

Instagram、フェイスブックなどのSNSアカウントを
乗っ取られる被害が多数発生中！！

投票依頼に関するメッセージに注意！

～手口の紹介～

- ① 犯人に乗っ取られた友人等のアカウントから、「アンバサダーに立候補したので投票して」などと、フェイスブックやInstagramでダイレクトメッセージが届きます。
- ② 友人に協力しようとして、投票に了承すると、**電話番号を聞かれ、相手から「SMS（ショートメッセージ）にアカウントの認証番号やリンク先URLをDMに貼って返信して」**等と指示されます。
- ③ 相手の指示通りにすると、アカウントが乗っ取られます！



友人になりすました犯人



アンバサダーに立候補したよー！
上位目指してるから、投票に協力
してくれない？「WhatsApp」という
アプリをダウンロードして！



投票のリンクを送るから
電話番号を教えて！



ショートメッセージが届くよ！
メッセージの数字6桁（又はメッ
セージのURL）を教えて。



アカウントの乗っ取り成功！
※新たに乗っ取ったアカウントの
フォロワーへまた被害が拡大していく...

ダイレクトメッセージの例

被害者



オッケー！任せて☆



あれ？教えてなかった？
090-**-**だよ！



届いたよ！
12345678
(又は<http://>～)だよ。

犯人は認証番号やリンク先を入手すれば、フェイスブックやInstagramなどのSNSアカウントにIDやパスワードを入力することなく、**パスワードを再設定し被害者のアカウントにログインできるのです！**

対策

- ① SNSで電話番号や認証番号を教えない
- ② アカウントに多要素の認証（生体認証、SMS等）を設定する
- ③ SNSのヘルプセンター等に不正アクセス被害を報告する
- ④ 不正アクセスされたことを自分自身のフォロワーに注意喚起する

