

## LINE アカウント乗っ取りを防ぎ、安全に使うためのポイント

### 1 他人にあなたの趣味嗜好や行動パターンを覗かれないために

なぜ？→あなたの行動行動パターンが分析され、それに合った広告配信されてしまう

#### ① 対策

ホーム画面右上の歯車マーク→プライバシー管理→Web 行動履歴を利用した追跡  
広告の受信→オフにする

#### ② 対策

ホーム画面右上の歯車マーク→プライバシー管理→LINE 内部識別子を利用した追  
跡型広告の受信→オフにする

#### ③ 対策

「対策②」の下にある「詳細を見る」をタップ→長文の途中に「お客様がお使いの  
ブラウザから取得するウェブサイトの行動履歴と…」というアンダーラインが引  
かれた部分をタップする→次の画面の下部に「有効」「無効」のボタンが現れる→  
「無効」を押す

### 2 位置情報を覗かれないために

なぜ？→外出先などで近くにある店やサービスの広告が配信されてしまう

#### ① 対策

ホーム画面右上の歯車マーク→プライバシー管理→情報の提供→位置情報の取得  
を許可→オフにする

### 3 企業や著名人などが運営する公式 LINE でのメッセージのやりとりや LINE 無料通話の履歴を覗かれないために

なぜ？→あなたの関心にあったコンテンツや広告が配信されたり、AI の学習データと  
して利用されてしまう

#### ① 対策

ホーム画面右上の歯車マーク→プライバシー管理→情報の提供→コミュニケーシ  
ョン関連情報→オフにする

#### ② 対策

「情報の削除」を押すことで、これまで取得されてしまった情報がある程度削除で  
きる

### 4 あなたの友達とのトーク内容を保護するために

既定では、トーク内容を暗号化して他者から除かれない設定になっている。ただし、あ  
なたと友達の双方が設定オンになっていないと、内容が暗号化されないので注意。

#### ① 確認

ホーム画面右上の歯車マーク→プライバシー管理→レターシーリング→オンにな  
っていれば OK！

### 5 詐欺師グループから狙われないために

詐欺師たちは電話番号を手がかりにして LINE の個人情報抜き取りをしている

#### ① 対策

ホーム画面右上の歯車マーク→友だちをタップ→友だちへの追加を許可

② 対策

ホーム画面右上の歯車マーク→友だちをタップ→友だち自動追加をオフにする

6 さらに被害を最小限にするために

あなた自身だけではなく家族や友人まで巻き込んでしまうリスクを減らしましょう

① 対策

(LINE ではなく) スマホの設定「歯車マーク」→アプリ→アプリ一覧のなかから  
LINE を選択→権限または許可→連絡先→許可しないにする

7 既に乗っ取られていないかを調べる方法

LINE はスマホからだけでなく、パソコンやタブレットからも利用できる。使い方によっては便利な機能だが、悪意の第三者からもログインされる危険性も

① 対策

ホーム画面右上の歯車マーク→アカウント→ログイン中の端末（表示されていないければ「ログイン許可」を一時的にオンにする）→現在あなたの LINE にログインしているスマホ以外のパソコン・タブレットなどが表示される

② 対策

①で見知らぬ端末名が出てきた場合、「ログアウト」ボタンを押し強制的に追い出すことが出来る。「現在ログイン中の他の端末がありません」という表示が出ていたら安心。

③ 対策

そもそもスマホ以外で LINE を使うことはないという方は、ログイン許可をオフにしておきましょう。

ホーム画面右上の歯車マーク→アカウント→ログイン許可をオフにしておく

8 今の LINE 設定が正しい情報になっているか調べる

トラブルが起きたときに必要な「本人確認」。以前のガラケーの電話番号や使っていないメールアドレスが LINE に登録されたままになっていませんか？

① 確認方法

ホーム画面右上の歯車マーク→アカウント→電話番号・メールアドレスを確認

9 衝撃の内容！LINE の場合【パスワードでログイン】は大変危険！

犯罪者の LINE 乗っ取りの7割は、パスワードでログインされている。つまり何らかの原因でパスワードが漏れてしまうと LINE はすぐに乗っ取られる。

LINE はパスワードでログインをオフにしておき、QR コードを使う。これだと自分のスマホがないとログイン出来ないので安全。

① 対策

ホーム画面右上の歯車マーク→アカウント→パスワードでログイン→オフにする

② さらに強化策

それでも誰かがログインしようとした場合、あなたに通知が届き、これを許可しない限りログイン出来ない保険のような機能があります。

①の項目の上にある「Web ログインの2要素認証」→オンにしておく