

今月の呼びかけ

「クラウドサービスからの情報漏えいに注意！」
～ スマートフォンで撮影した写真の保存先と公開範囲を意識していますか？ ～

2014 年 9 月、米国人気女優やモデルなど著名人のプライベート画像が多数流出したことが話題になりました。報道および Apple 社の調査^{*1}によると、iCloud^{*2}のアカウントが乗っ取られてしまったことで iCloud から多数の画像が流出したとされています。

手口の詳細は明らかになっていませんが、被害者が iPhone で撮影した写真データが iCloud に保存されていて、何らかの手段で被害者の iCloud のアカウント情報（Apple ID とパスワード）を入手した悪意ある第三者が iCloud に不正ログインし、iCloud に保存されていた写真データを窃取したと考えられます。

このような被害が発生するリスクは Apple 社のサービスに限ったことではなく、クラウドサービス全体に言えることです。

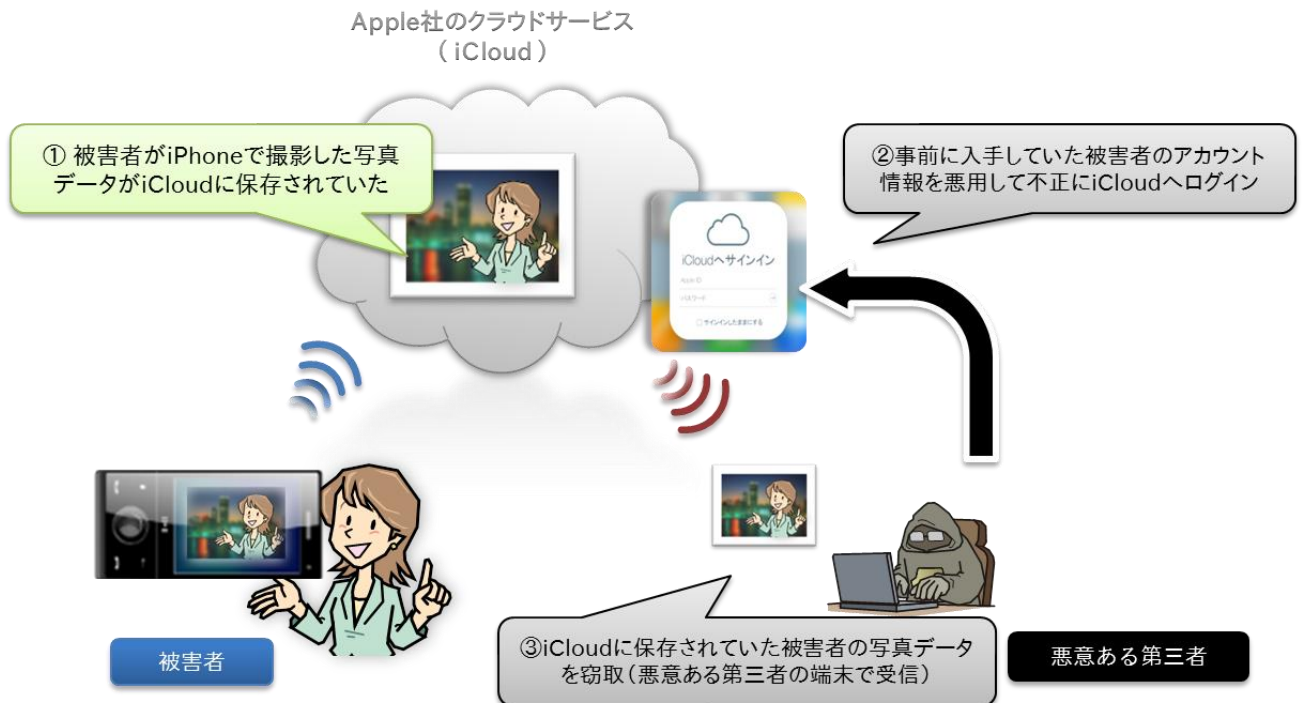


図 1 : iCloud から画像が流出した事件の概要

¹ Apple 社 : Apple Press Info 「著名人の写真に関する調査状況の報告」
<https://www.apple.com/jp/pr/library/2014/09/02Apple-Media-Advisory.html>

² iCloud: iCloud とは
http://support.apple.com/kb/PH2608?viewlocale=ja_JP

今月の呼びかけでは、前述の事件を踏まえ iCloud を例としてクラウドサービスを利用する上での留意点やアカウント管理のポイントを紹介します。

(1) クラウドサービスの概要

クラウドサービスはインターネットを通じてデータ保管やソフトウェア利用を提供するサービスの総称です。インターネットに接続できる環境を持つどの端末からも、同様のサービスを利用できることが特徴です。

