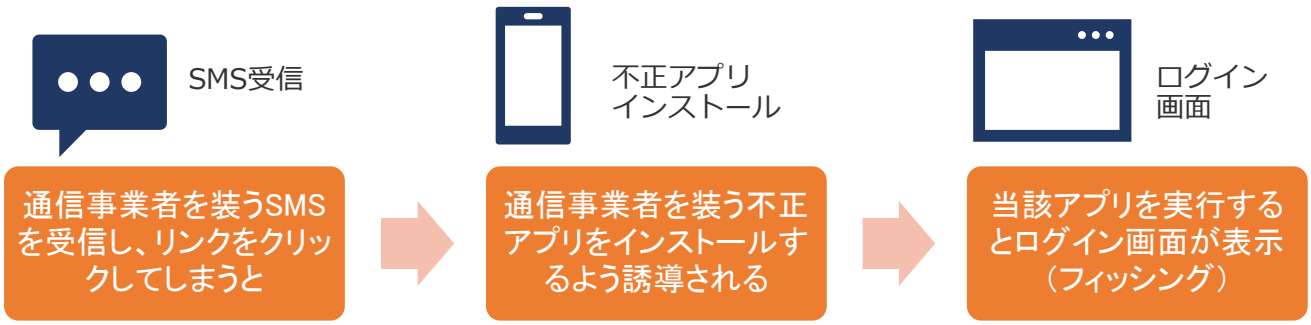
不正アプリに要注意！

～不正アプリによるフィッシングの手口～

○　通信事業者を装うＳＭＳにより不正アプリをインストールするよう誘導。
○　アプリを実行するとログイン画面が表示、その後暗証番号等の入力画面となり、そこで入力すると個人情報が盗み取られる。
○　Android端末だけでなく、iPhoneでも確認されています。

図　通信事業者を装うフィッシングの手口



※出典：一般財団法人日本サイバー犯罪対策センター

～被害に遭わないために～

■　電子メールやＳＭＳのメッセージに含まれているリンク先を安易にクリックしないこと。
■　通信事業者からの通知内容を確認するときは、公式サイトから確認すること。
■　アプリのインストールは、正規のアプリ通信サイト等の信頼できるサイトから行うこと。
■　ＩＤ・パスワードを入力する際は、信頼できる方法で表示した画面であることを確認して入力すること。
■　通信事業者の公式サイトにおいて、フィッシングに関する注意及び対策内容を確認すること。

【お問い合わせ先】
高知県警察本部生活安全部サイバー犯罪対策課　TEL088-826-0110