



サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

SNSの乗っ取りやなりすましメールに注意！！

✓ SNS（LINE、Instagram等）でアカウント乗っ取り被害が多発しています。

例えば
こんな手口

知人からの「投票お願い」は乗っ取り!?

① SNSを乗っ取られた
知人のアカウントから
メッセージが届く。



※知人のアカウントもすでに乗っ取られています。

② コンクールの投票を
依頼され、電話番号を
聞かれる。



※電話番号はパスワード変更をする
ために使用されます。

③ 「投票に認証コード
が必要」と求められ、
送信されてきたコード
を教えてしまうと乗っ
取られる。



※このコードはパスワード変更の
許可を与えるものです。

もしもアカウントが乗っ取られたら？



1 ログインできる状態であれば、すぐに
新しいパスワードに変更する。

※ ログインができない状態であれば、すぐにヘルプセンター等へ
連絡してください。

2 使用するパスワードは、他のアカウントで
使いまわさない。

3 自分以外の見覚えのない端末は、すべて
ログアウトする。

※ 特にパスワードを変更する時は、このチェックを入れずにいると、他の端末ではログアウト
されず、再度乗っ取られてしまう可能性があります。

パスワードを変更

現在のパスワード

新しいパスワード

☒ すべてのデバイスから
ログアウトする

対策のポイント

- パスワード認証だけでなく、必ず多要素認証やパスキーの設定をしましょう。
- 他人事ではなく自分事として考え、自己のセキュリティ意識を高めましょう。



大阪府警察ウェブサイト

その他サイバー犯罪対策に関する事は
大阪府警察のウェブサイトやXを確認ください



大阪府警察サイバーセキュリティ対策情報 X