪しいメッセージの見分け方

この文書について

Facebookメッセージ経由でアカウントを乗っ取られた方が、落ち着いて、最短で復旧するための手順書です。実際の被害対応の記録をもとに作成しています。

まず知っておいてほしいこと：何が起きているのか

あなたのアカウントで、こういうことが起きています。

友達のアカウントが乗っ取られる



友達のふりをしてメッセージで接触「**インフルエンサープログラムに参加しませんか**」



認証コードを聞き出す → **電話番号**を聞き出す



あなたの電話番号で**WhatsAppアカウント**を犯人が作成



Facebookの認証コードが**WhatsApp優先で犯人側に届く**ようになる



あなたのスマホにはSMSで認証コードが**届かなくなる**



犯人があなたのFacebookアカウントを操作 → **さらに別の友達に同じ手口で接触**（被害が連鎖的に拡大）

なぜSMSが届かなくなるのか

Facebook、Instagram、WhatsAppはすべてMeta社のサービスで、内部で連携しています。あなたの電話番号にWhatsAppアカウントが紐づいていると、Facebookは認証コードをSMSではなくWhatsApp経由で送ろうとします。犯人があなたの電話番号でWhatsAppアカウントを作ると、認証コードは犯人のWhatsAppに届き、あなたのSMSには届かなくなります。

つまり、2つのものが同時に奪われています。

1. **WhatsApp** — あなたの電話番号で犯人がアカウントを作っている
 2. **Facebookアカウント** — パスワードを変えられ、認証コードも届かない
- この2つを両方とも取り戻す必要があります。

復旧の全体像（この順番でやります）

順番	やること	目的
1	WhatsAppアプリをインストールして電話番号を取り戻す	認証コードを自分が受け取れるようにする
2	Facebook公式の復旧ページから本人確認する	乗っ取られたアカウントを取り戻す
3	パスワード変更・セキュリティ設定	再び乗っ取られないようにする
+	犯人の「裏口」を全部ふさぐ	パスワード変更だけでは防げない攻撃経路を閉じる
4	友達への周知・他サービスのパスワード変更	被害拡大を止める

ステップ1：WhatsAppの電話番号を取り戻す

なぜこれが最初なのか

犯人があなたの電話番号でWhatsAppアカウントを作っているため、Facebookの認証コードがすべて犯人のWhatsAppに届いてしまいます。先にWhatsAppの電話番号を取り戻さないと、Facebookの復旧もできません。

手順

WhatsAppアプリをインストールする

1

iPhoneのApp Storeを開いて、検索で「WhatsApp」と入力します。緑色の電話マークのアイコンの「WhatsApp Messenger」をインストール（「入手」をタップ）してください。

⚠ 検索する時は半角アルファベットで「WHATSAPP」と入力してください。「ワッツアップ」とカタカナで検索すると見つからないことがあります。

2

自分の電話番号で登録を開始する

WhatsAppを開いて、自分の携帯電話番号を入力して進みます。

3

「この携帯電話へのWhatsAppの移動を確認するには…」という画面が出る

犯人がすでにあなたの番号でWhatsAppを使っているため表示されます。

犯人のWhatsAppにコードが送られている状態です。あなたにはこのコードが届きません。これは正常な反応です。慌てないでください。

4

「認証コードが届かなかった場合」をタップする

画面の下の方にあるリンクをタップしてください。

5

「SMS」を選ぶ

選択肢の中から「SMS」を選んでください。これにより、SMSであなたの携帯電話に直接6桁のコードが届きます。

6

SMSで届いた6桁のコードを手動で入力する

あなたのスマホのメッセージ（SMS）に6桁のコードが届きます。自動入力されない場合は手動で入力してください。ハイフンは入力不要で、数字6桁だけ入力すれば大丈夫です。

