第 19-08-393 号
掲載日：2019 年 12 月 24 日
独立行政法人情報処理推進機構
セキュリティセンター

安心相談窓口だより

App Store 以外の配信アプリによるセクストーション被害を確認
～ iPhone の公式マーケット以外からのアプリインストールに注意 ～

IPA ではこれまでにセクストーション（性的脅迫）に関する相談事例の紹介や注意喚起を行ってきました(*1)。

セクストーションとは、「sex（性的な）」と「extortion（脅迫）」を組み合わせた造語で、被害者のプライベートな動画や写真を入手して、それをばらまくなどと脅して金銭などを要求する手口を意味します。

セクストーション被害の相談は、2014 年 7 月から累計で 86 件寄せられており、そのうち 2019 年は 12 月 23 日時点で 17 件です。

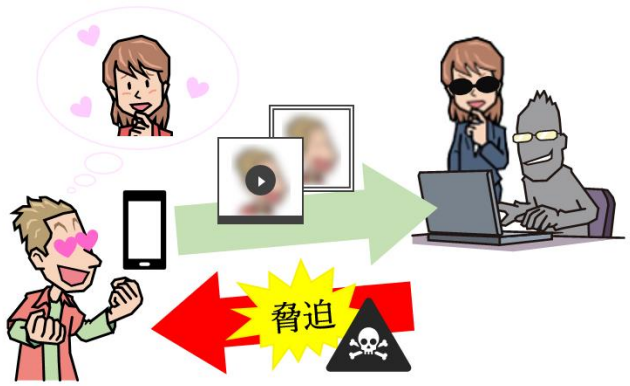

図 1:セクストーションの手口のイメージ

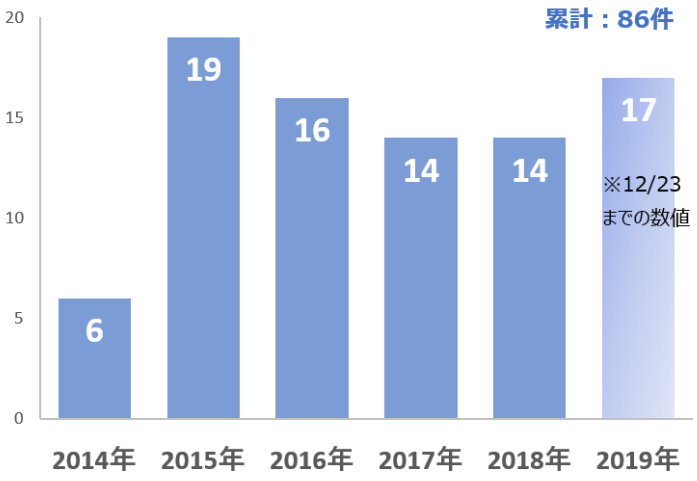

図 2:セクストーションに関する相談件数の推移(*2)

これまでに IPA に寄せられた相談事例では以下の手口がありました。

- Android 端末の利用者に対し、公式マーケット（Google Play）以外から不正アプリをインストールするよう誘導し、そのアプリで電話帳情報を窃取して、友人、知人にプライベート動画等をばらまくと脅す。

(*1) 「個人間でやりとりする写真や動画もネットに公開しているという認識を！」
https://www.ipa.go.jp/security/txt/2014/12outline.html
「iPhone ユーザを狙った不正アプリによるセクストーション被害が発生」
https://www.ipa.go.jp/security/anshin/mgdayori20161110.html
「主に中高生を対象としたセクストーション被害に関する注意喚起」
https://www.ipa.go.jp/security/anshin/mgdayori20170810.html
(*2) 集計期間：2014 年 7 月 1 日～2019 年 12 月 23 日

- iOS 端末（以下 iPhone）の利用者に対し、iPhone を脱獄(*3)させた上で公式マーケット（App Store）以外から不正アプリをインストールするよう誘導し、そのアプリで電話帳情報を窃取して、友人、知人にプライベート動画等をばらまくと脅す。
- 正規の SNS アプリのメッセージ機能を使い、インターネット上にプライベート動画等をばらまくと脅す。

2019 年 12 月には iPhone を脱獄させることなく「App Store」以外から不正アプリをインストールさせる手口が確認されました。

そこで、最近確認された手口と、被害にあわないための対策について解説します。

1. 最近確認された手口

手口は主に以下の流れでした。

（1）正規アプリでビデオ通話をする

- LINE で見知らぬ女性から突然コンタクトがある。
- 親しくなった後、ビデオ通話等でお互いの性的な姿を見せ合うことをもちかけられる。
  （その際やりとりした内容が、相手に何らかの形で録画されていると考えられる。）

