2019 年 6 月 30 日
在ドバイ日本国総領事館

電話・ＳＮＳを利用した詐欺被害に対する注意喚起
～ワン・タイム・パスワードは絶対に他人に教えないでください！～

電話やＳＮＳを介して個人情報をだまし取り，銀行口座から金を詐取する手口の詐欺被害が発生しています。相手が銀行や公的機関を名乗っていても，（個人の）携帯電話で連絡してくる場合は十分な注意が必要です。また，不用意にＩＤやワン・タイム・パスワードを相手に教えることは絶対にやめましょう。

【手口と特徴点】

○　犯人は，実在する銀行や公的機関の職員を名乗るだけでなく，WhatsApp 等のＳＮＳアカウントの写真を銀行等のロゴに設定したり，実際に銀行等が発出するメール等の内容に似せたりして，周到に準備しています。

○　犯人は，「このままだと口座が凍結される」「取引ができなくなる」など緊急性の高いメッセージを送信してきます。被害者がそれに応えて電話すると，手続に必要であるなどとして，ＩＤやクレジット･カード等の写真を送信するように要求してきます。

○　犯人は，こうした個人情報をもとに，被害者の口座から自らの口座等に送金する手続をオンラインで行います。この際も，通話を続けたままにするように言い，被害者が他者に連絡できないようにします。

○　送金を完了するためには，被害者の携帯電話等に送信されてくるワン・タイム・パスワード（ＯＴＰ）が必要ですが，犯人は「今すぐ手続をする必要がある」などと言葉巧みに話し，被害者にＯＴＰを教えるよう求めてきます。被害者がこれに応じると，取引が完了してしまい，口座からお金を詐取されてしまいます。

○　なお，携帯電話で各種手続をする際には，本人確認のために携帯電話あてに照合番号（Verification Code。４桁の番号であることが多い。）を送信し，それを回答するように求められることがあります。これは，送金等の取引完了のために用いられるＯＴＰ（６桁の番号であることが多い。）とは異なるものですので，注意が必要です。

以下のようなポイントに注意して，被害の防止に努めてください。

※　通常，銀行や公的機関がＳＮＳで個人情報を要求することはあり得ません。

※　また，銀行や公的機関の職員が個人の携帯電話で連絡してくることはありません。

※　不審な電話，身に覚えのない申出やメッセージには応じず，無視しましょう。

※　ＯＴＰは，送金取引を完了させるために必要な重要な情報です。決して他人には教えないようにしましょう。

※　メッセージを受けても，すぐに反応せず，誰かに相談するなど，冷静に対応しましょう。

被害に遭ってしまった場合や，詐欺と思われるアプローチを受けた場合は，在ドバイ日本国総領事館領事班に御相談ください。

以上