SANS SECURING THE HUMAN
NRI SECURE TECHNOLOGIES

OUCH! | 2014 年 8 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...

- 暗号とは？
- 保存データの暗号化
- 通信データの暗号化

暗号化機能について

暗号とは？

個人情報を守るために、職場の同僚や友人から「暗号化」した方がいいと勧められたことがあるでしょう。しかし、暗号と聞くと非常に難解そうに感じるでしょう。しかも、暗号で全てが守られるわけではなく、暗号でも守れないものが存在します。今月号では、なるべく平易な言葉を使って、暗号の必要性と正しい使い方について説明してみたいと思います。

ゲストエディター

クリストファー・クロウレイ（@CCrowMontance、+ChrisCrowley）は、ワシントンDC在住のコンサルタントです。同氏はSANSのMobile Device Security and Ethical Hacking （SEC575）コースの主任インストラクターであり、Incident Response Team Management (MGT535) のコース作成者でもあります。

みなさんが利用しているデバイスには、多種多様な情報が保存されています。例えば、銀行口座やクレジットカードの明細書、デジタル写真、メールのほか医療データなどがあると思います。もしデバイスの紛失あるいは盗難のような事件が起こったら、デバイスだけではなく、そこに保存されているデータも第三者の手にわたってしまう可能性があります。また、そのデバイスでオンラインバンキングやオンラインショッピングなどをしていたのだとしたら、クレジットカード番号や銀行の口座番号などのデータを盗まれてしまう可能性もあります。このような場合、重要なデータが暗号化されていると、第三者による不正アクセスや改ざんから守ることができます。

暗号化されていない情報は、平文と呼ばれます。平文の情報は、アクセスさえ出来てしまえば誰にでも見ることができます。暗号化とは平文の情報を判別不可能な形式、つまり暗号文に変換することです。そして暗号化された情報は「鍵」をかけて保護されます。これは、玄関のドアに鍵をかけるのと同じ考え方です。暗号の「鍵」として最も一般的に利用されているのはパスワードです。つまり、パスワードを知っている人のみが暗号文を復号して情報を読むことができます。そのため、暗号化された情報を守るには、鍵を守る必要があります。暗号をかける対象を大きく分けると2つあります。一つはパソコンなどに保存されているデータに対して、もう一つは、オンライン上で通信中のデータに対してです。

保存データの暗号

保存されているデータに暗号をかける目的は、コンピュータやモバイルデバイスに紛失や盗難が起こった場合、デバイスに保存されたデータを第三者に見られないようにするためです。15年前であれば、紛失や盗難の心配をすることもなかったでしょう。当時のコンピュータは非常に大きく、容易に運ぶことができませんでしたから。しかし、現在のノート型パソコンは1～2キロと軽量であり、モバイルデバイスに至っては数百グラムになっています。これらは非常に高性能で、大量の情報を保存することができますが、軽量でかつ小型化しているので紛失しやすい

暗号化機能について

という課題があります。他にも、USBドライブやCD-ROMなどの可搬記録媒体に多くの機微情報が含まれていることがあります。このようなデバイスやメディアに保存されている情報に暗号をかけるには、フルディスク暗号と呼ばれる方法が利用されます。この方法の利点は、デバイスやメディア上の情報全てを暗号するため、暗号化するデータを選択する必要がないことです。多くのOSではフルディスク暗号機能が実装されており、その機能を有効にするだけでフルディスク暗号を利用することができます。もし、お使いのコンピュータでフルディスク暗号機能が利用できる場合には、有効することを推奨します。また、携帯電話でもストレージデバイス部分はフルディスク暗号機能をサポートしています。例えば、iPhoneのiOSでは、フルディスク暗号が可能ですので、勤務先のヘルプデスクや上司に確認してみてください。私用のコンピュータの場合には、メーカーに問い合わたり、メーカのホームページなどでサポート文書を参照してください。

暗号化機能を利用することにより、大事な情報を守ることができますが、鍵の強度に依存することを忘れないでください。

通信データの暗号

情報は、通信中も盗聴や改ざんなどの危険性があります。通信データが暗号化されていない場合、通信データの中身を確認され第三者に取得される可能性があります。このような理由から機密情報の送受信を行うようなオンラインバンキング、メールの送受信、およびソーシャルメディアにアクセスする際は、通信のデータを暗号化することが重要です。ところで、通信データの暗号方法としては、HTTPSと呼ばれる方法が頻繁に利用されます。HTTPSは、ブラウザとWebサイトの間の通信を暗号化します。HTTPS通信であることをブラウザ上で確認するには、複数の方法があります。①URLの先頭がhttps://から始まっている、②ブラウザのURLバーが緑になっている、または③錠前のアイコンがブラウザのウィンドウ内に表示されているなどです。これらはいずれも、通信データが暗号されていることを表示しています。その他にも、公共のWi-Fiネットワークに接続する場合にはできる限り暗号化機能を利用してください。同様にして、メールの送受信する場合にも暗号化機能をできるだけ利用してください。多くのメールクライアントでは暗号化機能が利用できるようになっています。さらにISPによってはメールクライアントの暗号化機能を有効にするオプションを提供しているほか、メールクライアント自身でも暗号化機能を備えている場合があります。

正しい暗号化機能の使い方

暗号化には、以下のような共通点があります。

- 暗号の強度は、鍵の強度に依存します。鍵が第三者に渡ってしまえば、データにも第三者はアクセスできますので、鍵は安全に保管してください。

暗号化機能について

- 鍵にパスワードやパスコードを利用している場合は、強度のある長くて安全なパスワードを使い、決して忘れないようにしてください。もしこれらのパスワードやパスコードを忘れると、自身のデータにアクセスできなくなってしまいます。
- 暗号の強度は、コンピュータのセキュリティ強度に依存します。万一コンピュータがサイバー攻撃の被害にあったり、またはウイルスに感染した場合には、攻撃者は暗号化機能を回避できる場合があります。このような自体を招かないためにも、コンピュータやモバイルデバイスは安全な状態にしてください。
- 暗号化機能を選択できる場合には、常に強度の高い方法を選んでください。

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。

http://www.securingthehuman.org

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

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
iOSの暗号機能:	http://support.apple.com/kb/ht4175
Androidの暗号機能:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windowsの暗号機能:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
コンピュータの堅牢化:	http://www.securingthehuman.org/ouch/2012#december2012
パスワードマネージャー:	http://www.securingthehuman.org/ouch/2013#october2013

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 坂 恵理子, 関取 嘉浩