7

WhatsAppの初期設定を進める

「iCloudから復元しますか」→スキップ／名前を入力→自分の名前／「パスキーを追加しますか」→追加してOK／「チャットのバックアップ」→どちらでもOK

✓ **これで何が起きるか：**あなたがWhatsAppに正規の持ち主として登録されたことで、**犯人のWhatsAppは自動的にログアウトされます。**犯人はWhatsApp経由で認証コードを受け取ることができなくなります。この後のFacebook復旧手順で「WhatsAppでコードを送信する」を選ぶと、あなたのWhatsAppにコードが届くようになります。

ステップ2：Facebookアカウントの復旧

復旧作業の前に：必ず守ってほしいこと

Facebookは、あなたが**普段どの端末（スマホやPC）から、どのネットワーク（自宅のWi-Fi等）でログインしていたか**を記録しています。復旧リクエストを送るとき、普段使っている端末・回線からアクセスすると、Facebookが「この人は本当のアカウントの持ち主だ」と判断しやすくなります。

必ず守ってください：

- ✓ いつも使っているスマートフォンから操作する
- ✓ いつも使っているWi-Fi（自宅の回線等）に接続する
- ✕ 職場のPCや、友人のスマートフォンからは操作しない
- ✕ VPN（仮想プライベートネットワーク）は使わない

これを守らないと、復旧リクエストが「不正な試み」と判断されて自動的に拒否される確率が大幅に高まります。

復旧ページにアクセスする

iPhoneのSafari（ブラウザ）を開いて、以下のURLをアドレスバーに直接入力してください。

<https://www.facebook.com/hacked>

⚠ **Facebookアプリからではなく、必ずSafari（ブラウザ）で開いてください。** LINEやメッセージャーでリンクをタップすると、Facebookアプリが起動してしまい、別のアカウントの画面に飛ばされることがあります。

SafariでURLを入力する方法（慣れていない方向け）

1. iPhoneのホーム画面から**Safari**（コンパスのアイコン）を開く
2. 画面の上部にある**アドレスバー**をタップする
3. キーボードが**日本語入力**になっている場合は、**地球マーク**（🌐）をタップして**アルファベット入力（ABC）**に切り替える
4. <https://facebook.com/hacked>を1文字ずつ入力する（スラッシュは「123」数字モードに切り替えると見つかります）
5. 入力したら「開く」または「Go」をタップ

手順

1

「次へ」をタップ

「アカウントが不正にアクセスされた場合の対処方法」という画面が出ますので「次へ」をタップします。

2

アカウントを検索する

電話番号またはメールアドレスを入力します。まず電話番号で試してください。複数のアカウントが出た場合は、名前やプロフィール写真で判断してください。

3

「私のアカウントです」をタップ

検索結果に表示された自分のアカウントをタップします。

4

「このアカウントの利用を再開する」→「回復する」

「回復する」をタップして進みます。

5

コードの受け取り方法を選択する

「WhatsAppでコードを送信する」を選んでください。ステップ1でWhatsAppを取り戻しているの、あなたのスマホのWhatsAppにコードが届きます。メールで受信できる場合はメールでも構いません。

⚠️ 「WhatsApp」や「SMS」の選択肢が最初の画面に見当たらない場合は、「別の方法を試す」をタップしてください。さらにその先に「もっと見る」というリンクが隠れていることがあります。タップすると、SMS・WhatsApp等の追加の選択肢が表示されます。

6

WhatsAppに届く「リセットコード」を入力する

WhatsAppアプリを開いて、Facebookからのメッセージを確認してください。届いた数字をSafariの画面に戻って入力します。

7

QRコードが表示される — 一人で対処する方法

コード入力後、Safariの画面にQRコードが表示されます。自分のスマホの画面に表示されたQRコードを同じスマホのカメラで直接読み取ることはできませんが、一人でも対処できます。

iPhoneの「写真」アプリでQRコードを読み取る手順：

1. QRコードが表示されている画面のスクリーンショットを撮る（電源ボタン＋音量ボタンを同時押し）
2. iPhoneの「写真」アプリを開く
3. 今撮ったスクリーンショットを表示する
4. 写真の中のQRコードの部分を長押しする
5. iPhoneがQRコードを認識して、「Safariで開く」という選択肢が表示される
6. 「Safariで開く」をタップ

