

## LINE に危険性はあるか、その仕組みと過去のトラブル対応

[友だちを割り出す仕組み\(アドレス帳による友だち自動追加\)](#)

[トークや通話の暗号化\(レターシーリング\)](#)

[アカウント乗っ取り事件と2段階認証](#)

[トーク画面流出騒動とクローン iPhone による同時アクセス封じ](#)

[18歳未満のLINE ID 検索を制限](#)

[青少年のLINEトラブルへの啓蒙活動](#)

## LINE を使うと情報漏洩する？ 個人情報を守って安全に使う方法

LINE は便利ですが、さまざまな方法で情報漏洩されてしまう危険もあります。LINE の情報漏洩を防ぐ方法をまとめると、以下のとおりです。

友だちの自動追加をしない、させない

不正ログインされないようにする

暗号化されていないWi-Fiを使わない

スマホを貸したり、手放したりしない

## 電話帳情報を漏洩しないための設定方法

LINE で電話番号を登録すると、その番号を電話帳に登録している相手が「友だち」として表示されます。しかしこれは、電話帳情報を LINE の運営側に送信していることと同義です。

この情報送信に抵抗がある方は、つぎのように設定することをおすすめします。

## 「友だち自動追加」「友だちへの追加を許可」をオフにする

友だち自動追加をオフにすると、電話帳が勝手に LINE 側へ送信されるのを防げます。また、友だちへの追加をオフにすれば、あなたを電話帳に登録した人物から勝手に友だち登録されません。

1. 「右上の歯車アイコン」⇒「友だち」をタップ 2. 「友だち自動追加」と「友だちへの追加を許可」をオフにする



## 不正ログインされないようにする対策

悪意のある人物にアカウントを乗っ取られると、情報漏洩どころか詐欺行為などの犯罪行為に悪用される場合も考えられます。これを防ぐには、つぎのような設定が有効です。

ログインパスワードを複雑なものにする

パスコードロックをオンにする

PIN コードを設定する

他端末ログイン許可をオフにする

## Wi-Fi を使ったハッキングを防止する対策

悪意を持った人物の Wi-Fi に接続するだけで、ハッキングはいともたやすく実行されてしまいます。そのため自動接続をオンにするとか、「Free\_Wifi」など公衆 Wi-Fi を装った回線に接続しないことが重要です。

Wi-Fi の自動接続をオフにする

通信が暗号化されていない Wi-Fi (カギマークなし) を利用しない

本当に公共施設、店舗が提供する Wi-Fi か確認して利用する

## ウイルス感染での情報漏洩を防ぐ対策

スマホもパソコンと同様にウイルス感染します。

ウイルス感染すると情報を盗まれる可能性もあるため、注意が必要です。

スマホでウイルス感染する事例の多くが「悪質なアプリのインストール」です、とくに注意すべきは無料アプリのインストールといえます。

アプリ提供元が信頼できるか確認

アプリのレビューを確認(ただしサクラがいる可能性も)

アプリは Google Play など公式ストアから取得する

セキュリティアプリをインストールする

## スマホ版 LINE | 情報漏洩を防ぐ 3 つの対策法と未然防止の知識

### 1.LINE の個人情報をごっちり守る 3 つの情報漏洩対策

[①スマホ自体にパスコード、指紋認証を設定する](#)

[②LINE のパスコードロックを設定する](#)

[③設定した LINE アカウントのメールアドレス・パスワードを厳重に管理する](#)

### 2. 情報漏洩を未然に防ぐために知っておくべき 5 つの流出経路

[①第三者にスマートフォンを直接操作される](#)

[②LINE アカウントへの不正ログイン](#)

[③別の端末\(iPhone\)からの情報漏洩](#)

[④バックアップデータの送信ミス](#)

[⑤トークの相手が履歴を公開する](#)

### 3. LINE を安全に利用する 7 つのセキュリティ対策

[①利用前にはアドレス帳の送信に注意](#)

[②常に最新バージョンの LINE アプリを使う](#)

[③見ず知らずの人からのメッセージを拒否する](#)

