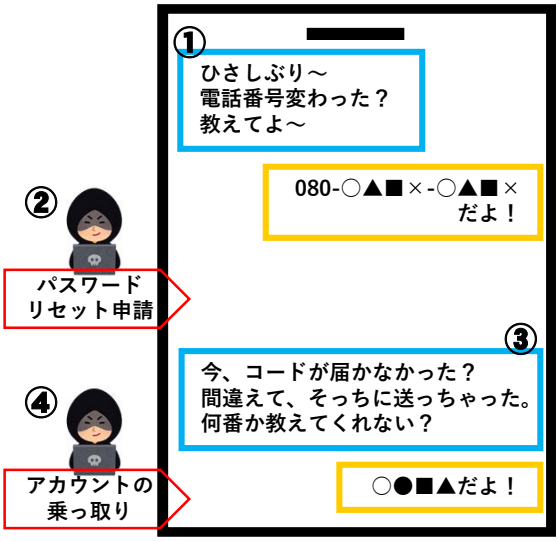
Vol. 2
令和７年３月25日
鹿児島県警察本部
サイバー犯罪対策課
Tel　099－206－0110

かごしまサイバー通信

【注意警報】SNSアカウントの乗っ取りに注意！

どのようにして乗っ取られるの？

SNSで認証された電話番号等が流出することでアカウントを乗っ取られます。
気づかずにパスワードリセット用の認証コード等を他人に教えたために、アカウントが乗っ取られるケースが増えています。



① 第三者が、知人を装いあなたの電話番号を聞き出す。
② 第三者が、パスワードリセット申請を行う。
③ パスワードリセット用の認証コードやURLが送信される。
④ 認証コードやURLを第三者に教えることで、SNSアカウントが乗っ取られる。

アカウントを乗っ取られたら、どうすればいいの？

★ SNSの「運営会社」へ連絡し「アカウントが乗っ取られた」ことを伝えてください。（対象SNSが「X」であれば「X」へ、「Instagram」であれば「Meta」へ連絡します。）

★ 各運営会社への連絡先は、インターネットで「SNS名＋ヘルプセンター」などと検索してください。

対策

★ 認証コード（数字４桁や６桁）やURLを第三者に教えない。

★ ID・パスワードの管理は適切に。

★ 多要素認証を利用する。

（「多要素認証」とは、サービスへのログインを安全に行うために、二要素以上を使って認証作業をすることです。「多要素認証」の例としては、「ID・パスワードの入力後、ワンタイムパスワードの入力を行う」などがあります。）