⚠️ Safariの元のタブ（QRコードが表示されていた画面）は閉じないでください。閉じると最初からやり直しになります。

⚠️ 写真アプリでQRコードを長押ししても何も起きない場合は、iPhoneの「設定」→「カメラ」→「QRコードをスキャン」がオンになっていることを確認してください。また、iOS 15以降であればこの機能が利用できます。

それでもうまくいかない場合は、スクリーンショットをLINE等で信頼できる人に送り、QRコードを読み取ってもらい、表示されたURLを送り返してもらう方法でも対処できます。

8

セルフィー動画で本人確認

QRコードのURLを開くと、「セルフィー動画で本人確認を実施」という画面が出ます。これはFacebookの正規の本人確認機能です。「セルフィー撮影をする」をタップして、画面の指示に従って顔を撮影してください。特別な準備は不要です。

9

パスワードの変更画面が表示される

本人確認が完了すると、Safariの元のタブが自動的に「パスワードを変更」画面に切り替わっています。今まで使っていたパスワードとは全く違う新しいパスワードを入力してください。他のサービスと同じパスワードは絶対に使わないでください。変更したパスワードは、iPhoneの「メモ」アプリにすぐ記録してください。

⚠ パスワード変更の途中で「セッションの有効期限が切れました」と表示されることがあります。これは乗っ取り犯も同時にアカウントを操作しているために起きることがあります。「もう一度ログイン」をタップして、**今入力した新しいパスワード**でログインし直してください。新しいパスワードで入れない場合は、変更前のパスワードも試してみてください。

ステップ3：復旧後のセキュリティを固める

Facebookにログインできたら、以下の設定を行ってください。

3-1. すぐにやること

ログイン端末の確認と追い出し

「設定とプライバシー」→「設定」→「アカウントセンター」→「パスワードとセキュリティ」→「ログインの場所」

アカウント名をタップすると、現在ログインしている端末が一覧表示されます。/hacked 経由でパスワードを変更した際に犯人の端末は追い出されているはずです。自分の端末だけが表示されていればOKです。

3-2. 復旧直後はできない設定がある（重要）

/hacked 経由で復旧した直後は、Facebookが「普段使っていないデバイスからのアクセス」と判断するため、**一部の重要な設定変更がブロック**されます。

すぐにできること：

- ✓ パスワードの変更（完了済み）
- ✓ ログイン端末の確認と追い出し

すぐにはできないこと（後日、再度試す）：

- ✗ メールアドレスの追加・変更
- ✗ 2段階認証の設定

これはFacebookのセキュリティ制限です。犯人にも同じ制限がかかるため、むしろ安全を守ってくれています。焦らなくて大丈夫です。

3-3. 後日やること（忘れずに）

2段階認証をオンにする

「パスワードとセキュリティ」→「2段階認証」→「SMSまたはWhatsApp」を選択。これをオンにすれば、パスワードが漏れても、あなたのスマホに届くコードがなければログインできなくなります。設定後に表示される**リカバリーコード**も必ず保存してください（スクリーンショットを撮ってメモアプリに貼り付け）。

メールアドレスの確認と変更

「アカウントセンター」→「プロフィールと個人の情報」→「連絡先情報」から、今使えるメールアドレスを追加し、古い・使えないメールアドレスを削除してください。

連携アプリの確認

「設定とプライバシー」→「設定」→「アプリとウェブサイト」で、見覚えのないアプリが連携されていたら削除してください。

追加チェック：犯人の「裏口」を全部ふさぐ

以下は、パスワード変更と2段階認証だけでは防げない攻撃経路を閉じるためのチェック項目です。犯人はアカウントに入った直後に複数の「裏口」を作ります。パスワードを変えても、これらが残っていると再び乗っ取られます。

