パスワードとその管理を容易なものにする

はじめに

よくパスワードは、自身のアカウントを保護する上で重要なものだと聞かされます（これは事実です）が、全てのパスワードを安全に作成し管理する簡単な方法を教わることは滅多にありません。以下にパスワードを容易なものにし、アカウントのアクセス制限を行い、あなたの将来を守るための簡単な方法を示します。

パスフレーズ

常軌を逸した、複雑なパスワードの時代は今日で終わりにしましょう。そのようなパスワードは覚えることが難しいだけでなく、入力が面倒な上、昨今の処理能力が高いコンピュータを使用すると、攻撃者によって簡単に特定されてしまう可能性があります。パスワードを設定する際に大事なことは、パスワードを長くすることと、文字が多ければ多いほど強力になるということです。そのようなパスワードはパスフレーズと呼ばれており、短い文や無作為に選んだ複数の単語から成る強力なパスワードの一つです。次に2つの例を示します。

TIME FOR STRONG COFFEE!（ストロングコーヒーの時間）
LOST-SNAIL-CRAWL-BEACH（迷子のカタツムリが這うビーチ）

これらは、どちらも20文字以上で覚えやすく入力も簡単ですが、特定されにくい強力なパスワードです。パスワードに符号や数字、大文字を使用するよう求めるウェブサイトや状況に出くわす機会があると思います。これは正しいことですが、最も重要なことはパスワードの長さであることを覚えておいてください。

パスワードマネージャ

アカウント一つ一つに、個別のユニークなパスワードを設定する必要があります。複数のアカウントで同じパスワードを使用している場合、あなたは自分自身を大きな危険に晒してしまっています。全ての攻撃者が共通して行っていることは、あなたが使用しているウェブサイトをハッキングし、あなたのものを含む全てのパスワードを盗み、盗んだパスワードを用い、あなたが持つ全てのアカウントであなたに成りすましてログインすることです。このようなことは、想像以上に頻繁に発生しています。信じられないという方は、こちらのウェブサイト（www.haveibeenpwned.com）で、これまでにハッキング攻撃を受け、パスワードが窃取された可能性のあるウェブサイトのうち、あなたが使用しているものを確認してみてください。では、対策をするためにはどうすれば良いのでしょうか。パスワードマネージャを使用しましょう。

パスワードマネージャは、全てのパスワードを暗号化された場所に安全に保存できる特別なプログラムです。覚える必要があるものは、パスワードマネージャのパスワードのみです。パスワードマネージャは、必要な時に自動で適切なパスワードを取り出し、ウェブサイトへのログインを実行してくれます。また秘密の質問への答えの保存や、パスワードを使い回している場合の指摘、確実に強力なパスワードを使用するためのパスワード生成など、他にも様々な機能を備えています。さらにほとんどのパスワードマネージャは、ほぼ全てのコンピュータやデバイス間で安全な同期が可能なため、どのようなシステムを使用しているかに関わらず、常に全てのパスワードへ簡単かつ安全にアクセスできます。

最後に、パスワードマネージャ用のパスワードをメモしておき、そのメモを必ず自宅の安全な場所で保管しましょう。パスワードマネージャの中には、パスワードマネージャ用のパスワードを印刷できる機能を持つものがあります。印刷しておくことで、パスワードを忘れたとしてもバックアップを保持できます。もしくは、病気の時や緊急時に、配偶者や信頼できる家族の誰かが、あなたに代わってパスワードマネージャ内の情報を復旧させることが可能です。

二段階認証

二段階認証（または二要素認証、多要素認証とも呼ばれます）を使用することで、セキュリティがより強固なものとなります。二段階認証では、アカウントにログインする際にパスワードと、スマートフォンで生成される、もしくは携帯電話に送信されるコードの2つが要求されます。この方法により、サイバー攻撃者があなたのパスワードを入手したとしても、それだけではあなたのアカウントにログインできないようになります。二段階認証は設定が容易で、作業が必要となるのは新しいコンピュータや機器から初めてログインする際の一度だけです。できる限り、特に銀行や年金、退職金口座、メールといった重要なアカウントについては、二段階認証を有効化しておきましょう。パスワードマネージャを使用している場合、強力なパスフレーズと二段階認証の両方を使用することを強くお勧めします。

くだらない話に聞こえるかもしれませんが、これら3つの簡単な方法はあなたの仕事や名声、将来の財産を守る上で長く役に立つものです。

ゲストエディタ

ジャスティン・ヘンダーソン氏（@SecurityMapper）は、H & A Security Solutions社の共同設立者であり、SANS Instituteにおいて講師を務めています。またSANS Cyber DefenseのSIEMに関するコースの著者でもあります。ヘンダーソン氏はサイバーディフェンスに関すること全てに関心を持っており、15年に渡りコンサルティング業に従事しています。

リソース

Have I Been Pwned:	https://haveibeenpwned.com/
二段階認証に関するウェブサイト:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
ポスター「You Are a Target」:	https://www.sans.org/u/OGi

 Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