[④「友だち自動追加」「友だちへの追加を許可」をオフにする](#)

[⑤ID 検索による友だち追加を拒否する](#)

[⑥メッセージ通知の本文内容を非表示にする](#)

[⑦他の端末からのログインを許可しない](#)

### 4. まとめ

LINE は手軽に利用できるコミュニケーションツールですが、使い方によってはプライベートな情報が漏洩してしまうケースもあります。しかし、その原因はユーザー自身の管理能力不足によるところが大きく、日頃からスマホやパスワードの管理を徹底していれば防げる場合がほとんどです。

これから LINE を安全かつ安心して使うために、

スマホ自体にパスコード、指紋認証を設定する

LINE のパスコードロックを設定する

アカウントのメールアドレス・パスワードを厳重に管理する

この 3 つは、最低限のセキュリティ対策として必ず実施してください。

### LINE の「サービス向上のための情報利用…(同意画面)」情報利用を“拒否”する方法

サービス向上のための情報利用に関するお願い



LINEは不正利用の防止、サービスの提供・開発・改善や広告配信を行うために以下の情報を利用します。友だちとのテキストや画像・動画などのトーク内容、通話内容は含みません。これらの情報は、LINE関連サービスを提供する会社や当社の業務委託先にも共有されることがあります。また、今回の方針変更に伴い、[プライバシーポリシーも変更](#)されます。

LINE の画面に唐突に表れた「サービス向上のための情報利用に関するお願い」とはいったいなにかの。事の発端は 2018 年 1 月 16 日前後に表れ始めた LINE の同意画面だ。突然表れた同意画面に動揺を隠せなかった方もいるだろう。私も突然表れた同意画面に戸惑いはあったが、急いでいたこともあり「なにか出てきたけど、同意しないと LINE が使えないかも。」と同意をしてしまった口だ。

ラインはLINE株式会社が提供しているコミュニケーションアプリである。スマホの浸透と共に、様々なデバイスで利用できることから日本のインフラの一部として活躍しているラインは、老若男女を問わず親しまれているメッセージ App だ。Android や iOS など OS を気にすることもなく 簡単にメッセージのやり取りもできることからメールに打って変わって重宝される様になった対話ツール。しかし、こうした App の存在は、それを提供する者がいて存在し、使用をする上で App を提供する会社(デベロッパー) との規約は必ず存在する。

今回、LINE は新たな一手として、次の様なサービス向上に関する同意画面を表示させた。

これから新規で LINE のアカウントを取得する際にも表示されると思われます。

「サービス向上のための情報利用に関するお願い」全文 情報利用に関するお願いは以下の通りだ。

LINE は不正利用の防止、サービスの提供・開発・改善や広告配信を行うために以下の情報を利用します。

友だちとのテキストや画像・動画などのトーク内容、通話内容は含みません。

これらの情報は、LINE 関連サービスを提供する会社や当社の業務委託先にも共有されることがあります。また、今回の方針変更に伴い、[プライバシーポリシーも変更](#)されます。

## 利用される情報

友だちとのコミュニケーションに関する以下の情報

- スタンプ、絵文字、エフェクト・フィルター
- トークの相手、日時、既読、データ形式、取消機能や URL へのアクセスなどの利用状況
- タイムラインの投稿内容、周辺情報(「自分のみ」の投稿は周辺情報のみ。周辺情報とは、投稿日時、投稿されたコンテンツの形式、コメント欄のスタンプ、観覧時間等です。)

※送信取消されたものも含みます。

公式アカウントとのトーク内容を含むコミュニケーション

LINE が提供しているブラウザ、保存や共有といった各種機能の利用状況

※トークルームで保存や共有といった機能を使った場合、その対象コンテンツのデータ形式等も利用できます。

LINE 経由で URL にアクセスした際のアクセス元情報

例えば、友だちとのトークルームからアクセスした場合、そのトークルームのことを指します。

この他、「通知メッセージ機能」もご利用いただくことが可能です。

**同意することに危険はあるのか** この情報から分かることは次の通り。

一般の友だちとのトーク内容は利用しないが、どんな操作をして、どういうスタンプを使い、誰とトークをしているのか、そこに流れてきた画像などを どう扱う(保存など) のかなど、既読になる時間はどのくらいか、ほぼ全てのことについて、LINE はデータ収集をして利用する。ということになる。

