OUCH! | 2016 年 12 月

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- はじめに
- 個人の情報
- データの完全消去
- SIM / 外部の記憶媒体

モバイルデバイスを安全に破棄する

はじめに

スマートフォン、スマートウォッチやタブレットなどのモバイルデバイスは、とてつもない早さで進化を遂げています。そのため、一年おきにデバイスを交換する人もいます。しかし、残念ながら多くの人がデバイスに保存されている多くの個人情報を考慮せずにデバイスを破棄しています。このニュースレターでは、モバイルデバイスに保存されている個人情報の種類について解説し、これらを完全削除した上でデバイスの破棄または返却を行う方法も解説します。利用しているモバイルデバイスが会社によって支給されたもので、会社のデータが保存されている場合は、適切なバックアップと破棄の手順に関して一度上司と相談を行った上で、以下の手順に従うようにしてください。

ゲストエディター

ヘザー・マハリク氏 (@HeatherMahalik; +HMahalik) は、ManTech CARD社においてフォレンジックに関する取り組みを主導する調査官です。彼女は、SANS Institute の Advanced Smartphone Forensics (FOR585) の共著者、主任講師であり、またWindows Forensic Analysis (FOR408) の講師でもあります。smartforensics.com にてブログを使い、情報発信を行っています。

個人の情報

モバイルデバイスは、想像以上に機密データを保存しており、多くの場合はパソコンよりも多いです。その情報の中に含まれるものとして：

- 住まい、会社、頻繁に訪れる場所の情報
- 電話帳やアプリケーションに保存されている、家族、友人や同僚などの連絡先
- 発信、着信、不在着信を含む通話の履歴
- SMS、ボイスやその他のマルチメディアメッセージ
- チャット用アプリやゲーム、ソーシャルメディア内のチャット履歴
- GPSによる位置や携帯基地局の履歴から得られる位置の履歴
- ウェブブラウジングや検索の履歴、Cookieとキャッシュされたページ
- 個人の画像、ビデオ、音声録音や電子メール
- 保存されたパスワードによる個人アカウントへのアクセス。例えば、オンラインバンキングや電子メール
- クラウドに保存されている画像、ファイルや情報へのアクセス
- 健康に関する情報。例えば、年齢、心拍数、血圧や食事の履歴

データの完全消去

上記で解説したようにモバイルデバイスには多くの機微な情報が保存されている可能性があります。モバイルデバイス

モバイルデバイスを安全に破棄する

を寄付する、新しいのと交換する、家族に譲渡する、売るまたは単純に破棄するなど、破棄の手法に関わらず、最初に保存されているすべての機密情報を完全削除する必要があります。気付かないかもしれませんが、単純に削除しただけでは足りません。なぜなら、これらの情報はインターネット上にある無料のツールを使って復旧できてしまうからです。そのため、すべてのデータを安全に消去する必要があります。これを完全消去と呼びます。ここでは、データを上書きすることで、リカバリできない状態にします。データを完全消去する前にバックアップを取ってください。このバックアップを使って新しいデバイスへの移行が楽になります。

モバイルデバイスを破棄する際は、出荷状態に戻し、SIMカードとSDカードを外してください。

デバイスのデータを安全に完全消去する一番簡単な方法は、「出荷状態に戻す」機能を利用することです。これを利用することで、デバイスを最初に購入した状態に戻します。モバイルデバイスからデータを完全消去するために使える一番簡単で安全な方法であることが我々の調査の中で判明しています。この機能は、デバイスによって提供方法が異なります。以下に2つのメジャーなデバイスについて記載します：

- Apple iOS：設定｜一般｜リセット｜すべてのコンテンツと設定を消去
- Android：設定｜バックアップとリセット｜データの初期化

残念ながら Windows Phoneデバイスから個人データを完全削除するためには出荷状態に戻すだけでは足りません。現在、これらのデバイスから個人情報をすべて完全削除する手法について研究が行われています。デバイスを出荷状態に戻す上で、不明な点が残っている場合は、マニュアルやメーカーのウェブサイトを確認してみてください。絶対に覚えておかなければならないのは、容易にリカバリできてしまうため、個人情報を削除するだけでは足りない、ということです。

SIM & External Cards

デバイスに保存されているデータと同時に SIM (加入者識別モジュール)カードをどうするかを考えなければなりません。SIMカードは、モバイルデバイスのユーザがセル方式またはデータ通信を行うために使われます。デバイスを出荷状態に戻しても、SIMカードには、ユーザである自分のアカウント情報を保持したままの状態で残ります。新しいデバイスで同じ電話番号を引き続き利用する場合は、携帯プロバイダに相談し、SIMカードの移行をしてください。新しいデバイスが、別の大きさのSIMカードを利用するなど、SIMカードが移行できない場合は、古いSIMカードを引き取り、シュレッダーをかけるなど、他人によって再利用されないように物理的に破壊してください。

モバイルデバイスを安全に破棄する

モバイルデバイスには、追加ストレージのためにSDカードを利用するものもあります。多くの場合、これらの追加ストレージには、画像、スマートフォンアプリや他の機微なコンテンツが保存されています。デバイスを破棄する前に外部の記憶媒体を外すことを忘れないで下さい。(デバイスによっては、SDカードがバッテリパックの側、または下に隠されている場合があります) これらのカードは、新しいモバイルデバイスでの再利用が可能なほか、USBアダプタを使って、パソコン用の保存領域としての利用も可能です。SDカードの再利用ができない場合は、古いSIMカードと同じく物理的に破壊することをお勧めします。

このニュースレターに記載されていることで不明点がありましたら、モバイルデバイスを購入したお店に行って、技術者による手助けをもとめてください。最後にモバイルデバイスを単純に破棄することを考えている場合は、寄付することも一度考えてください。このようなモバイルデバイスを寄付として受け入れる組織は多くあります。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI　セキュアテクノロジーズは、国内最大の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。 http://www.nri-secure.co.jp

リソース

タブレットを安全に使用するには:	https://securingthehuman.sans.org/ouch/2016#january2016
バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015
Advanced Smartphone Forensics Course:	https://sans.org/for585
OUCH ニュースレターのアーカイブ:	https://securingthehuman.sans.org/ouch/archives

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Translated By: 内山　貴之, 時田　剛