図2は、Apple社が提供する iCloud というクラウドサービスにおける「自分のフォトストリーム^{※3}」という機能を利用した、複数の端末間での写真データ同期のイメージです。iCloud の「自分のフォトストリーム」を有効にすると、1 台の端末で撮った写真が、自動的に iCloud にアップロードされます。これにより自分が所有する複数の端末間で写真データが同期され、閲覧することができます。



図2: 「自分のフォトストリーム」による写真データ同期のイメージ図

iCloud を利用すると写真以外にも、メール、連絡先、カレンダー等、普段は iPhone から確認、操作している情報を、他の場所にある iPad やパソコンから確認したり、操作したりすることができます。

³ iCloud: 「自分のフォトストリーム」に関してよくお問い合わせいただく質問 (FAQ)
http://support.apple.com/kb/HT4486?viewlocale=ja_JP

(2) クラウドサービスのリスク

もし iCloud のアカウント情報が何らかの方法で悪意ある第三者の手に渡ってしまった場合、iPhone や iPad で撮影した写真や、iCloud から確認できるメール、連絡先、カレンダー等の情報が窃取され、漏えいしてしまうというリスクがあります。

例えば、あるユーザーの iCloud のアカウント情報が悪意ある第三者の手に渡ってしまい、そのユーザーが「自分のフォトストリーム」を有効にしていた場合、以下のような流れで写真データが漏えいし、冒頭のプライベート画像流出のような事件に発展する可能性があります。

- ① 「自分のフォトストリーム」を有効（図3）にしていると、ユーザーが iPhone で撮影した写真は、自動的に iCloud にアップロードされる。
- ② 悪意ある第三者は iCloud が利用できる端末から、ユーザーのアカウント情報を悪用して iCloud に不正ログインする。
- ③ iCloud に保存されているユーザーの写真データが悪意ある第三者の端末にダウンロードされる。
- ④ 入手したユーザーの写真データを、悪意ある第三者がインターネット上に流出させる。



図3：iPhoneでの「自分のフォトストリーム」の設定を変更する画面^{*4}

他にも iCloud に不正ログインされると、iCloud Drive^{*5}に保存されているファイル等が漏えいしてしまうことも考えられます。また、iCloud バックアップを利用している場合は、自動的にバックアップされたデータが悪意ある第三者の iPhone に復元されると、様々な情報の漏えいにつながる可能性があります。

⁴ iPhone 5、iOS 8.0.2 での画面

⁵ Apple 社の提供するクラウドストレージサービス。iCloud 上に様々なファイルを保存することができる。

(3) クラウドサービスを利用する際の注意点

iCloudに限らず、どこからでもアクセスできるという機能は、他の一般的なクラウドサービスでも共通のことで、便利な一方、リスクでもあります。

データをパソコン上にだけ保管している場合は、パソコンさえしっかり守っていれば情報漏えいの被害に遭いません。一方、クラウドサービスを利用してデータを同期している場合は、もし悪意ある第三者に ID とパスワードを知られてしまうと、クラウドサービスに不正ログインされてしまい、情報漏えいの被害に遭う可能性があります（図4）。