なお、企業アカウントとのトークは、全文提供する形だ。

トークの内容は利用しないと言われても「あなたの行動は常に監視をしています。」と捉える方も少なからず

いるのではないだろうか。企業アカウントのトークを利用すると言われれば、「荷物番号などの情報も LINE に利用されてしまうのか」など、様々な危険性を示唆する声も聞こえてきそう。

LINE の件を交えて少しインターネットの情報についてお話をするが、LINE を含むインターネットの回線を利用したデータの送信や受信には、インターネット上に置かれたサーバー(機械) を経由して相手と情報のやり取りを行っている。

LINE も LINE が管理をするデータサーバにトークを送信することで、相手先へ内容が転送されておりそのデータの中にはトーク内容やトークに使われたスタンプの内容も一緒に送信されている。

今回「同意」をする事で、その情報の他に、どういう操作を行ったのか、誰と話しているのかをデータとして LINE に送信することに同意を求めた形となる。ただし、先にも書いたように、「(個人間の) トーク内容は利用しない」という旨が記載されていることから、今後も内容自体について監視をされることはなさそう。

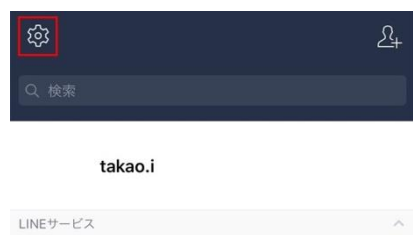
しかし、今も昔もトークを含めた内容が LINE に送信され、それを介して相手へメッセージが伝わることには変わりはなく、安全面からも LINE に関わらず暗証番号などの第三者に知られてはいけない内容については十分に注意を払う必要はあるだろう。

## 設定を変更することもできる

LINE では情報を利用することに同意をする形となっているが、そのデータを提供するか否かをオンオフをする事ができる。

### 設定 > プライバシー管理 > 情報の提供

#### ▼設定画面を開く



LINE 画面の下部帯から「友だち(一覧)」を表示させ、左上にある**設定(歯車)** をタップする。

#### ▼「プライバシー管理」を開く



## ▼「情報の提供」を開く



## ▼チェックの有無を確認する



「情報の提供」設定にあるチェックを外していく作業で、以下の情報の送信を止めることができる。

### トークルーム情報

トーク内容を除いた操作などの情報が LINE に送信される(企業とのやり取りは除く)。日本では個人情報が発信することをあまり好まない傾向にあり戸惑う方も多い。違和感を覚える場合はチェックを外しておこう。

### ウェブ追跡型広告の受信

ユーザーが利用した単語などから関心が高いと想定される商品を広告として表示させる機能。昨今のインターネット広告ではよく使われる馴染みのある手法で、ユーザー視点の広告が表示される。「どうせ表示されるなら興味のある広告がいい」と思う方はオンにしておき、「なんだか嫌だ」と思う場合にはチェックを外す。

### 通知メッセージ

「通知メッセージ」は、企業と LINE に登録された電話番号を照合して、番号が一致した場合に企業から配送や決済などに関する重要な通知を受信する通知が送られるサービスのことだ。

このサービスは、電話番号を利用することで本人を特定して、企業とのやり取りをする設定となっている。この機能を利用するには、予め企業のアカウントを友だち追加することが必要な場合もあり、あまり馴染みがなく悩んでいる場合は外しておいても構わないだろう。

### LINE Beacon

ラインビーコンは、Bluetooth(近距離データ通信) を利用したサービスで、お店の近くを通ると LINE に そのお店の商品やクーポン情報が届くというものだ。このチェックがオンになっていても スマホの Bluetooth 接続がオフになっている場合は設定が機能しない。

以下は参考資料です。 ctrl キーを押しながらクリックで Web ページが表示されます。

[LINE の使い方 総まとめ](#)