



伊豆中央警察サイバー通信 第5号

SNSアカウントの乗っ取りに注意！

既に乗っ取られた友人のアカウントから次のようなメッセージが来ます。

パターン1：フィッシング（アカウント乗っ取り）



友人になりすまし

私のSNSデータが消失してしまいました。解除するには、何人かの友人の確認が必要となりますので、下記サイトにアクセスしてあなたのアカウントでログインしてください。

<https://●●●●●>

フィッシングサイトに誘導



情報を入力するとアカウント乗っ取りの被害に遭う可能性が高いです。

パターン2：プリペイドカード情報の送信を求める



友人になりすまし

近くのコンビニでプリペイドカードを何枚か買ってきて欲しんだけどいいかな？

大丈夫だよ

お金は明日渡すよ。
今、買ってきてもらえるかな。
●万円分のカードを買って、カードに書かれた16桁のコードの写真を撮って送ってください。

犯人がカード残高を利用できるようになります。



カード情報送信

注意事項

犯人は乗っ取ったアカウントを使って、**友だちリストに登録されているアカウントに対して**上記の様なメッセージを送信してきます。

メッセージで、「サイトにアクセスを求めるもの」や「プリペイドカード情報の送信を求めるもの」は犯罪被害に遭う可能性が高いため、**電話等で直接送信者に確認**してください。

また、パスワードやPINコードは**他人に教えない**ようにしましょう。

