SIM スワップ詐欺に要注意

スマホ回線が突然切れ、その間に多額の財産が盗まれる「SIM スワップ詐欺」が増えています。スマホには、「SIM カード」と呼ばれる契約者情報を記録した小型のカードが挿入されています。

SIM スワップとは、サイバー犯罪者がこの他人の「SIM カードの複製を入手」することです。犯罪者は他人の情報の入手のためフィッシング詐欺で、他人の ID、電話番号、フルネーム等を入手し、情報を手に入れると電話やインターネット等で、携帯電話会社に連絡し、他人（被害者）に成りすまし、SIM カードの複製を手に入れる方法です。

携帯ショップで SIM カードの発行を行いますが、携帯ショップで必要になるのが、被害者名義の身分証明書で、写真をすり替えた偽造運転免許証等を提示し、本人（被害者）を偽り、新しい SIM カードを取得し、被害者のスマホを乗っ取ります。

犯罪者は、手に入れた複製の SIM カードをスマホ端末に挿入するだけで、通話記録、メッセージ履歴等、被害者のアカウント上の情報やデータすべてにアクセスできます。この時点で、犯罪者に、アカウントの支配権が完全に握り、被害者の銀行アプリにアクセスして別の口座に移動ができます。本人に気づかれないように銀行口座から不正の送金するのが「SIM スワップ詐欺」です。

SIM スワップ詐欺を防ぐには

① 個人情報の取扱いに注意する。

○ サイトが公式か、SSL による通信の暗号化された接続である等セキュリティ対策が施されているか、また、URL が「https://」で始まっているを確認します。

② フィッシング詐欺に注意する。

○ 身に覚えのある送信名でも、文章にスペルミスや文法ミス等が含まれるメールやテキストメッセージを警戒します。ドメインにも最新の注意を払い、偽物でないことを確認するほか、怪しいリンクや添付ファイルを開かない。

③ 通信が途絶えていないか確認する。

○ 複製の SIM カード使用されると、被害者の携帯 SIM カードはモバイルネットワークにアクセスできないため、電話やメールの発受信が出来なくなります。この場合は至急、警察や携帯電話会社に連絡し、SIM の無効化とデータ回復の手続きを取ります。