★ 最重要：アカウントセンターに犯人のアカウントが紐づいていないか確認する

このチェックが最も重要です。ここを見落とすと、他のすべての対策が無意味になります。

犯人はあなたのFacebookに入った直後に、犯人が作ったInstagramアカウント（ダミー）をあなたの「アカウントセンター」にこっそり連携させることがあります。この連携が残っていると、犯人は自分のInstagramにログインするだけで、パスワードも2段階認証も一切なしに、あなたのFacebookに自由にアクセスできてしまいます。

確認手順：

1. Facebookアプリ → 「三本線（≡）」 → 「設定とプライバシー」 → 「設定」 → 「アカウントセンター」
2. 「プロフィール」をタップ
3. あなたのアカウントセンターにリンクされている**すべてのアカウントの一覧**が表示される

チェックポイント： 自分が作った覚えのないInstagramアカウント、知らない名前のFacebookプロフィール、見覚えのないアカウントがないか確認してください。

不審なアカウントがあった場合： そのアカウントをタップ → 「アカウントを削除」または「アカウントのリンクを解除」 → 確定

⚠ 連携解除がうまくいかない場合は、自分で新しいInstagramアカウントを一時的に作り、自分のアカウントセンターにリンクしてください。これで「最低1つの連携」の条件が満たされ、犯人のアカウントを削除できるようになります。

連絡先情報から犯人の痕跡を消す

犯人は、あなたのアカウントに自分のメールアドレスや電話番号を追加していることがあります。これが残っていると、犯人は「パスワードを忘れた」機能を使って、いつでもアカウントを再び乗っ取れます。

確認手順： 「アカウントセンター」→「個人の詳細」→「連絡先情報」で、自分のものではないメールアドレスや電話番号がないか確認し、不審なものや古いものはすべて削除してください。

不審な連携アプリを削除する

「設定とプライバシー」→「設定」→「アプリとウェブサイト」で、見覚えのないアプリ、不審な名前のサービス、使っていない古いアプリがないか確認し、不審なものは削除してください。迷ったら削除して大丈夫です。

Messengerの送信履歴を確認して不審なメッセージを取り消す

1. Messengerアプリを開く
2. 最近のチャットを確認して、自分が送った覚えのないメッセージがないか探す
3. 見覚えのないメッセージがあったら → 長押し → 「送信を取り消す」（「すべての人の元から削除」を選ぶ）

アクティビティログを確認する

Facebookアプリで自分のプロフィールを開き、「…」 → 「アクティビティログ」をタップ。自分がした覚えのない投稿、知らないページへの「いいね」、知らないアカウントのフォロー、プロフィールの変更がないか確認し、見覚えのないものは削除してください。

なりすましアカウントがないか確認する

犯人があなたの名前や写真を使って偽のアカウントを作っている場合があります。見つけたら、そのプロフィールの「…」メニューから「報告する」 → 「なりすまし」を選んで通報してください。

メール（Gmail等）の安全も確認する

Facebookに登録しているメールアドレスは、パスワードリセットの通知やセキュリティ警告の届け先です。犯人がメールにも入り込んでいたら、Facebookをいくら直してもメール経由でまた乗っ取られます。

Gmailの場合、特に確認すべきこと：

転送ルールの確認（盲点になりやすい）： パソコンで mail.google.com を開き、右上の歯車マーク → 「すべての設定を表示」 → 「メール転送とPOP/IMAP」タブで、見覚えのないアドレスへの転送が設定されていないか確認してください。

フィルタの確認（これも盲点）： 同じ設定画面の「フィルタとブロック中のアドレス」タブで、「facebook」「meta.com」などの条件で自動削除や転送がされるフィルタが作られていないか確認してください。