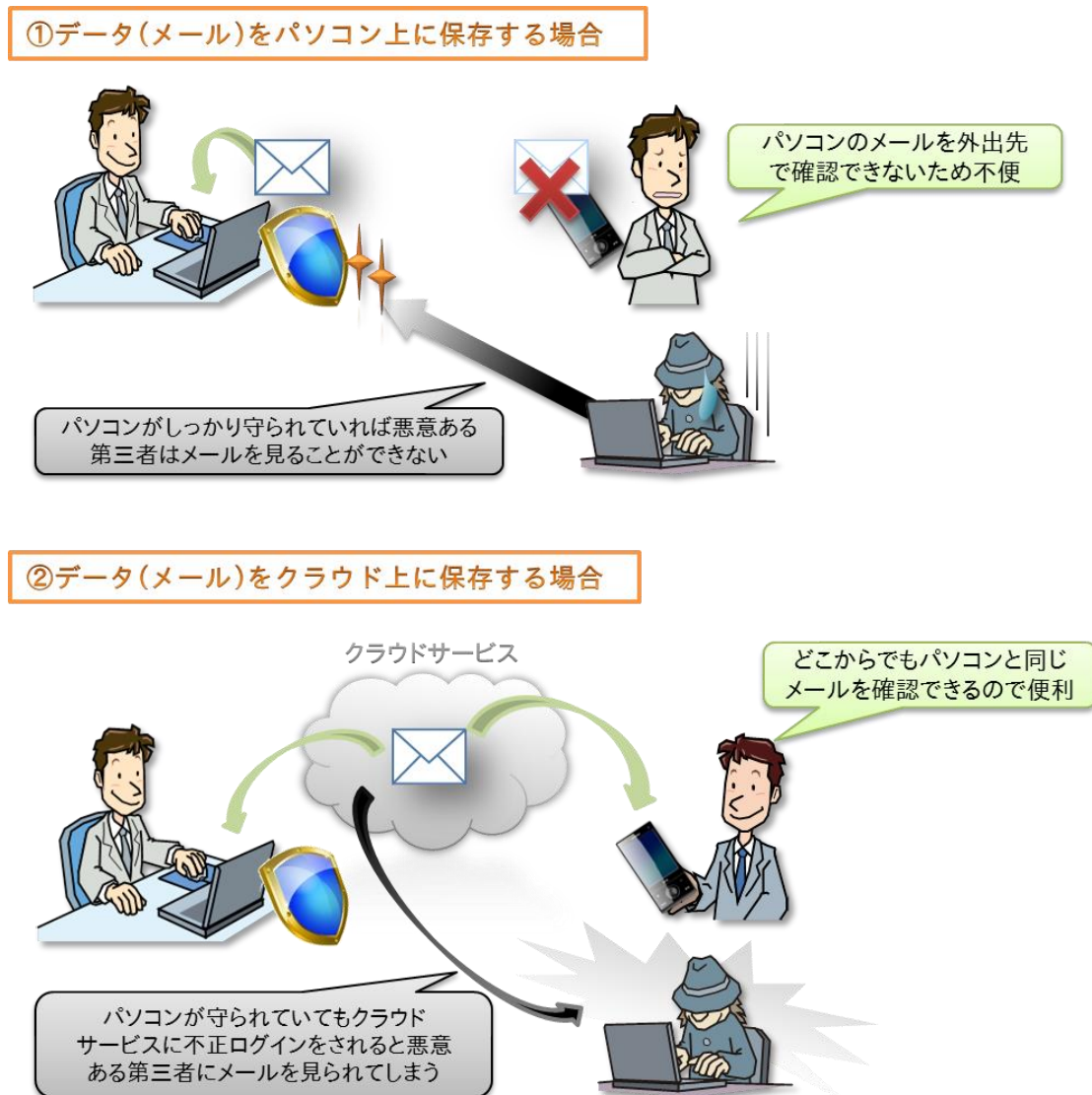


図4：データをパソコンに保存する場合とクラウドに保存する場合の利便性とリスク

そのため、他のインターネットサービスと同様に、クラウドサービスの利用においても、ID とパスワードを適切に管理することが重要です。加えて必要のないデータは共有しないことが賢明です。

■クラウドサービスを利用する際の注意点

【1】不正ログインされないようにする。

以下のような対策を取っておくことで、自分が利用しているクラウドサービスが悪意ある第三者に不正ログインされる危険性を低減させることができます。

- ・安易に推測できるパスワードを使用しない。
- ・パスワードを使い回さない。
- ・IDとパスワードの入力は、確実に本物と判断できるサイト上でのみ行う（フィッシング対策）。
- ・セキュリティオプション（ログイン通知、二段階認証など）が提供されている場合は積極的に採用する。

繰り返しとなりますが、「自分のフォトストリーム」を有効にしていると、iPhoneで撮影した写真はすべて自動的に iCloud に保存され、他の端末と同期されます。もし、悪意ある第三者に不正ログインされると、自分の知らない間にデータを閲覧されたり、窃取されたりする危険性があります。

【2】クラウドサービスを理解した上で利用する。

利用するクラウドサービスの特性を理解して、使用の判断を慎重に行ってください。クラウドにアップロードする対象を必要のあるものだけに限定することで、もしクラウドサービスが悪意ある第三者に不正ログインされても、漏えいする情報を最小限に抑えることができます。

例えば、前述の「自分のフォトストリーム」で、写真データの同期が不要な場合は設定を確認し、無効にしておく安全です。また、写真以外にも、メール、連絡先、カレンダーなどの共有についても個別に判断し、適切な設定を行ってください。

