個人を狙ったサイバー攻撃に関する留意事項

平成 30 年８月 27 日
個人情報保護委員会事務局

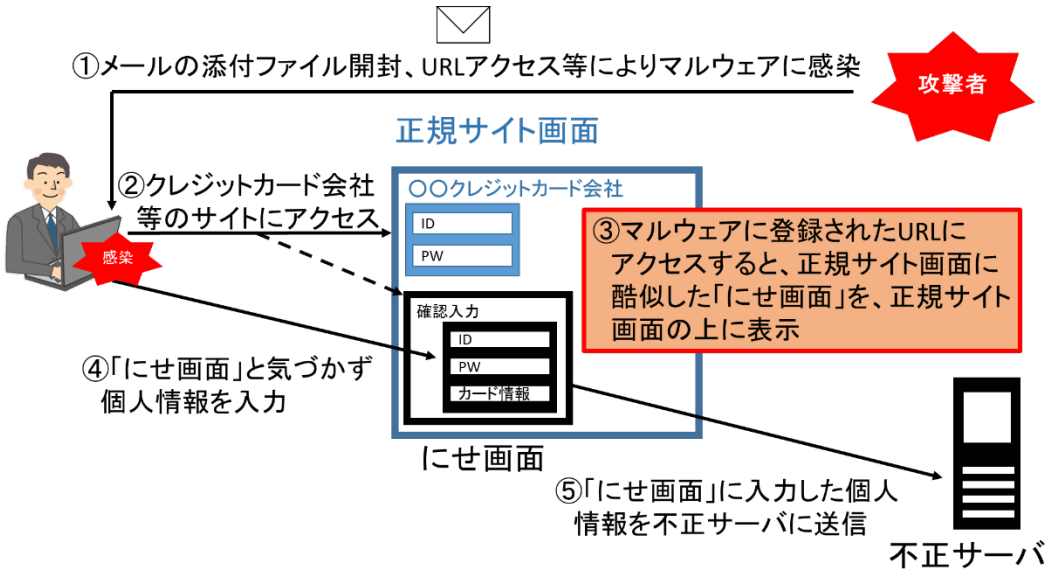
昨年５月以降、当委員会において個人情報取扱事業者からの個人データの漏えい等報告を受け付けており、委員会として、事実関係の詳細を確認の上、適切な対応を促すとともに、適切な再発防止策の策定を確認しているところです。

一方で、事業者からの漏えい以外に、サイバー攻撃等により、直接個人から個人情報を不正に取得しているケースが数多く存在しており、インターネットを利用する一人ひとりが気を付けることが必要です。特に不審なメールに添付されているファイルを開いたり、URL にアクセスしたりしないようにしましょう。