Gmailのパスワード変更と2段階認証： myaccount.google.com → 「セキュリティ」からパスワード変更と2段階認証の設定をしてください。

ログイン履歴の確認： パソコンでGmailの受信トレイを開き、画面の一番下の右隅にある「詳細」をクリックすると、最近のアクセス元が確認できます。見覚えのない国や地域からのアクセスがあったら、「他のすべてのウェブセッションからログアウト」をクリックしてください。

ログインアラートをONにする

「アカウントセンター」 → 「パスワードとセキュリティ」 → 「ログインアラート」 → 通知をONにする。知らないデバイスからログインがあったとき、即座に通知が届くようになります。

Facebookページ・広告を使っている方は追加確認（該当者のみ）

ページの管理権限： business.facebook.com → 「設定」 → 「ビジネス設定」 → 「ユーザー」で、見覚えのない管理者や編集者がいたら削除。

広告キャンペーン： 広告マネージャで、自分が出した覚えのない広告がないか確認。不審な広告は即座に停止・削除。

支払い情報： 「請求と支払い」で、見覚えのないクレジットカードや不正な請求がないか確認。不正請求があった場合は、Metaサポートに報告し、カード会社にチャージバックを申請してください。

ステップ4：被害の拡大を止める

4-1. 友達に知らせる投稿をする

復旧したFacebookアカウントで**全体公開**の投稿をしてください。投稿の例文：

「私のFacebookアカウントが乗っ取られていました。最近、私のアカウントから届いた"インフルエンサープログラム"に関するメッセージは、すべて乗っ取り犯が送ったものです。絶対にリンクを開いたり、認証コードや電話番号を教えたりしないでください。もし対応してしまった方は、すぐにご連絡ください。ご迷惑をおかけして申し訳ありません。」

4-2. 他のサービスのパスワードを至急変更する

同じパスワードを使い回していた場合、そのパスワードを使っているすべてのサービスが危険です。

変更の優先順位：

1. **銀行・金融機関**（ネットバンキング等） ← **最優先**。ログイン自体はパスワードだけでできてしまうことがあります。
2. **メール**（Gmail等）。メールアカウントを乗っ取られると、他のすべてのサービスのパスワードリセットができてしまいます。
3. **Facebook以外のSNS**（Instagram、LINE等）
4. **その他のサービス**（ネットショッピング、サブスクリプション等）

4-3. iPhoneのパスワードアプリを活用する

iPhoneには「パスワード」という標準アプリがあります。ホーム画面を下にスワイプして「パスワード」と検索すると見つかります。⚠マークがついているものは、パスワードの使い回しや漏洩が検知されたものです。**すべて異なるパスワードに変更してください。**

復旧がうまくいかない時のQ&A

Q. WhatsAppで「認証コードが届かなかった場合」をタップしてもSMSが届かない

カウントダウンが表示されることがあります。「次の時間が経過したら、新しいコードが送信されます」と表示されたら、カウントが0になるまで待ってから「新しいコードを取得」をタップしてください。

Q. facebook.com/hacked にアクセスするとFacebookアプリが開いてしまう

LINEやメッセージャーからリンクをタップすると、Facebookアプリに飛ばされることがあります。**Safariのアドレスバーに直接URLを手入力してください。** キーボードが日本語入力になっている場合は、地球マーク (🌐) をタップしてアルファベット入力 (ABC) に切り替えてから入力してください。

Q. facebook.com/hacked でパスワードを入力しても「正しくありません」と出る

犯人がすでにパスワードを変更している可能性があります。「別の方法を試す」をタップしてください。さらに「もっと見る」というリンクが隠れていることがあります。タップするとSMS等の選択肢が出てきます。

Q. 写真アプリでQRコードを長押ししても反応しない

iOS 15以降の機能です。iPhoneのバージョンが古い場合は使えません。その場合は、スクリーンショットをLINE等で信頼できる人に送り、QRコードを読み取ってもらい、表示されたURLを送り返してもらってください。

Q. 「セッションの有効期限が切れました」と何度も表示される

乗っ取り犯も同時にアカウントを操作している場合に起きることがあります。何度かログインし直してください。パスワードは変更直後の新しいものを使ってください。新しいパスワードで入れない場合は、変更前のパスワードも試してみてください。

