青い森のサイバーセキュリティ

令和４年２月
青森県警察本部保安課
サイバー犯罪対策室

通信事業者を装う偽SMSと不正アプリ

iPhoneにも通信事業者を装う偽SMSが！

令和３年10月号でもお知らせしたところですが、当初Android端末のみを対象としていたこの手口が、iPhoneにおいても確認されましたので、改めてお知らせします。

特に今回は、ＳＭＳ（ショートメッセージサービス）から不正アプリをインストールさせ、ネットワーク暗証番号等を抜き取ろうとするのが特徴となっています。

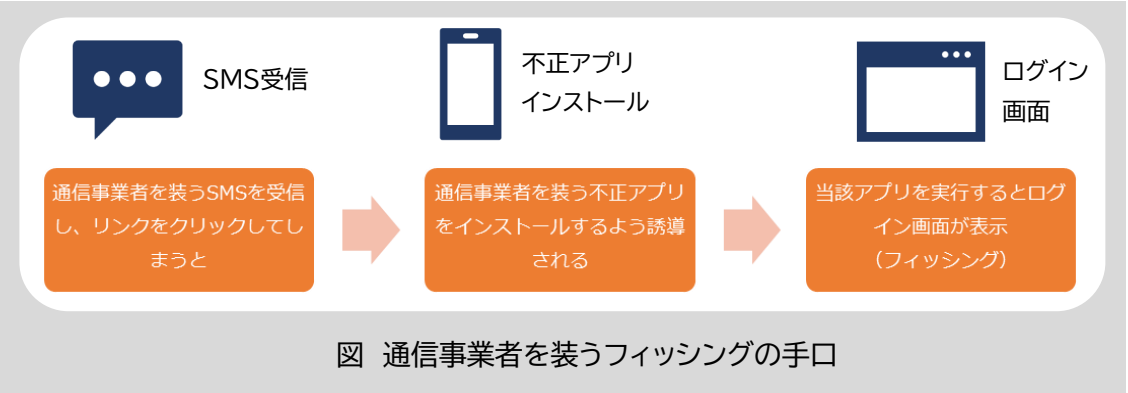

図　通信事業者を装うフィッシングの手口

iPhoneでの手口～構成プロファイルの悪用による不正インストール

iPhoneにおいては、不正アプリのインストールに構成プロファイルが悪用されていると考えられます。

通信事業者を装うSMSに従ってリンク先に進むと、通信事業者を装う構成プロファイル及びセキュリティアプリをインストールするよう誘導され、画面に表示されるメッセージに従って「インストール」や「許可」を押下することで、最終的に不正アプリのインストールが完了してしまいます。

その後、インストールした不正アプリを起動するとネットワーク暗証番号の入力画面となり、入力した情報が抜き取られる恐れがあります。

図　不正アプリのインストール(iPhone)

出典：一般財団法人日本サイバー犯罪対策センター, “通信事業者を装ったフィッシング（不正アプリに注意）“,
https://www.jc3.or.jp/threats/examples/article-409.html