その他、iPhoneで「写真の共有」設定を有効にしていると、複数ユーザー間で写真を共有できます。これは事前に他のユーザーを招待したり、他のユーザーからの招待を受けたりして、限られたユーザー間で写真を共有するクラウドサービスです。iPhoneで共有したい写真を選択すると、その写真を他のユーザーと共有することができます（図5）。

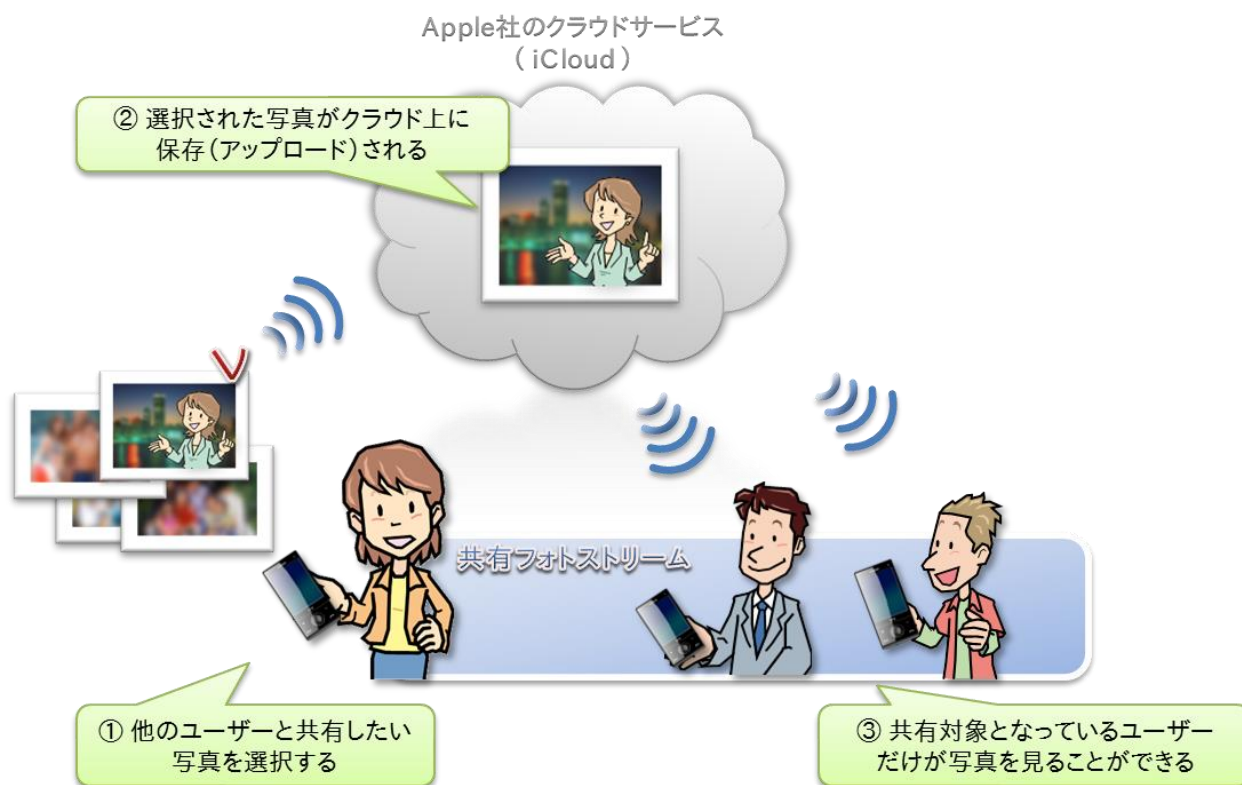


図5：「写真の共有」設定を有効にした場合の情報共有のイメージ図

このように、同じ写真に関するクラウドサービスでも公開対象や公開範囲などに違いがあります。そのため、クラウドサービスのそれぞれの特性を理解せずに利用していると、冒頭のプライベート画像流出のような思わぬトラブルにいつの間にか巻き込まれてしまう恐れがあります。

クラウドサービス利用時には、適切なアカウント管理とそのサービスの特性を理解した上で、利用の判断を慎重に行ってください。

※本紙に記載の製品名、サービス名等は、各社の商標もしくは登録商標です。

■お問い合わせ先

IPA 技術本部セキュリティセンター 加賀谷／野澤

Tel: 03-5978-7591 Fax: 03-5978-7518

E-mail: isec-info@ipa.go.jp