Q. 復旧後に「現在はこの変更はできません」と表示される

Facebookが「普段使用していないデバイス」と判断しているためです。パスワード変更とログイン端末の確認だけは先に済ませて、メールアドレスの変更や2段階認証の設定は後日、再度試してください。

Q. 「本人かどうかの確認にご協力ください」という通知が来た

誰かがあなたのアカウントにログインしようとしている時に表示されます。自分がログイン操作をしていないタイミングで表示された場合は、「いいえ、私ではありません」をタップしてください。

Q. 犯人は何が目的なの？

乗っ取ったアカウントを使って、そのアカウントの友達に同じ詐欺メッセージを送り、連鎖的にアカウントを乗っ取っていきます。最終的にはアカウントを使った広告出稿や、さらなる詐欺行為に利用されます。

今後このような被害に遭わないために

今後ずっと覚えておきたい3つのこと

① 「6桁のコードを教えて」は、どんな相手でも100%詐欺。

Facebook、Instagram、LINE、Google——どのサービスであっても、友人や家族を名乗る相手から「コードを教えて」と言われたら詐欺です。本物のサービスが他人経由でコードを要求することは絶対にありません。

② 3ヶ月に1回、セキュリティ設定を見直す。

ログインの場所、アカウントセンターのリンク済みアカウント、連絡先情報、連携アプリ——この4つをざっと確認する習慣をつけてください。5分で終わります。

③ 不審なメッセージが来たら「まず電話で本人に確認」。

友達から急にリンクやお願いが届いたとき、チャット上で返信するのではなく、電話やLINEなど別の方法で本人に直接確認してください。これだけで、ほとんどの被害を防げます。

絶対に守ること

- ・認証コードは絶対に他人に教えない。どんなに親しい友人からのお願いでも、認証コードや電話番号を求められたら、それは乗っ取り犯です。
- ・パスワードを使い回さない。iPhoneのパスワードアプリを使えば、サービスごとに異なるパスワードを自動生成・保存できます。
- ・2段階認証をオンにする。Facebook、Gmail、銀行など重要なアカウントには必ず設定してください。

怪しいメッセージの見分け方

以下のようなメッセージが来たら、すべて詐欺だと思ってください。

- ・「インフルエンサープログラムに招待します」
- ・「認証コードを送るので教えてください」
- ・「コードを送るために電話番号を教えてください」
- ・突然の儲け話や投資の話

ビジネスをしている知人から来ても、メッセージャー上のメッセージだけでは本人である保証はありません。少しでも違和感があれば、電話やLINEなど別の手段で本人に直接確認してください。

パスワードの使い回しが発覚した場合

今回の乗っ取りをきっかけに、複数のサービスで同じパスワードを使っていたことが分かった場合、そのパスワードを使っている**すべてのサービス**のパスワードを変更してください。iPhoneのパスワードアプリを開いて、マークがついているものをすべて変更することをおすすめします。特に銀行・金融機関、メール（Gmail等）は最優先です。

最後に

乗っ取られたことは恥ずかしいことはありません。犯人の手口は巧妙で、実在する友人の名前で届くメッセージを疑うのは簡単ではありません。今回のケースでも、ビジネスをしている知人からの「インフルエンサープログラム」という話を、何の疑いも持たず信じてしまったことがきっかけでした。

大切なのは、気づいた時点ですぐに対処することです。放置すると、あなたのアカウントからさらに被害が広がります。

この文書の手順に沿って、1つずつ進めてください。焦らなくて大丈夫です。

このマニュアルを周りの方にも共有してください。今回のような乗っ取りは、ひとりの被害が友人ネットワーク全体に連鎖する仕組みです。復旧が完了したら、身近な方——特にITに詳しくないご家族やご友人——に渡してあげてください。「知っているかどうか」だけで、被害を防げます。