１．個人を狙ったサイバー攻撃の例

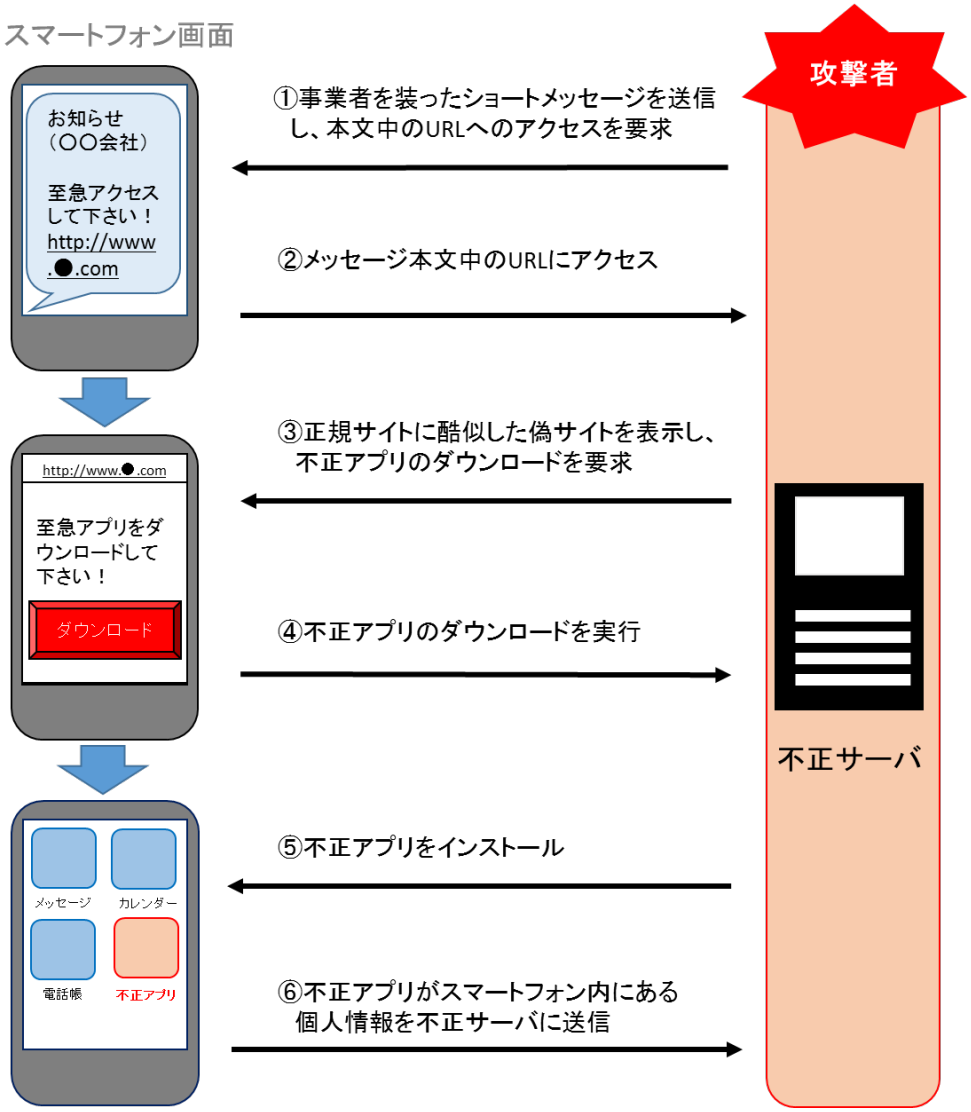
① バンキングトロージャン

いわゆるマルウェアによる攻撃のひとつで、感染すると、正規サイトにアクセスした利用者のパソコンに、「にせ画面」を表示させ、クレジットカード情報等の個人情報を収集する。元々はインターネットバンキングがターゲットにされていたが、最近ではクレジットカード会社のサイトが狙われるケースも増えている。



② スミッシング（SMS フィッシング）

事業者を装ったショートメッセージがスマートフォンに送られ、メール本文中の URL にアクセスすると、事業者の公式サイトに酷似した偽サイトが表示され、スマートフォン用アプリ（個人情報を窃取する不正アプリ）をインストールするとスマートフォンの個人情報が抜き取られる。



２．個人情報を不正に取得された場合の影響

個人情報を不正に取得されると、以下のようなさらなる被害を受ける可能性があります。

・クレジットカード情報を不正に取得された場合

クレジットカードの不正利用による金銭被害を受ける可能性があります。

・メールアドレスを不正に取得された場合
フィッシングメールやマルウェアの送信を受け、被害が拡大する可能性があります。
・ID/パスワードを不正に取得された場合
リスト型攻撃により別サイトのポイントが不正利用されたり、さらに他の個人情報を不正に取得されたりする可能性があります。

３．対策

①バンキングトロージャン（マルウェア）への対策

・不審なメールの添付ファイルを開いたり、URL のリンク先へアクセスしたりしない。
・ログインページに普段表示されないポップアップが出ても、いったん操作を止めて落ち着き、不用意に個人情報やクレジットカード情報を入力しない。
・ウィルス対策ソフトの導入やパターンファイルを更新する。
・ＯＳなどソフトウェアのパッチを速やかに適用する。

②スミッシング（フィッシング）への対策

・不審なショートメールに記載の URL にはアクセスしない。
・不審なショートメールに返信しない。
・提供元が不明なアプリをインストールしない。

※日頃からクレジットカードの利用明細を確認し、不正利用が疑われるようであれば、できるだけ早くクレジットカード会社に連絡しましょう。

４．関連リンク

〇フィッシング対策協議会ウェブページ
「消費者の皆様へ」：https://www.antiphishing.jp/consumer/
〇独立行政法人　情報処理推進機構(IPA)ウェブページ
「情報セキュリティ安心相談窓口」
：https://www.ipa.go.jp/security/anshin/index.html
〇一般財団法人　日本サイバー犯罪対策センター(JC3)ウェブページ
「情報提供」　：https://www.jc3.or.jp/info/index.html

以上