⇩

（2）App Store 以外からアプリをインストールするよう誘導される

- 「LINE がつながりにくくなった」等の理由から他のアプリを紹介するとして、App Store 以外のウェブサイトの URL を案内される。
- 相手の誘導に従い、指示されたウェブサイトから不正アプリをインストールしてしまい、さらにアプリにアクセス権限を許可してしまうことにより、スマートフォンの連絡先情報を窃取される。

⇩

（3）ビデオ通話の動画を友人や知人にばらまくと脅され、金銭を要求される

- 突然 LINE で知らない男性から連絡があり、ビデオ通話の動画をスマートフォンの連絡先に登録している知人等にばらまかれたくなかったら、20 万円支払えと恐喝される。
- 証拠として録画された動画と、連絡先のデータが送られてくる。

なお、**金銭を支払った後も恐喝され続けるケースや、金銭の支払いに応じたかどうかによらず動画をばらまかれるケースも確認されています。**

2. 「App Store」以外で配信されていた不正アプリの検証結果

iPhone のアプリは、通常、開発者が Apple 公式マーケットである「App Store」に公開して配信することで、ユーザが利用できるようになります。しかし、１．の手口で使用された不正アプリは、App Store で配信されているものではありませんでした。

企業や組織で社内用アプリを配信するための仕組みである「Apple Developer Enterprise Program(*4)」を悪用して、App Store 以外のサイトでアプリを配信していると考えられます。

(*3) iOS で制限されている機能を解除するような改造行為であり Jailbreak とも呼ばれる。例えば、脱獄をすることで、公式マーケットで公開されている以外のアプリをインストールすることが可能となる。

(*4)「Apple Developer Enterprise Program」
https://developer.apple.com/jp/programs/enterprise/（外部サイトに接続します）

今回 IPA で検証した不正アプリはスマートフォン端末内の連絡先データへのアクセス権限を有していましたので、アプリをインストールして、アプリの信頼に関する設定を行ってしまうと、連絡先のデータが窃取される可能性があります。

今回確認された不正アプリのインストールの流れ(iOS 12.4.4)を下記に説明しますが、**このような操作を行って不正アプリをインストールしないようにしてください。**

図 3：「App Store」以外から不正アプリをインストールする流れ（クリックして拡大）

3. 被害に遭った場合の対処

- セクストーションの被害に遭った場合は、相手に対して連絡することは避け、警察へ相談してください。
  警察庁：都道府県警察本部のサイバー犯罪相談窓口等一覧
  https://www.npa.go.jp/cyber/soudan.htm （外部サイトに接続します）
- 不正アプリがインストールされている間は、スマートフォンは電源を切るか、機内モードにして通信を遮断してください。また、警察に相談する際は、アプリと、LINE 等のやり取りは削除せず、証拠として残しておくことお勧めします。最終的にはスマートフォンは初期化してから使用してください。
- 相手の手の内に渡った動画や連絡先の情報を、取り戻したり削除させることは極めて困難です。

4. 被害に遭わないために

■アプリのインストールは公式マーケットから

- iPhone、Android どちらの場合も、原則として公式マーケット以外からアプリのインストールを行わないでください。
- 公式マーケット以外からアプリをインストールする必要がある場合は、アプリの開発者情報など、安全性を十分に確認してください。安全性の判断が出来ない場合は、インストールは控えてください。
- 公式マーケットからアプリを入手する場合でも、アプリに対するレビュー内容や、アプリの開発者情報などを確認し、不審な点がある場合にはインストールは控えてください。
- アプリと同様に、不審な構成プロファイル(*5)をインストールしないように注意してください。

■他人に見られたら困るプライベートな写真や動画は撮ったり第三者に送ったりしない

- 他人に見られて困るような写真や動画は、セクストーションやリベンジポルノに悪用される可能性があります。
- そのため日頃から、その様な写真や動画はそもそも撮影したり、他人と共有を行わないことが賢明です。

更新履歴

2019 年 12 月 24 日　掲載

本件に関するお問い合わせ先

情報セキュリティ安心相談窓口
Tel: 03-5978-7509　Fax: 03-5978-7518
E-mail: anshin@ipa.go.jp
セキュリティセンター　中島／加賀谷

(*5) 不審な構成プロファイルをインストールした場合、「端末内の設定が変更される」、「端末の固有情報が外部に送信される」といった可能性が考えられます。