SANS SECURITY AWARENESS
NRI SECURE TECHNOLOGIES
OUCH! | 2017 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...

- パスワード
- 2要素認証とは
- 仕組み

ログイン情報を保護する

はじめに

認証というプロセス（自分の身元を証明する行為）は、メールやソーシャルメディア、オンラインバンキングのアカウント情報などを保護するために重要です。気付いていない人もいるかもしれませんが、自分の身元を証明する方法は3つあります：パスワードなどの知っている情報 (知識情報)、運転免許証などの持っている情報 (所持情報) そして指紋などの自分固有の情報 (生体情報) があります。それぞれに長所や短所があります。一般的に使用される認証方法は、知識情報またはパスワードを利用する方法です。しかし、パスワードのみでは年々安全性が低くなっていることが指摘されています。本ニュースレターでは、パスワード以外のものを使ってアカウントのログイン情報を保護するための手法を解説します。2要素認証と呼ばれる手法です。

ゲストエディタ
ティファニー・ショーニケ氏は、National Cyber Security Alliance (@staysafeonline) において、キャンペーンなどのディレクターを勤めています。彼女は、ホワイトハウスや政府機関、民間企業と協力して、2要素認証を普及させるSTOP. THINK. CONNECT.（立ち止まる、考える、楽しむ）の取り組みとして、Lock Down You Login を立ち上げました。

パスワードだけでは不十分

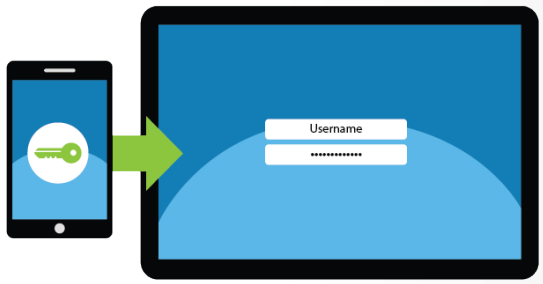
パスワードは、知識情報を使って自分の身元を証明する手法です。しかし、誰かにパスワードを推測または窃取されたりすることで、自分になりすまされ、全ての情報にアクセスされる可能性があります。アカウントがハッキングされる要因として一番多いのは、パスワードの漏えいです。このため、推測されにくいパスフレーズやアカウントごとに異なるパスワードの利用、パスワードを他人と共有しないことを教わります。このアドバイスは、妥当ですが、十分ではありません。幸いなことに、自分の情報を保護するための簡単な手法があり、2要素認証と呼ばれています。

2要素認証とは?

2要素認証 (または 2段階認証、複数要素認証、2FA) は、パスワードだけを利用するよりも遥かに強度が高まります。2要素認証では、自分の身元を証明するために一つでは無く、二つの手法を必要とします。ATM 用のカードが良

ログイン情報を保護する

い事例です。ATM　機器でお金を下ろす際、2要素認証を利用しています。現金を入手するためには、二つのものが必要です。一つ目は ATMカード (所持情報)、二つ目は PIN 番号 (知識情報) です。ATM カードを紛失または盗難された場合でも、PIN 番号を知らない限り、他人はお金を引き出すことはできません。つまり盗難者は、ATM　カードと　PIN　番号の両方が無いと、お金を勝手に引き出すことができないということです。2要素認証は、これと同じコンセプトです。



可能な限り、2要素認証を使ってアカウントを保護してください。インターネット上で、自分を守るためにできること中でも効果が高いものです。

2要素認証の仕組み

2要素認証は、主要な銀行、メールおよびソーシャルネットワーキングのサイトで提供されています。また、多くのサイトでは、2要素認証を有効にするための手順　(追加情報はリソースを参照)　が詳細に解説されています。2要素認証を有効にした後、次のように動作することが多いです。まず、はじめに、通常通りユーザ名とパスワードを使ってアカウントにログインします。これが、二つのうち、一つ目の要素 - 知識情報です。その後、固有のコードをスマートフォンなどでテキストメッセージとして受信し、ログイン画面で入力します。これが、2要素目 - スマートフォンを所持していないとコードは確認できません。これによって、アカウントを保護できます。サイバー犯罪者がパスワードを盗んだとしても、スマートフォンも所持していないとアカウントへのアクセスはできません。

テキストメッセージ経由で固有のコードを受信する代わりに、スマートフォンに認証用のアプリをインストールすることもできます。このモバイルアプリは、ログインする度に固有のコードを生成します。このモバイルアプリを利用する利点として、コードがテキストメッセージ経由で送られるのではなく、コードを生成するためにアプリの安全性が高いことが挙げられます。また、通話サービスを使用していない状態でも固有のコードを入手することができるという利点もあります。このアプリを利用することで、いつでもログインするためのコードを生成することが可能です。

ログイン情報を保護する

2要素認証は、一見作業が増えるように見えますが、自分の個人情報の安全性は遥かに高まります。アカウントがハッキングされてからではなく、メールやオンラインバンキング、ソーシャルメディアなどの重要なアカウントに対し、2要素認証を有効にして保護を強化してください。そして、自分のアカウントのセキュリティが向上したことで少しでも安心してください。

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、国内でも有数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などの提供を通じて、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

パスフレーズについて:	https://securingthehuman.sans.org/ouch/2017#april2017
2要素認証を提供しているサイト:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google の2要素認証:	http://www.google.com/landing/2step/

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Translated By: 内山　貴之, 時田　剛