OUCH! | 2016 年 06 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？
- 何が暗号化できるか？
- 暗号を正しく利用する

暗号について

暗号とは？

会話の中で「暗号」という言葉を聞き、暗号を使って自分や自分に関する情報を守る方法を聞くことがあるかもしれません。ただ、暗号はとても複雑で分かりづらいものです。また、暗号の限界を知る必要があります。このニュースレターでは、分かりやすい言葉で暗号を説明するとともに、暗号によって自分がどうやって守られるか、そして正しく活用するための手順を紹介します。

ゲストエディター

フランチェスカ・ボスコ氏（@francibosco）は、研究者でもありながらプロジェクトマネジャーとして、サイバー犯罪、サイバーセキュリティそしてテクノロジーの誤使用に関するプロジェクトを管理しています。国連地域間犯罪司法研究所で勤務しており、Tech and Law Centerの共同創立者でもあります。

利用しているデバイスには、個人用の文書、写真、メールなど多くの機密情報が保持されています。そのため、デバイスを紛失、または盗難されたりしてしまった場合は、これらの情報はデバイスを保持している人によってアクセス可能になってしまいます。また、オンライン上で、買い物や銀行取引など重要な取引をすることもあるでしょう。これらの取引を監視している人がいれば、口座情報やクレジットカード番号などの個人情報を盗まれる可能性もあります。暗号化を使うことで、このような時に不正な第三者が情報にアクセスしたり、変更したりできないように自分を守ってくれます。

暗号は数千年前から活用されています。現代の暗号は、過去のものよりはるかに複雑ですが、まったく変わらない目的で利用されています。それは、正規の人のみが解読可能な状態で秘密のメッセージを別の人に送り届けることです。文章などの情報が暗号化されていない状態は、平文と呼ばれます。この場合は、誰もが読むことができ、情報にもアクセスが可能です。暗号を使うことで、この情報を通常では読めない、アクセスできない、暗号文に変換します。現代の暗号は、複雑な数式と一意の鍵を使って、平文を暗号文に変換します。この鍵が、情報に対するアクセスおよび読めるようにするために使われます。多くの場合において、パスワードまたはパスフレーズが鍵として使用されます。

何が暗号化できるか？

通常、2種類のデータを暗号化できます。一つ目は静止状態のデータ（例えば、モバイル機器に保存されているデータ）です。もう一つは、動いているデータ（例えば、受信するメールや友人とのチャット）です。

静止状態のデータを暗号で保護することは、デバイスを紛失したり、盗まれたりした時にとても重要です。現代のデバイスはとても性能が高く、多大な情報を保持している反面、容易に失くしてしまうほどコンパクトになっています。また、USBドライブや外付けのハードディスクなど、他のモバイルメディアも機密情報を保持しています。このよう

暗号について

なデバイスに対しては、フルディスク暗号化（FDE）と呼ばれる暗号化の手法が広く使われており、システム内のディスク上にあるすべてのデータを暗号化します。これにより、システム上のデータはすべて自動的に暗号化されるため、暗号化するデータを選択する必要がありません。今、販売されているほとんどのパソコンにはFDEが搭載されていますが、手動で有効にする必要があるかもしれません。Macのコンピュータでは、FileVaultと呼ばれており、Windowsのコンピュータではバージョンにより名称が異なりますが、BitLockerまたはDevice Encryptionが利用可能です。多くのモバイルデバイスもFDEを搭載しています。iPhoneおよびiPadで使われるiOSはパスコード設定時にFDEが自動的に有効化されます。Android　は、Googleが6.0（Marshmallow）から特定の条件を満たしているハードウエアの場合、FDEをデフォルトで有効にするようになりました。

暗号は情報を保護するためのとても強力な手法ですが、鍵の強度に依存しています。

情報は通信中も狙われます。この際、データが暗号化されていなかったら、監視されたり、改ざんされたり、傍受されたりする可能性があります。そのため、オンライン上での取引に関する情報や通信を暗号化する必要があります。通信の中で一般的に利用される暗号化は、HTTPSと呼ばれています。これを使うことで、ブラウザとウェブサイト間の通信はすべて暗号化されます。HTTPSで通信しているかを確認する方法には、URLの中でhttps://と記載されているか、ブラウザに錠前のアイコンがあるか、あるいはURLのバーが緑に変わっているかを確認する方法があります。二つ目の例として、メールを送受信する際にもデータが狙われます。多くのメールクライアントは暗号をサポートしており、手動で有効にする必要があるものもあります。通信中のデータを暗号化する三つ目の例として、二人のユーザが iMessage、Wickr、Signal、WhatsAppまたはTelegramなどを使ってチャットしている場合です。これらのアプリは、エンドポイント同士で暗号をしており、機デバイス間で通信されるデータを第三者によるアクセスから守っています。これにより、通信中の相手のみが送った情報を読める、ということになります。

暗号を正しく利用する

暗号を利用している際に、適切に保護されていることを確かにするため、暗号を正しく利用することが何よりも重要です。

- 暗号の強さは、使われる鍵の強度と同じです。第三者によって鍵を推測されたり入手されたりした場合、自分のデータに誰でもアクセス可能になってしまいます。鍵はしっかりと保護してください。例えば、パスワードまたはパスフレーズを鍵としている場合、強度がある一意のものを使用してください。パスワードが長ければ長いほど、攻撃者による推測、ブルートフォース攻撃が難しくなります。また、パスワードは忘れないでください。忘

暗号について

れてしまうと、情報を復号できなくなってしまいます。すべてのパスワードを記憶できない場合は、パスワードマネージャの活用をお勧めします。

- 暗号の強さは、使用しているデバイスのセキュリティの強度とも関連しています。デバイスが過去に情報を漏えいしてしまったり、マルウエアに感染してしまったりしている場合、サイバー攻撃者は暗号を迂回することができます。そのため、デバイスをセキュアにするための手順も行う必要があります。例えば、アンチウイルスソフトウエアのインストールや強いパスワードの設定、そしてデバイスを常に最新の状態に保つ、などが挙げられます。
- 多くのモバイルアプリやパソコン用のアプリケーションはデータや通信を守るために強い暗号を提供しています。利用または購入を検討しているアプリケーションが暗号をサポートしていない場合は、他の選択肢を検討してください。

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。
securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳ー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

暗号の解説:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
パスフレーズについて:	https://securingthehuman.sans.org/ouch/2015#april2015
パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2015#october2015
マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
タブレットを安全に使用するには:	https://securingthehuman.sans.org/ouch/2016#january2016

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